Cisco Broadband Access Center 3.9 Release Notes

Revised: December, 2014, OL-32133-01

These release notes contain details on the new software features, bug fixes, and documentation for Cisco Broadband Access Center (Cisco BAC), Release 3.9.

Contents

Introduction

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

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.

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

Cisco BAC enables you to provision and manage 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, TR-106, and TR-196 standards. These devices include Ethernet and ADSL gateway devices, wireless gateways, VoIP ATAs, DLC, and other devices that are compliant with CWMP. For details about the features supported in Cisco BAC 3.9, see New Features in Cisco BAC 3.9, page 3 section.

System Components

Cisco BAC comprises:

- A Regional Distribution Unit (RDU) that is a software that you install on your server. The RDU is the primary server in a Cisco BAC deployment. Through its extensible architecture, the RDU supports the addition of new technologies and services.
- The Device Provisioning Engine (DPE) that is a software that you install on your server. The DPE server handles all device interactions for the RDU.
- An administrator user interface through which you can monitor and manage Cisco BAC.
- A Java provisioning application programming interface (API). You can use this to integrate Cisco BAC into an existing operations support-system environment. You can use the provisioning API to register devices in Cisco BAC, assign device configuration policies, run CWMP operations on the device, and configure the entire Cisco BAC provisioning system.
- Cisco Network Registrar extensions (CNR extensions), are the links between Cisco BAC and Cisco Network Registrar. You should install this component on all Cisco Network Registrar servers in your Cisco BAC environment. If you are deploying Cisco BAC in a failover environment, ensure that you install the extensions on the failover servers, as well.
- A STUN server that 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.
- The Cisco Prime Access Register (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.

System Requirements

You must have the Solaris 10, or Linux 5.x or 6.1 operating system installed on your system to use the Cisco BAC software. For information on installation, see the *Cisco Broadband Access Center 3.9 Installation Guide*.

Licensing Requirements

You require a valid license key to successfully provision devices that use Cisco BAC. These licenses are specific to the:

- CWMP technology
- DPE component
- Feature Pack Licensing

Note Feature Pack licensing is required only for Java based DPE Technology extensions. If you have not yet received your licenses, contact your Cisco representative.

New Features in Cisco BAC 3.9

The new features in Cisco BAC 3.9 are:

Advanced LTE Provisioning

Cisco BAC supports construction of configuration template for advanced LTE parameters, and writes the constructed parameters to Ubiquisys LTE access point.

The new advanced LTE parameters, based on TR-196v2 data model, are available as part of the existing parameter dictionary, *tr196-cwmp-dictionary-v2.0.xml*. If the location of LTE is valid, these parameters are passed to LTE using the configuration templates.

Based on *TR-181 Issue 2 Amendment 2* and *TR-196 Issue 2 Femto Access Point Service Data Model*, the following parameters are supported for this feature:

Device.ManagementServer.PeriodicInformEnable

Device.ManagementServer.PeriodicInformInterval

Device.ManagementServer.PeriodicInformTime

Device.Time.NTPServer1

Device.Time.LocalTimeZoneName

Device.Time.LocalTimeZone

Device.Time.X_CISCO_COM_OperatorNTPServer1

Device.Time.X_CISCO_COM_OperatorNTPServer2

Device.FAP.X_CISCO_COM_DIAGNOSTICS.PostEventUploadURL

Device.FAP.X_CISCO_COM_DIAGNOSTICS.PostEventUploadUsername

Device.FAP.X_CISCO_COM_DIAGNOSTICS.PostEventUploadPassword

Device.FAP.PerfMgmt.Config.Enable

Device.FAP.PerfMgmt.Config.URL

Device.FAP.PerfMgmt.Config.Username

Device.FAP.PerfMgmt.Config.Password

Device.FAP.PerfMgmt.Config.PeriodicUploadInterval

Device.FAP.PerfMgmt.Config.PeriodicUploadTime

Device.FAP.PerfMgmt.Config.X_CISCO_COM_JobId

FAPService.1.CellConfig.LTE.RAN.Mobility.IdleMode.Common.Qhyst

Device.Services.FAPService.1.DNPrefix

Device.Services.FAPService.1.FAPControl.LTE.Gateway.SecGWServer1

Device.Services.FAPService.1.FAPControl.LTE.Gateway.S1SigLinkServerList

Device.Services.FAPService.1.FAPControl.LTE.Gateway.S1SigLinkPort

Device.Services.FAPService.1.AccessMgmt.LTE.AccessMode

REM Scan Capability Check for LTE and 4G Scan Support

During the scan flow for LTE, Cisco BAC checks for the actual UMTS and GSM capability of the device, even though FC-3G-REM-SCAN and FC-2G-REM-SCAN are set to *true* for the device.
This ensures that the wait time for the scan completion is avoided, if the LTE does not support UMTS and GSM capabilities.

A new custom property FC-4G-REM-SCAN (boolean) is also introduced to support the GA scan flow of LTE. This feature also ensures that the LTE neighbor is also identified, apart from the 2G and 3G neighbors (as supported in the previous releases).

Enhancement in REM-based Location Verification

A new custom property FC-DNB-CONFIG-NWL-LIST-COUNT is introduced. Using this, you can configure the number of neighbors that are updated in NWL benchmark. The neighbors are sorted based on power.

This release also supports RSSI for NWL benchmark update and for the 3G neighbor power comparison.

A new custom property FC-DNB-FREQ-MATCH is also introduced to compare the neighbors using frequency, instead of GUID.

A new custom property FC-PERIODIC-NWL-SCAN-INTERVAL is introduced to set the periodic NWL scan interval. Based on success or failure of location verification this property will be updated. For success, it is set as 24 hours; for failure it is set as 20 minutes.

The periodic NWL scan interval is also set based on the success or failure of location verification. For success, it is set as 24 hours; and for failure, it is set as 20 minutes.

Intra Chassis Chained Location Verification

This release of Cisco BAC supports Intra Chassis Chained Location Verification to skip the location verification on one technology type (2G, 3G, 4G) from same chassis, if other technology type has already completed location verification. This is applicable to location verification methods like GPS and REM scans.

This feature is applicable among all RATs in a chassis, and whichever access point (AP) passes the location verification first, becomes the anchor AP in the chassis. To achieve this, new custom properties are introduced:

- FC-CIC-ENABLED
- FC-CIC-STATUS
- FC-CIC-STATUS-TS
- FC-CIC-ANCHOR-AP-EID
- FC-CHASSIS-ID
- FC-PEER-RAT-ID

Modified UMTS Provisioning Flow

A new custom property FC-GPS-TIME-OUT is introduced to configure the scan timeout value for GPS, at the initial boot. This value is used to wait for the GPS status to become as 'Success' or 'Error_Timeout', before proceeding with PLMN/NWL based location verification.

The NWL benchmark is also saved/updated if DNM location verification is successful, apart from DNB method. To achieve this, new custom properties are introduced:

- FC-DNM-BENCHMARK-UPDATE
- FC-DNB-FAIL-ACTION

Static Neighbor List Configuration

For the Femtocell AP, Cisco BAC supports configuring a Static Neighbor List, which is a fixed neighbor configuration, without considering the detected neighbors by the Access Point as a result of the REM scan process.

All the parameters under the following objects are supported (as defined in TR-196v2 data model), and can be defined in the configuration template:

- .FAPService.{i}.CellConfig.LTE.RAN.NeighborList.LTECell.{i}
- .FAPService.{i}.CellConfig.LTE.RAN.NeighborList.InterRATCell.UMTS.{i}

- .FAPService.{i}.CellConfig.LTE.RAN.NeighborList.InterRATCell.GSM.{i}
- .FAPService.{i}.CellConfig.LTE.RAN.NeighborList.InterRATCell.CDMA2000.{i}
- .FAPService.{i}.CellConfig.LTE.RAN.NeighborListInUse.LTECell.{i}
- .FAPService.{i}.CellConfig.LTE.RAN.NeighborListInUse.InterRATCell.UMTS.{i}
- .FAPService.{i}.CellConfig.LTE.RAN.NeighborListInUse.InterRATCell.GSM.{i}
- .FAPService.{i}.CellConfig.LTE.RAN.NeighborListInUse.InterRATCell.CDMA2000.{i}

Security Hardening

This release of Cisco BAC provides strict password rules to enhance security. The new rules apply to the Administrator User Interface login and the user management.

The password rules are enhanced with the following changes:

- Password length should be between 8 and 127 characters
- The password must include at least one special character, one numeric character, one alphabet in uppercase, and one alphabet in lower case. BAC supports the five special characters (*,@#
- While changing the password, the new password should not contain a similar pattern (three consecutive characters) as with the previous password.

Subgroup Support for CIG

This release of Cisco BAC supports subgroup under a group. The subgroup can be associated with an Anchor AP for supporting Chained Intra Grid (CIG).

Whenever BAC receives boot notification from an AP, and if it is the first one to complete Location Verification, it is qualified as Anchor AP. The details of this Anchor AP is updated on both subgroup and the group where it belongs.

For supporting this feature, the property FC-CIG-GROUP-TYPE is enhanced to support comma-separated values, and a new property FC-PARENT is introduced to specify the parent group of subgroup. The subgroup and parent group can be of different group types.

AP Tamper Detection and Reset

- AP can be tampered and cleared on individual AP level
- AP can be tampered and cleared on Chassis level.

AP can be tampered and cleared on individual level

When the AP is found to be tampered, it is marked as tampered. While the AP is booted, the DPE finds that the AP is tampered and is avoided for further initialization with DPE. To reset the device, the operator needs to manually reset the device by visiting the location.

By using the tamper detection and reset functionality, the operator can clear the tamper flag of the device from remote location.

AP can be tampered and clear on Chassis level

The AP tamper detection and reset on Chassis level is a STOP gap solution to LTE AP. The reason behind is LTE AP does not support data model for tampering. So considering this if UMTS is tampered in a Chassis, BAC should have a mechanism to set LTE (peer RAT) also tampered.

In order to work with this feature, Chassis ID is must and it should be received in each inform of AP. BAC has the capability to retrieve Chassis ID and Peer RAT ID from each of inform of AP and store them in a session and then check the AP reports that is tampered, if it is tampered BAC perform the operation to set the peer RAT as tampered as well.

If current AP and Peer RAT AP set as tampered, tamper event (TAMPERED_EVENT) will be fired with Chassis and Peer RAT ID details.

The following custom properties need to be enabled to perform this feature on UMTS:

FC-TAMPER-ENABLED and for LTE this is an optional.

Key Performance Indicators (KPI) for RDU and DPE

Cisco BAC collects the counter values of various Key Performance Indicators (KPI) periodically, for both DPE and RDU, and presents these values in .csv file format. This helps to upload these counters to performance management products like Cisco Prime Performance Manager.

IPv6 Address support for LTE device

In this release, BAC will start supporting the LTE FAPs (HeNB devices) which would be assigned with IPSec address in IPv6 format. As a part of that, BAC will support connection request through discovery mechanism ("/IPDevice/connectionRequestMethod" set as "Discovered") for the LTE FAPs (HeNB devices) provided DPE is running on a server that supports dual stack. Connection request for LTE FAPs with IPv6 IPSec address using lease query method will not be supported in this release.

Chassis ID Discovery and Mapping

The Chassis ID discovery and mapping is a feature introduced in RMS 5.0 and its main purpose of this feature is to discover chassis and peer RAT details from inform message.

Irrespective of Chained Intra Chassis location verification is enabled or disabled, BAC should have a capacity to discover the configured parameters (Chassis ID and Peer RAT ID) of any technology type devices (UMTS, LTE) on each forced inform.

The following custom properties will be updated on device level with chassis and peer RAT details:

FC-CHASSIS-ID

FC-PEER-RAT-ID

GPN and GPV Optimization

Improvement in CWMP Session Time by Minimizing DPE to AP Transactions This release of Cisco BAC provides improved CWMP session time. This is achieved by:

- Enabling the DPE to discover the capability parameters of the AP only once, and not during all inform messages
- Avoiding GPV for every value change on the AP, by referring to the SAC value from the RDU instead of GPV to the AP
- Avoiding redundant GPV and GPN performed on AP for the same parameters. This is done by grouping the related parameters.

Broadband Access Center 3.9 Bugs

Use the Bug Search tool to search for a specific bug or to search for all bugs in a release.

Procedure

Step 1 Go to http://tools.cisco.com/bugsearch.

Step 2 At the Log In screen, enter your registered Cisco.com username and password; then, click **Log In**. The Bug Search page opens.

Note If you do not have a Cisco.com username and password, you can register for them at http://tools.cisco.com/RPF/register/register.do.

Step 3 To search for a specific bug, enter the bug ID in the Search For field and press **Enter**.

Step 4 To search for bugs in the current release:

a. In the Search For field, enter **Broadband Access Center 3.9**, and press **Enter** (Leave the other fields empty).

b. When the search results are displayed, use the filter tools to find the types of bugs you are looking for. You can search for bugs by modified date, status, severity, and so forth.

Tip To export the results to a spreadsheet, click **Export Results to Excel**.

Related Documentation

For details, see the Cisco Broadband Access Center 3.9 Administration Guide and the Cisco Broadband Access Center 3.9 Installation Guide.

The following document gives you the list of user documents for Cisco Prime Network Registrar 8.1:

http://www.cisco.com/en/US/docs/net_mgmt/prime/network_registrar/8.1/doc_overview/guide/CPNR_8_1_Doc_Guide.html

The following document gives you the list of user documents for Cisco Prime Access Registrar 6.0:

http://www.cisco.com/en/US/docs/net_mgmt/prime/access_registrar/6.0/roadmap/guide/PrintPDF/ardocgd.html

Accessibility Features in Broadband Access Center 3.9

For a list of accessibility features in Broadband Access Center, see the Voluntary Product Accessibility Template (VPAT) on the Cisco website, or contact accessibility@cisco.com.

Note All product documents are accessible except for images, graphics, and some charts. If you would like to receive the product documentation in audio format, braille, or large print, contact accessibility@cisco.com.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at: http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.