Cisco Broadband Access Center 3.7 Installation Guide

March 30, 2012

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-25684-01

Cisco Broadband Access Center 3.7 Installation Guide

CONTENTS

Preface

The *Cisco Broadband Access Center 3.7 Installation Guide* describes general requirements and installation procedures for Cisco Broadband Access Center, which is referred to as Cisco BAC throughout this installation guide.

This chapter provides an outline of the other chapters in this guide, details information about related documents that support this Cisco BAC release, and demonstrates the styles and conventions used in the guide.

Audience

System integrators, network administrators, and network technicians can use this installation guide to install Cisco BAC on a Solaris or Linux operating system.

Organization

This guide includes the following sections:

Section	Title	Description
Chapter 1	Introduction	Describes general requirements for a successful installation of Cisco BAC.
Chapter 2	Before You Begin	Describes factors to consider as you prepare to install Cisco BAC. For example, the individual components of Cisco BAC, the database requirements, and the order of operations for installing the software.
Chapter 3	Installing and Uninstalling Cisco BAC on Solaris	Describes how to install the individual components of Cisco BAC on Solaris.
Chapter 4	Installing and Uninstalling Cisco BAC on Linux	Describes how to install the individual components of Cisco BAC on Linux.
Chapter 5	Configuring the Syslog Utility to Receive Cisco BAC Alerts	Describes how to configure the syslog file to receive alerts after Cisco BAC is installed.

Conventions

This document uses the following conventions:

Convention	Indication
bold font	Commands and keywords and user-entered text appear in **bold** font.
italic font	Document titles, new or emphasized terms, and arguments for which you supply values are in *italic* font.
[ ]	Elements in square brackets are optional.
{x | y | z }	Required alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
`courier` font	Terminal sessions and information the system displays appear in `courier` font.
< >	Nonprinting characters such as passwords are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Note Means *reader take note*.

Tip Means *the following information will help you solve a problem*.

Caution Means *reader be careful*. In this situation, you might perform an action that could result in equipment damage or loss of data.

Product Documentation

Note We sometimes update the printed and electronic documentation after original publication. Therefore, you should also review the documentation on Cisco.com for any updates.

Table 1 describes the documentation that is available for this Cisco BAC release.

Table 1 Product Documentation

Document Title	Location
Cisco Broadband Access Center 3.7 Documentation Overview	On Cisco.com at this URL: http://www.cisco.com/en/US/docs/net_mgmt/broadband_access_center/3.7/documentation/overview/Cisco_BAC37_DocOverview.html
Cisco Broadband Access Center 3.7 Release Notes	On Cisco.com at this URL: http://www.cisco.com/en/US/products/sw/netmgtsw/ps529/prod_ release_notes_list.html
Cisco Broadband Access Center 3.7 Administrator Guide	On Cisco.com at this URL: http://www.cisco.com/en/US/products/sw/netmgtsw/ps529/prod_maintenanceS_guides_list.html
Cisco Broadband Access Center 3.7 Integration Developer's Guide	On Cisco.com at this URL: http://www.cisco.com/en/US/products/sw/netmgtsw/ps529/prod_command_reference_list.html
Cisco Broadband Access Center 3.7 DPE CLI Reference	On Cisco.com at this URL: http://www.cisco.com/en/US/products/sw/netmgtsw/ps529/prod_command_reference_list.html
Cisco Broadband Access Center 3.7 Third Party and Open Source Copyrights	On Cisco.com at this URL: http://www.cisco.com/en/US/products/sw/netmgtsw/ps529/products_licensing_information_listing.html

Related Documentation

Note We sometimes update the printed and electronic documentation after original publication. Therefore, you should also review the documentation on Cisco.com for any updates.

Table 2 describes additional documentation that is available for this release of Cisco BAC.

Table 2 Related Documentation

Document Title	Available Format
Release Notes for Cisco Network Registrar 7.2	On Cisco.com: http://www.cisco.com/en/US/products/sw/netmgtsw/ps1982/prod_release_notes_list.html
Installation Guide for Cisco Network Registrar, Release 7.2	On Cisco.com: http://www.cisco.com/en/US/products/sw/netmgtsw/ps1982/prod_installation_guides_list.html
User Guide for Cisco Network Registrar, Release 7.2	On Cisco.com: http://www.cisco.com/en/US/products/sw/netmgtsw/ps1982/products_user_guide_list.html
Command Reference Guide for Cisco Network Registrar, 7.2	As an HTML document that you can view in your web browser when you install the software. The document is available at **Start > Programs > Network Registrar > Network Registrar CLI Reference Guide**. On Cisco.com: http://www.cisco.com/en/US/products/sw/netmgtsw/ps1982/prod_command_reference_list.html
Quick Start Guide for Cisco Network Registrar, Release 7.2	On Cisco.com: http://www.cisco.com/en/US/products/sw/netmgtsw/ps1982/prod_installation_guides_list.html

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 an RSS feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service. Cisco currently supports RSS Version 2.0.

CHAPTER 1

Introduction

This chapter gives 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 the Cisco BAC provisioning system. You should install the RDU on a Solaris 10 server or a Linux 5 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 DPE CLI Reference, Release 3.7*. For information on the Cisco BAC watchdog process, see the *Cisco Broadband Access Center Administrator's Guide, Release 3.7*.

- 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 DPE CLI Reference, Release 3.7*.

- CNR extensions

  The 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 fail-over environment, ensure that you also install the extensions on the fail-over servers.

  You must install Cisco BAC Cisco Network Registrar extensions on a server running Network Registrar 7.2. If you do not want to install these extensions, you do not need to install Cisco Network Registrar.

- CAR extensions

  The CAR extensions are the links between Cisco BAC and Cisco Access Registrar. You should install this component on all Cisco 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 CAR extensions on a server running Cisco Access Registrar 5.0.0.3 or later. If you do not want to install these extensions, you do not need to install Cisco Access Registrar.

  Cisco 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.

CHAPTER 2

Before You Begin

This chapter describes the requirements and dependencies for installing Cisco BAC successfully.

Operating System Requirements

On Solaris

You must install Cisco BAC on a Sun SPARC platform that runs Solaris 10 operating system with at least 4 GB of memory. We recommend that you use a Sun SPARC multiprocessor platform.

Note Before installing Cisco BAC, download and install the recommended Solaris patches from the Sun Microsystems support site.
Cisco BAC ships with the required JRE version 1.6.0_27, which resides in the *BPR_HOME*/jre directory.

Ensure that you have the latest Solaris patch bundle for the operating system installed in your system, before you install Cisco BAC. We recommend *Solaris 10 08/11* for Solaris 10 operating system.

You must also download and install the Java Platform Standard Edition (Java SE) cluster patches recommended by Sun Microsystems to install Cisco BAC on a system that runs Solaris 10, see Table 2-1.

Table 2-1 Java Standard Edition Cluster Patches for Solaris 10

Patch	Description
120900-04	libzonecfg patch
121133-02	Zones library and zones utility patch
119254-44	Install and patch utilities patch, for more information, see Chapter 3, "Installing and Uninstalling Cisco BAC on Solaris"
118918-24	Solaris crypto framework patch
119042-10	svccfg and svcprop patch
119578-30	FMA patch
144488-09	Kernel patch

Before you install Cisco BAC, you must install the **SUNWxcu4** package available as part of the Solaris OS installation. This is an optional package that you might not have installed while installing Solaris.

On Linux

For Linux, you must install Cisco BAC on Red Hat Enterprise Linux 5 using x86 and 64 bit hardware system with at least 4 GB of memory. The SELinux should be disabled. Also, ensure that before installing Cisco BAC, you install the **sysstat** package for the proper execution of the diagnostic scripts. This is an optional package which you might have not installed while installing Linux.

Minimum Hardware Requirements

Table 2-1 lists the minimum hardware requirements for the various Cisco BAC components.

Table 2-2 Minimum Hardware Requirements

Component	Model	RAM	CPU	Minimum Disk
DPE	Sun T5210 Solaris 10 Linux 5	4 GB 4 GB	1 with 4 cores 1 with 4 cores	2,15K rpm
RDU	Sun T5210 Solaris 10 Linux 5	16 GB 16 GB	1 with 8 cores 1 with 8 cores	2,15K rpm
STUN (required only for devices behind NAT setup)	Sun T5210 Solaris 10 Linux 5	4 GB 4 GB	1 with 4 cores 1 with 4 cores	2,15K rpm
RAID Array	Storage Tek 3320	512 MB	—	8,15K rpm Two RAID 1+0 volumes
SSL Accelerator and Load Balancer	Cisco ACE 4710 or module for Cisco 7600	—	—	—

Deployment Requirements

This section details the minimum hardware requirements that you need to successfully deploy Cisco BAC in your environment. This section contains:

Smallest Fully Redundant Deployment

A smallest fully redundant deployment of about 500,000 devices can be configured with one provisioning group that has two DPEs. This setup requires:

- Two RDU servers
- One RAID unit
- Two DPE servers
- One CAR server
- Two Cisco ACE units
- Two Cisco Network Registrar servers
- STUN server (required only for devices behind NAT setup)
- CMHS server

Incremental Scaling

For every additional 500,000 devices that you add, you need two DPEs configured in a new provisioning group. A single deployment can handle up to eight million devices.

A single pair of load balancers can handle DPEs in multiple provisioning groups. We recommend that you determine the number of load balancers, based on the network configuration of your service provider.

Types of Installation

This section describes how to install individual Cisco BAC components. The installation program enables you to install one or all components of Cisco BAC; that is, RDU, DPE, Cisco Network Registrar Extension Points, Cisco Access Registrar Extension Points and STUN server.

Note This release does not feature a lab installation, but you can perform its equivalent by installing all components on a single machine. To perform the activity, we recommend that you have at least 500 MB of disk space available.

You can install RDU, DPE, Cisco Network Registrar and Cisco Access Registrar through the CLI. For details on component installation, see Installing and Uninstalling Cisco BAC on Solaris, page 3-1 for Solaris and Installing and Uninstalling Cisco BAC on Linux, page 4-1 for Linux.

Before you install Cisco BAC, familiarize yourself with the installation startup processes and checklists described in Before You Begin, page 2-1.

See the Installation Worksheet, page 2-9, for information on Cisco BAC installation parameters.

Installation Checklist for Solaris

Before you run the installation program, use the following checklist to ensure your readiness.

Table 2-3 Installation Checklist for Solaris

Task	Checkoff
1. Verify the system hardware and software requirements described in Introduction, page 1-1.	❑
2. Verify the file system block size of the directory in which you intend to install the Cisco BAC database and the database transaction log files (see the Database Requirements, page 2-6).	❑
3. Ensure that you have root access to the computers on which you intend to install Cisco BAC components.	❑
4. Have your Cisco BAC license key or keys at hand. You need a valid license key for each technology that you want to provision with Cisco BAC, namely CWMP and the DPE. If you have not received your licenses, contact your Cisco representative before you proceed further.	❑
5. Determine the home directory (*BPR_HOME*) on which you want to install the Cisco BAC component or components. The default directory is /opt/CSCObac. We recommend that you have at least 500 MB of disk space available for the home directory as well as for the /tmp directory and 5 MB of disk space available for /etc/init.d directory.	❑
6. For the RDU, determine where you want to install the data directory (*BPR_DATA*) and the database transaction logs (*BPR_DBLOG*). By default, the database transaction logs directory (*BPR_DBLOG*) is installed in the same directory as the data directory (*BPR_DATA*). We recommend that you locate the database transaction logs directory on the fastest disk on the system. The installation program, by default, installs the data directory (*BPR_DATA*) in a location other than that of the home directory (*BPR_HOME*). The default location for the data directory is /var/CSCObac. We recommend that the data directory be on a different physical disk than the home directory; for example, /var/disk0/CSCObac. Your disk should have a minimum 1 GB free space. The specified directory becomes the top-level directory under which the installation program creates a number of subdirectories; for example, /var/disk0/CSCObac/rdu/db.	❑

Table 2-3 Installation Checklist for Solaris (continued)

Task	Checkoff
7. Cisco BAC servers use the same password for all components in your network. This password is used as a token to authenticate communication among the different components of the Cisco BAC server. Enter the shared secret password used by the Cisco BAC components for the RDU in the network. The shared secret password is the same for all Cisco BAC servers in your network. To find a list of Cisco BAC installation parameters, see Installation Worksheet, page 2-9.	❑
8. You must enter a listening port number for the RDU. This port is the interface that the RDU uses to communicate with the DPE. The default port is 49187.	❑

Installation Checklist for Linux

Before you install Cisco BAC, review the checklist in Table 2-4.

Table 2-4 Installation Checklist for Linux

Task	Checkoff
1. Verify whether your system meets the minimum system hardware and software requirements described in Chapter 1, "Introduction."	❑
2. Ensure that you have access to the computers on which you intend to install Cisco BAC components.	❑
3. Save your license file on the system from which you intend to launch the Cisco BAC administrator user interface through a web browser. You need a valid service license file to configure Cisco BAC licensing.	❑
4. Determine the home directory (*BPR_HOME*) in which you want to install the Cisco BAC component or components. The default directory is /opt/CSCObac. Ensure that the target installation directory has enough disk space. We recommend that you have at least 500 MB of disk space available; otherwise installation will not take place.	❑
5. Verify that you have at least 512 MB of free space available in the /tmp directory for successful installation.	❑
6. For the RDU, determine where you want to install the data directory (*BPR_DATA*) and the database logs (*BPR_DBLOG*). The default directory is /var/CSCObac. Ensure that the target installation directory has enough disk space. We recommend that you locate the data directory on a different physical disk than the home directory; for example, /var/disk0/CSCObac. The disk should have at least 1 GB of free space. The installation program, by default, installs the data directory, the database transaction logs directory, and the logs directory in the same location. We recommend that you locate the database transaction logs directory on the fastest disk on the system. Also, ensure that 1 GB of disk space is available.	❑

Table 2-4 Installation Checklist for Linux (continued)

Task	Checkoff
7. For the RDU, determine the listening port number. The RDU uses this interface to communicate with the other Cisco BAC components, such as DPEs and Cisco Network Registrar extension points. The default port is 49187.	❑
8. For the RDU, determine the shared secret password that Cisco BAC servers on your network use, as a token to authenticate communication with one another. The shared secret password should be the same for all Cisco BAC servers on your network.	❑
9. For the RDU, determine the ports through which you will access the administrator user interface, using HTTP or HTTP over SSL (HTTPS). The default ports are: – 80 for HTTP – 8443 for HTTPS	❑
10. For the DPE, ensure that 2 GB of disk space is available in the data directory.	❑
11. Ensure that Cisco Network Registrar 7.2 is installed and running on the servers on which you are installing Cisco BAC extensions.	❑
12. For the Cisco Network Registrar extensions, determine the name of the provisioning group to which the Cisco Network Registrar server belongs.	❑
13. For the Cisco Network Registrar extensions, determine where you want to install the data directory (*BPR_DATA*). The default directory is /var/CSCObac. Ensure that 200 MB of disk space is available.	❑
14. To disable SELinux feature, you must disable enforcement on the system. **a.** To temporarily disable enforcement on a running system, run: `/usr/sbin/setenforce 0` **b.** To permanently disable enforcement during a system startup, change: `enforcing` to `disabled` in /etc/selinux/config, and then reboot the machine. By default, the SE Linux feature is set to enforcing.	❑
15. To disable iptable, run: `/etc/init.d/iptables stop`, and then reboot the machine. **Note** The Admin UI page will not open if Iptable is in enabled state on the system.	❑

Database Requirements

Before you install Cisco BAC, check the following:

- File System Block Size, page 2-7.
- Support for Large Files, page 2-8.

File System Block Size

On Solaris, for optimum performance and reliability of the Cisco BAC database, configure the file system or systems that contain the database files and database transaction log files, with an 8-KB block size or greater. If your system configuration does not support an 8-KB block size, then configure the block size in multiples of 8 KB; for example, 16 KB or 32 KB.

The block size cannot be changed after the Unix File System (UFS) is mounted with a value. The value has to be set during Solaris disk partition.

On Linux, block size is selected at the time of high-level formatting. If the mke2fs (i.e.,make ext2 filesystem) command is used to create the filesystem, valid block size vales are 1024, 2048 and 4096 bytes. The block size for any existing ext2 or ext3 file system (the most common file system types on Linux) can be obtained by using the dumpe2fs command with the device name as an argument.

The installation program prompts you to specify a directory in which you prefer to install database files and database transaction log files. These directories are identified in Cisco BAC with system variables BPR_DATA and BPR_DBLOG, respectively.

To verify that a directory resides on a file system with a minimum block size:

Step 1 Run the UNIX **mount** command without any parameters to determine on which file system device the directory resides. The default directory is /var/CSCObac.

For example:

```
# mount
/var on /dev/dsk/c0t0d0s4 read/write/setuid/intr/largefiles/onerror=panic/dev=2200004 on Mon Nov 26
08:07:53
```

In this example, the file system device is */dev/dsk/c0t0d0s4*.

Step 2 To determine the block size of the file system, use the **df** command.

For example:

On Solaris:

```
# df -g /dev/dsk/c0t0d0s4
/var       (/dev/dsk/c0t0d0s4 )     8192 block size      1024 frag size
         961240 total blocks      851210 free blocks    755086 available    243712 total
files
         239730 free files        35651588 filesys id    ufs fstype         0x00000004
flag            255 filename length
```

In this example, the block size is 8192 bytes, which is 8 KB. The block size of the selected directory, therefore, is correct.

On Linux:

```
# df -k .
Filesystem           1K-blocks      Used Available Use% Mounted on
/dev/sda2             16246460   3248448  12159420  22% /
#  /sbin/dumpe2fs /dev/sda2 | grep 'Block size'
Block size:               4096
```

In this example, the block size is 4096 bytes, which is 4 KB.

Support for Large Files

Ensure that the file system in which you place database files is configured to support files larger than 2 GB.

To verify large file support:

Step 1 Run the UNIX **mount** command without parameters.

Step 2 Note whether the intended file system contains the keyword **largefiles**.

For example:

```
# mount
/var on /dev/dsk/c0t0d0s4 read/write/setuid/intr/largefiles/onerror=panic/dev=2200004 on Mon Nov 26
08:07:53
```

In this example, the output contains the keyword **largefiles**. This file system, therefore, can support files greater than 2 GB.

Required Port Information

Before you install Cisco BAC, determine the ports on which the Cisco BAC components, the RDU, the DPE, CNR extensions and CAR extensions, listen during communication to one another or to the CPE.

The installation program checks for the availability of all ports: both configurable and nonconfigurable.

If the port that you have specified is unavailable, the installation program displays a message; otherwise, the message similar to the following, appears:

```
Not a valid port number
```

In the case of a nonconfigurable port, the installation program notifies you and exits the program without making any changes to the system.

Table 2-5 lists the required external inbound ports and their default values.

Table 2-5 Default External Inbound Ports Used by Cisco BAC Components

Component	Default Port Number	Protocol	Configurable	Used by
RDU	161	UDP	No	SNMP Get
RDU	49187	TCP	Yes	DPE and API access
RDU	80	TCP	No	Admin Web UI HTTP
DPE	49186	UDP	Yes	CPE Prov Group locator
DPE	2323	TCP	Yes	DPE CLI
DPE	7547	TCP	Yes	TR-069 CWMP 1
DPE	7548	TCP	Yes	TR-069 CWMP 2
DPE	7549	TCP	Yes	HTTP File Service 1
DPE	7550	TCP	Yes	HTTP File Service 2

Table 2-5 Default External Inbound Ports Used by Cisco BAC Components (continued)

Component	Default Port Number	Protocol	Configurable	Used by
CNR-EP (Listening port)	68	UDP	Yes	Lease Query
CAR-EP	7551	HTTP	Yes	FAS
STUN	3478	UDP	Yes	STUN Binding Service
STUN	8000	HTTP	Yes	CXF

Table 2-6 lists the external outbound ports and their default values.

Table 2-6 Default External Outbound Ports Used by Cisco BAC Components

Component	Number	Protocol	Configurable	Used by
RDU	162	UDP	No	SNMP Traps
DPE	49186	UDP	Yes	CPE Prov Group locator
DPE	162	UDP	Yes	SNMP Traps
CNR-EP (Server port)	67	UDP	Yes	Lease Query
CAR	1645, 1646	UDP	Yes (in CAR)	FAS (RADIUS)

Table 2-7 lists the internal ports and their default values.

Table 2-7 Default Internal Ports Used by Cisco BAC Components

Component	Number	Protocol	Configurable	Used by
RDU	49887	TCP	Yes	Internal watchdog and SNMP agent communication
DPE	49887	TCP	Yes	Internal watchdog and SNMP agent communication
RDU	8001	SNMP (UDP)	Yes	SNMP Internal
DPE	8001	SNMP (UDP)	No	SNMP Internal

Installation Worksheet

This section describes the basic configuration information that you need to ensure a successful installation of Cisco Broadband Access Center (Cisco BAC). Table 2-7 is a worksheet that you can use to record the information specific to the installation.

Table 2-8 Cisco BAC Installation Parameters

Prompt	Description	Default Value
Home directory	Root directory to install Cisco BAC.	/opt/CSCObac
Data directory	Root directory that stores the Data directory for the Cisco BAC components.	/var/CSCObac
Database logs directory	Root directory that Cisco BAC uses to install the database transaction logs for Cisco BAC components.	/var/CSCObac
Logs directory	Root directory to install the general transaction logs for Cisco BAC Components.	/var/CSCObac
RDU port number	Port number that the RDU uses to communicate with the other Cisco BAC Components.	49187
Port number of administrator user interface	Port number that you use to access the Cisco BAC administrator user interface using HTTP.	80
Default Cisco BAC administrator	User name that you use to access the Cisco BAC administrator user interface.	bacadmin
Default administrator password	Password to access the Cisco BAC administrator user interface.	changeme
Installation password	Password that you use to install Cisco BAC from the CLI.	secret
Default DPE CLI password	Password that you use to access the DPE CLI.	changeme
CNR extension points provisioning group name	Name of the provisioning group for CNR extensions.	None
STUN HTTP Listening port	STUN CXF RESTful server port.	80
STUN UDP Listening port	STUN server UDP port.	3478
STUN HTTP user name	STUN CXF RESTful server user name.	bacadmin
STUN HTTP user name	STUN CXF RESTful server port.	cisco
Shared secret	Shared secret password for UDP connection request authentication.	secret

CHAPTER 3

Installing and Uninstalling Cisco BAC on Solaris

This chapter explains how to work with the Cisco BAC program to install the Cisco BAC components—RDU, DPE, Cisco Network Registrar Extension Points, Cisco Access Registrar Extension Points and STUN server. You can install the Cisco BAC components from the CLI. Both interfaces are supplied with the product.

You can download the Cisco BAC softwares from the below location:

http://www.cisco.com/cisco/software/navigator.html?mdfid=273446653

Caution If you interrupt the installation program after it begins copying files, you must manually clean up the locations of copied files, specifically *BPR_HOME*. For detailed information, see Uninstalling Cisco BAC, page 3-33.

Be sure to install the RDU before installing the DPE. If you choose to install the DPE without installing the RDU, or without an RDU already installed on your system, the DPE fails to function normally.

When the program prompts you to enter a value during installation, note that the values in square brackets are default values. If you press **Enter** without entering fresh values, the program takes the default value.

During installation, the program generates a definitions file bpr_definitions.sh, which is copied to the target home directory (*BPR_HOME*). The definition file stores the values for the:

- Installation location (*BPR_HOME*)
- Data location (*BPR_DATA*)
- Database transactions log location (*BPR_DBLOG*)
- Cisco BAC class path (*BPR_CP*)
- All installed components (*COMPONENTS*)

The bpr_definitions.sh file is updated whenever new components are installed or added.

Note Verify the existence of a text file called log.txt, which indicates that errors occurred during the installation process. This file is located under the *BPR_HOME* directory.

Installing Components in Interactive Mode

This section explains the procedures that you follow to install one or more Cisco BAC components interactively, from the command line.

Note Before you begin any of these procedures, you must complete the initial procedure described in Installation Checklist for Solaris, page 2-4.

You can install the Cisco BAC components from the CLI, as described in:

- Installing the RDU, page 3-2
- Installing the DPE, page 3-4
- Installing the Cisco Network Registrar Extension Point, page 3-6
- Installing the Cisco Access Registrar Extension Point, page 3-10
- Installing the STUN Server, page 3-12

If you exit the Cisco BAC installation after the database is installed, you must uninstall the *BPR_HOME* and the *BPR_DATA* directories before you install Cisco BAC again. (For information on uninstallation, see Uninstalling Cisco BAC, page 3-33.) Also, if you stop the installation mid-way, the log file is not generated.

If you rerun the installation without uninstalling the specified directories, you cannot change the location of the *BPR_DATA* or the *BPR_DBLOG* directories.

Installing the RDU

This section describes how to install the RDU. You must install the RDU on a Solaris 10 server that meets the requirements described in the section, Operating System Requirements, page 2-1. You should install the RDU on a high-end system that is the most reliable server in your network. We recommend that you configure the RDU server to use a static IP address.

Note Before installation, remove /rdu/db from /var/CSCObac/ directory.

To install RDU from the CLI:

Step 1 Log into the intended Cisco BAC host as root.

Step 2 Enter the following command to start the installation program in interactive mode:

```
# install-path/BAC_3.7_SolarisK9/install_bac.sh
```

where *install-path* specifies the complete path to the directory in which the BAC_3.7_SolarisK9 directory has been created.

The installation program verifies that you have installed the required patches to the Solaris operating system. When the verification ends, the Welcome information appears.

Step 3 Press **Enter** to continue.

The installation program prompts you to select one or more components.

Step 4 Enter **y** and press **Enter** at the RDU prompt.

To skip installing a DPE, CNR extension points, CAR extension points and STUN, enter **n** and press **Enter**. You can choose to install these components later.

Step 5 Enter **y** and press **Enter** to continue.

The Home Directory Destination prompt appears.

Step 6 Accept the default directory, /opt/CSCObac, by pressing **Enter**; or enter a different directory.

Step 7 Enter **y** and press **Enter** to confirm the directory.

The data directory destination prompt appears.

Step 8 Accept the default directory, /var/CSCObac, by pressing **Enter**; or enter another directory.

Step 9 Enter **y** and press **Enter** to confirm the directory.

Step 10 Enter the database transaction logs destination.

Step 11 Accept the default directory, /var/CSCOba*c*, by pressing **Enter**; or enter another directory.

Step 12 Enter **y** and press **Enter** to confirm the directory.

Step 13 Enter the listening port for the RDU.

Step 14 Accept the default value, 49187, by pressing **Enter**; or enter another port number.

Caution If you change the default listening port value, ensure that the new value does not conflict with any existing port assignments. Also, ensure that you configure all DPEs with the correct RDU port number. See the *Cisco Broadband Access Center DPE CLI Reference, Release 3.7,* for details on configuring the DPE.

The installation program obtains the IP address of the RDU automatically. You need not enter this value manually.

Step 15 Enter **y** and press **Enter** to confirm the listening port number.

Step 16 Enter the shared secret password that you want to use for authentication between the Cisco BAC servers; the default password is **secret**.

Note You must use the same shared secret password for all RDUs and DPEs in your network.

Step 17 Press **Enter** to continue the installation.

The program displays the installation parameters that you selected.

Step 18 Enter **y** and press **Enter** to confirm the parameters, and install the RDU component.

Step 19 Enter **y** and press **Enter**.

The program prompts you to continue with the installation.

Step 20 Enter **y** and press **Enter**.

After a successful installation, the following message appears:

```
Installation of <CSCObac> was successful.
```

Step 21 Launch the Cisco BAC administrator user interface to verify whether the RDU is running.

a. Enter the administrator's location by using this syntax:

http://*machine_name*/

where *machine_name* identifies the computer on which the RDU is running.

Note To access the administrator user interface using HTTP over SSL/TLS, enter **https://***machine_name*/

The main Login page appears.

b. Change the Cisco BAC administrator password. To do this:

Enter the default username (**bacadmin**) and password (**changeme**), and click **Login**.

The Change Password screen appears and prompts you to change the default password.

c. Enter a new password, and click **Login**.

Optionally, configure the syslog file for alerts on the RDU server.

Note You can set up the syslog file on any Cisco BAC component server.

Installing the DPE

This section describes how to install the DPE.

Note Before proceeding to install the DPE, ensure that the RDU resides on your system. For details on installing the RDU, see the Installing the RDU, page 3-2. RDU can also be installed on a different machine.

To install the DPE from the CLI:

Step 1 Log into the intended Cisco BAC host as root.

Step 2 Enter the following command to start the installation program in interactive mode:

install-path/**BAC_3.7_SolarisK9/install_bac.sh**

where *install-path* specifies the complete path to the directory in which the BAC_3.7_SolarisK9 directory has been created.

The installation program verifies that you have installed the required patches to the Solaris operating system. When the verification ends, the Welcome information appears.

Step 3 Press **Enter** to continue.

The installation program prompts you to select one or more components.

Step 4 Enter **y** and press **Enter** at the DPE prompt.

To skip installing a RDU, CNR extension points, CAR extension points and STUN, enter **n** and press **Enter**. You can choose to install these components later.

Step 5 Confirm the components that you want to install;

Step 6 Enter **y** and press **Enter**.

The program prompts you to confirm the components that you want to install.

Step 7 Enter **y** and press **Enter** to continue.

The home directory Destination prompt appears.

Step 8 Accept the default directory, /opt/CSCObac, by pressing **Enter**; or enter a different directory.

Step 9 Enter **y** and press **Enter** to confirm the directory.

The data directory destination prompt appears.

Step 10 Accept the default directory, /var/CSCObac, by pressing **Enter**; or enter another directory.

Step 11 Confirm the directory, press **y** and **Enter**.

The program prompts you to enter the RDU information required to install DPE.

Step 12 Enter the IP address (or hostname) and the listening port of the host on which you have installed the RDU.

Step 13 Accept the default information, by pressing **Enter**; or enter alternative information.

Step 14 Enter the IP address (or hostname) and the listening port of the host on which you have installed the RDU.

Step 15 Accept the default information, by pressing **Enter**; or enter alternative information.

Step 16 Enter the shared secret password that you want to use for authentication between the Cisco BAC servers; the default password is **secret**.

Step 17 Press **Enter** to continue.

Note You must use the same shared secret password for all RDUs and DPEs in your network.

The program prompts you to continue with the installation.

Step 18 Enter **y** and press **Enter**.

After a successful installation, the following message appears:

```
Installation of <CSCObac> was successful.
```

Step 19 After you install the DPE, ensure that you change the DPE login password and the enable password from the CLI. The default DPE login password and enable password is *changeme*.

- To change the login password, access the CLI in the enabled mode, and enter:

  ```
  dpe# password password
  ```

  where *password* identifies the new DPE password.

- To change the DPE enable password, enter the following command:

  ```
  dpe# enable password password
  ```

  where *password* identifies the local configured password currently in effect or, optionally, provides a new password. If this parameter is omitted, you are prompted for the password.

  For more information, see the *Cisco Broadband Access Center DPE CLI Reference, Release 3.7*.

Step 20 Configure the DPE from the CLI. For more information, refer to the *Cisco Broadband Access Center DPE CLI Reference, Release 3.7*.

Optionally, you can configure the syslog file for alerts on the DPE server.

Note You can set up the syslog file on any Cisco BAC component server.

Installing the Cisco Network Registrar Extension Point

Install Cisco BAC extensions on all Cisco Network Registrar servers in your Cisco BAC environment. If you are deploying Cisco BAC in a fail-over environment, you must also install the extensions on the failover servers. After you install the extensions, you must configure them.

Cisco Network Registrar Extension Point Prerequisite

As a prerequisite to install CNR_EP, you must have installed Cisco Network Registrar. For Cisco Network Registrar installation information, see Installation Guide for Cisco Network Registrar, Release 7.2. This section explains how to install, configure, and validate these extensions.

You can download the Cisco BAC softwares from the below location:

http://www.cisco.com/cisco/software/navigator.html?mdfid=268439531

Note Cisco BAC 3.7 has been tested with Cisco Network Registrar 7.2. Cisco Network Registrar 7.2 has the fix for co-resident Cisco Network Registrar and Cisco Access Registrar.

We recommend that you configure the Cisco Network Registrar server to use a static IP address.

To install the Cisco Network Registrar Extension Point from the CLI:

Step 1 Log into the intended Cisco BAC host as root.

Step 2 Enter the following command to start the installation program in interactive mode:

install-path/**BAC_3.7_SolarisK9/install_bac.sh**

where *install-path* specifies the complete path to the directory in which the BAC_3.7_SolarisK9 directory has been created.

The installation program verifies that you have installed the required patches to the Solaris operating system. When the verification ends, the Welcome information appears.

Step 3 Press **Enter** to continue.

The installation program prompts you to select one or more components.

Step 4 Enter **y** and press **Enter** at the CNR prompt.

To skip installing a RDU, DPE, CAR extension points and STUN, enter **n** and press **Enter**. You can choose to install these components later.

Step 5 Enter **y** and press **Enter**.

The program prompts you to confirm the components that you want to install.

Step 6 Enter **y** and press **Enter** to continue.

The home directory destination prompt appears.

Step 7 Accept the default directory, /opt/CSCObac, by pressing **Enter**; or enter a different directory.

Step 8 Enter **y** and press **Enter** to confirm the directory.

The data directory destination prompt appears.

Step 9 Accept the default directory, /var/CSCObac, by pressing **Enter**; or enter another directory.

Step 10 Enter **y** and press **Enter** to confirm the directory.

The program prompts you to enter the required information on the RDU, to install the extensions.

Step 11 Enter the IP address (or hostname) and the listening port of the host on which you have installed the RDU.

Step 12 Press **Enter** to accept the default information; or enter alternative information.

You are prompted to enter the name of the extension point provisioning group. The program prompts you to confirm the installation.

Step 13 Press **y** and **Enter** to confirm and continue.

Step 14 Enter the shared secret password that you want to use for authentication between the Cisco BAC servers; the default password is **secret**.

The program prompts you to continue with the installation.

Step 15 Enter **y** and press **Enter**.

After a successful installation, the following message appears:

```
Installation of <CSCObac> was successful.
```

Enabling Cisco Network Registrar Extension Point

To enable the Cisco Network Registrar Extension Point.

Step 1 After installing Cisco Network Registrar Extension Point, run this command to enable the Cisco Network Registrar extension points:

NR_HOME/local/usrbin/nrcmd -s < BPR_HOME/cnr_ep/bin/bpr_cnr_enable_extpts.nrcmd

In case the default setting are changed, use the below options instead of -s.

The options are:

```
-C <cluster>   the Cluster to log in to
-N <name>      the Name to log in as
-P <password> the Password to log in with
```

Step 2 Restart the Cisco Network Registrar server using this command:

```
/etc/init.d/nwreglocal stop
/etc/init.d/nwreglocal start
```

Note Before you can use the Cisco Network Registrar server, you must configure scopes required for DHCP server.

Configuring Extensions

After you install the Cisco BAC extensions on the Cisco Network Registrar server, you must configure the extensions. The procedure described in this section assumes that:

- The Cisco BAC component is installed in /opt/CSCObac.
- Cisco Network Registrar is installed in /opt/nwreg2.
- The Cisco Network Registrar username is **admin** and the password is **changeme**.

To configure extensions:

Step 1 Log into the Cisco Network Registrar server, with *root* access.

Step 2 At the command line, enter:

```
# NR_HOME/local/usrbin/nrcmd -N admin -P changeme -b <
BAC_HOME/cnr_ep/bin/bpr_cnr_enable_extpts.nrcmd
```

- To reload the Cisco Network Registrar server, enter:

```
# /etc/init.d/nwreglocal stop
# /etc/init.d/nwreglocal start
```

- To reload the DHCP server alone, enter:

```
# NR_HOME/local/usrbin/nrcmd -N admin -P changeme "dhcp reload"
```

Note Before you can use the Cisco Network Registrar server, you must configure client classes, scope-selection tags, policies, and scopes.

Validating Extensions

To validate the extensions installed on the Cisco Network Registrar server, from the Cisco Network Registrar Command Line Tool (**nrcmd**), run:

Depending on whether you installed a local or regional cluster, the **nrcmd** tool is located in:

- Local—/opt/nwreg2/local/usrbin
- Regional—/opt/nwreg2/regional/usrbin

```
nrcmd> extension list
100 Ok
dexdropras:
    entry = dexdropras
    file = libdexextension.so
    init-args =
    init-entry =
    lang = Dex
    name = dexdropras
preClientLookup:
    entry = bprClientLookup
    file = libbprextensions.so
    init-args = BPR_HOME=/opt/CSCObac,BPR_DATA=/var/CSCObac
    init-entry = bprInit
    lang = Dex
    name = preClientLookup
nrcmd>
```

Note The *BPR_HOME* and *BPR_DATA* values may be different in your installation.

Also, in the **nrcmd** program, run:

```
nrcmd> dhcp listextensions
100 Ok
post-packet-decode: dexdropras
pre-packet-encode:
pre-client-lookup: preClientLookup
post-client-lookup:
post-send-packet:
pre-dns-add-forward:
check-lease-acceptable:
post-class-lookup:
lease-state-change:
generate-lease:
environment-destructor:
pre-packet-decode:
post-packet-encode:
nrcmd>
```

Installing the Cisco Access Registrar Extension Point

Install Cisco BAC extensions on all Cisco Access Registrar servers in your Cisco BAC environment. If you are deploying Cisco BAC in a failover environment, you also must install the extensions on the fail-over servers.

After you install extensions, you must configure them. This section explains how to install, configure, and validate these extensions.

Cisco Access Registrar Extension Point Prerequisite

As a prerequisite to install Cisco Access Registrar Extension Point, you should have installed Cisco Access Registrar 5.0.0.3 or later. For CAR Extension Point installation information, see *Installation Guide for Cisco Access Registrar, release 5.0*.

The default value for tomcat server port (8005) and web UI port (8080) are the same for both Cisco Network Registrar and Cisco Access Registrar servers. Hence, you need to change either the tomcat server port or web UI port before installing Cisco Access Registrar Extension Point.

The tomcat server port of the Cisco Access Registrar server and web UI port can be changed in /opt/CSCOar/apache-tomcat-5.5.27/conf/server.xml.

The tomcat server port of the Cisco Network Registrar server and web UI port can be changed in /opt/nwreg2/local/tomcat/conf/server.xml.

You may choose to install Cisco Network Registrar or Cisco Access Registrar, first. However, we recommend that you install Cisco Access Registrar before Cisco Network Registrar. Cisco Network Registrar allows you to change the Web UI (tomcat) port as part of the installation.

Cisco Access Registrar 5.0.0.6 requires either JRE 1.5.x or 1.6.x, but CAR_EP needs JRE 1.6.x, so use JRE 1.6.x for Cisco Access Registrar 5.0.0.6.

We recommend that you configure the Cisco Access Registrar server to use a static IP address.

To install the Cisco Access Registrar Extension Point from the CLI:

Step 1 Log into the intended Cisco BAC host as root.

Step 2 Enter the following command to start the installation program in interactive mode:

install-path/**BAC_3.7_SolarisK9/install_bac.sh**

where *install-path* specifies the complete path to the directory in which the BAC_3.7_SolarisK9 directory has been created.

The installation program verifies that you have installed the required patches to the Solaris operating system. When the verification ends, the Welcome information appears.

Step 3 Press **Enter** to continue.

The installation program prompts you to select one or more components.

Step 4 Enter **y** and press **Enter** at the Cisco Access Registrar Extention Point prompt.

To skip installing the RDU, DPE, CNR extension points and STUN, enter **n** and press **Enter**. You can choose to install these components later.

Step 5 Enter **y** and press **Enter**.

The program prompts you to confirm the components that you want to install.

Step 6 Enter **y** and press **Enter** to continue.

The Home Directory Destination prompt appears.

Step 7 Accept the default directory, /opt/CSCObac, by pressing **Enter**; or enter a different directory.

Step 8 Enter **y** and press **Enter** to confirm the directory.

The data directory destination prompt appears.

Step 9 Accept the default directory, /var/CSCObac, by pressing **Enter**; or enter another directory.

Step 10 Enter **y** and press **Enter** to confirm the directory.

The program prompts you to enter information on the RDU required to install the extensions.

Step 11 Enter the IP address (or hostname) and the listening port of the host on which you have installed the RDU.

Step 12 Accept the default information, by pressing **Enter**; or enter alternative information.

The program prompts you to confirm the installation.

Step 13 Enter **y** and press **Enter** to confirm and continue.

The program prompts you to continue with the installation.

Step 14 Enter **y** and press **Enter**.

After a successful installation, the following message appears:

```
Installation of <CSCObac> was successful.
```

Setting up Cisco Access Registrar Extension Points

To setup the Cisco Access Registrar Extension Point, after installing Cisco Access Registrar Extension Point, run the below script to create and setup extension points in Cisco Access Registrar:

```
BPR_HOME/car_ep/bin/configARExtension.sh
```

The DPE Auth Service hosts address and port should be manually provisioned. By default, the host address is *localhost* and auth service port is 7551. To change the default properties run the following script with appropriate options:

```
BPR_HOME/car_ep/bin/changeARProperties.sh
```

- To configure the DPE Auth service interface run the above script with the following option:

  ```
  sh changeARProperties.sh -host address
  ```

- To configure the DPE Auth service port run the script with the following option:

  ```
  sh changeARProperties.sh -port port_number
  ```

- To display the configured properties for Cisco Access Registrar Extension Point, run the script with the following option:

  ```
  sh changeARProperties.sh -d
  ```

- To list the options of the script, run the following script:

  sh changeARProperties.sh -help

  Cisco BAC displays the following list of options:

```
-C <cluster>   the Cluster to log in to
-N <name>      the Name to log in as
-P <password> the Password to log in with
```

Installing the STUN Server

Install the STUN on a server that meets the requirements described in Cisco BAC Components, page 1-1.

To install the STUN server:

Step 1 Log into the intended Cisco BAC host as root.

Step 2 Enter the following command to start the installation program in interactive mode:

install-path/**BAC_3.7_SolarisK9/install_bac.sh**

where *install-path* specifies the complete path to the directory in which the BAC_3.7_SolarisK9 directory has been created.

The installation program verifies that you have installed the required patches to the Solaris operating system. When the verification ends, the welcome information appears.

Step 3 Press **Enter** to continue.

The program prompts you to choose the component that you want to install.

Step 4 Enter **y** and press **Enter** at the STUN server prompt.

To skip installing the RDU, DPE, Cisco Network Registrar extension points and the Cisco Access Registrar extension points, enter **n** and press **Enter**. You can choose to install these components later.

The home directory prompt appears.

Step 5 Accept the default directory, /opt/CSCObac, by pressing **Enter**; or enter another directory.

Step 6 Confirm the directory location. To do this, enter **y** and press **Enter**.

The data directory prompt appears.

Step 7 Accept the default directory, /var/CSCObac, by pressing **Enter**; or enter another directory.

Step 8 Confirm the directory location.To do this, enter **y** and press **Enter**.

The program prompts you to enter information on the RDU required to install the extensions.

Step 9 Enter the IP address (or hostname) and the listening port of the host on which you have installed the RDU.

Step 10 Accept the default information, by pressing **Enter**; or enter alternative information.

Step 11 Confirm the information. To do this, enter **y** and press **Enter**.

The program prompts you to enter the STUN HTTP listening port.

Step 12 Accept the default information, by pressing **Enter**; or enter alternative information.

The program prompts you to enter the STUN UDP listening port.

Step 13 Accept the default information, by pressing **Enter**; or enter alternative information.

The program prompts you to enter the STUN HTTP user name.

Step 14 Accept the default information, by pressing **Enter**; or enter alternative information.

The program prompts you to enter the STUN HTTP password.

Step 15 Accept the default information, by pressing **Enter**; or enter alternative information.

The program prompts you to enter the password to be used for UDP CR authentication.

Step 16 Accept the default information, by pressing **Enter**; or enter alternative information

The program prompts you to enter the shared secret password. Enter the shared secret password that you want to use for authentication between the Cisco BAC servers.

Step 17 Re-enter the password for confirmation, and press **Enter**.

The installation proceeds, and displays the following message after successful installation:

```
Installation of <CSCObac> was successful.
```

Installing Components in Noninteractive Mode

This section explains the procedures that you follow to install one or more Cisco BAC components from the command line in noninteractive mode.

In order to install Cisco BAC in noninteractive mode, you must first generate a response file, in which you store values for installing a component. You can then use the response file as input while installing that component.

For subsequent installations of the same component, you only need to use a single command, which removes all installation prompts and installs the component using the values contained in the response file.

To install Cisco BAC in noninteractive mode, you must perform the following steps:

Step 1 Generate a response file, using:

```
# pkgask -r response -d install-path /BAC_3.7_SolarisK9/CSCObac.pkg CSCObac
```

where *install-path* specifies the complete path to the directory in which the *BAC_3.7_SolarisK9* directory has been created.

Running this command does not install Cisco BAC on your system; it only generates the response file in which you store values for installation.

Note that there can only be one response file. As a result, you can use the response file only to install the component for which you generate the response file. If you want to install another component, you must generate a response file for that component and install that component, using the response file generated for it.

For example, if you generate a response file to install the DPE, and, subsequently, you want to install Cisco Network Registrar extensions, you must generate a response file separately to install Cisco Network Registrar extensions. You cannot use the response file that you generated to install the DPE, to install Cisco Network Registrar extensions.

Step 2 After you generate the response file, start the installation program in noninteractive mode, using:

```
# install_bac.sh -r responsefile
```

Note Before you begin any of the procedures described in this section, complete the initial installation procedure described in Installation Checklist for Solaris, page 2-4.

The following sections provide instructions on installing components in noninteractive mode:

- Installing the RDU in Noninteractive Mode, page 3-14
- Installing the DPE in Noninteractive Mode, page 3-16
- Installing the Cisco Network Registrar Extensions in Noninteractive Mode, page 3-17
- Installing the Cisco Access Registrar Extensions in Noninteractive Mode, page 3-19
- Installing the STUN Server in Noninteractive Mode, page 3-20

Installing the RDU in Noninteractive Mode

Install the RDU on a server running Solaris 10 that meets the requirements described in Operating System Requirements, page 2-1. You should install the RDU on a high-end system that is the most reliable server in your network.

Note We recommend that you configure the RDU server to use a static IP address.

To install the RDU, complete the initial installation described in Installation Checklist for Solaris, page 2-4.

Generating the Response File for the RDU

To generate a response file for RDU installation:

Step 1 Enter:

```
# pkgask -r response -d install-path /BAC_3.7_SolarisK9/CSCObac.pkg CSCObac
```

where *install-path* specifies the complete path to the directory in which the *BAC_3.7_SolarisK9* directory has been created.

The response file is created in the directory in which you run the **pkgask -r** command.

If you want the response file to be generated in a specific location, enter:**# pkgask -r** *response-file-path* **-d CSCObac.pkg**

where *response-file-path* specifies the path to the directory in which you want the response file to be generated; for example, */tmp/response*. You can also give the response file any name; for example, *outputFile*.

The installation program verifies that you have installed the required patches to the Solaris operating system. When the verification ends, the Welcome information appears.

Step 2 Press **Enter** to continue.

The installation program prompts you to select one or more components.

Step 3 Enter **y** and press **Enter** at the RDU prompt.

To skip installing a DPE, Cisco Network Registrar extension points, Cisco Access Registrar extension points and STUN server, enter **n** and press **Enter**. You can choose to install these components later.

The program prompts you to confirm the components that you want to install.

Step 4 Enter **y** and press **Enter** to continue.

Step 5 Accept the default directory, /opt/CSCObac, by pressing **Enter**; or enter a different directory.

A confirmation prompt appears.

Step 6 Enter **y** and press **Enter** to confirm the home directory location

The program prompts you to enter the data directory location.

Step 7 Accept the default directory, */var/CSCObac*, by pressing **Enter**; or enter a different directory.

Step 8 Enter **y** and press **Enter** to confirm the data directory location,

The database log directory prompt appears.

Step 9 Accept the default directory, /var/CSCObac, by pressing **Enter**; or enter another directory.

Step 10 Enter **y** and press **Enter** to continue to confirm the directory.

The program prompts you to enter the information related to the RDU listening port.

The listening port is the port number that the RDU uses to communicate with other Cisco BAC components, such as DPEs and Cisco Network Registrar extension points.

Step 11 Accept the default port number, 49187, by pressing **Enter**; or enter another port number.

Caution If you change the default listening port value, ensure that the new value does not conflict with any existing port assignments. Also, ensure that you configure all DPEs with the correct RDU port number. For details on configuring the DPE, see the *Cisco Broadband Access Center DPE CLI Reference, 3.7*.

Step 12 Confirm the listening port number; enter **y** and press **Enter** to continue.

The program prompts you to enter the shared secret password.

Step 13 Enter the shared secret password that you want to use for authentication among Cisco BAC servers, and confirm the password.

Note You must use the same shared secret password for the RDU, all DPEs, and Cisco Network Registrar extension points in your network.

Step 14 Press **Enter** to continue.

The program displays the parameters you have selected to install the RDU.

Step 15 Enter **y** and press **Enter** to confirm the installation parameters.

A message appears indicating that a response file has been created.

Step 16 After you generate the response file, start the installation program in noninteractive mode, using:

```
# install_bac.sh -r responsefile
```

Once you run the above command, the program installs the RDU. After successful installation, a message appears.

Installing the DPE in Noninteractive Mode

Install the DPE on a server running Solaris 10 that meets the requirements described in Operating System Requirements, page 2-1.

We recommend that you configure the DPE server to use a static IP address.

During DPE installation, if the program detects a TFTP server or a ToD server running on the same server as the DPE, the installation displays an error message and exits. To terminate the TFTP or ToD server, perform the steps that the error message lists.

To install the DPE, complete the initial steps described in Installation Checklist for Solaris, page 2-4.

Generating the Response File for the DPE

To generate a response file for DPE installation:

Step 1 Enter:

```
# pkgask -r response -d install-path /BAC_37_SolarisK9/CSCObac.pkg CSCObac
```

where *install-path* specifies the complete path to the directory in which the BAC_37_SolarisK9 directory has been created.

The response file is created in the directory in which you run the **pkgask -r** command. If you want the response file to be generated in a specific location, enter:

```
# pkgask -r response-file-path -d CSCObac.pkg
```

where *response-file-path* specifies the path to the directory in which you want the response file to be generated; for example, */tmp/response*. You can also give the response file any name; for example, *outputFile*.

The installation program verifies that you have installed the required patches to the Solaris operating system. When the verification ends, the Welcome information appears.

Step 2 Press **Enter** to continue.

The program prompts you to add user name and user group name.

Step 3 Press **Enter** to continue.

The installation program prompts you to select one or more components.

Step 4 Enter **y** and press **Enter** at the DPE prompt.

To skip installing the RDU, Cisco Network Registrar extension points, Cisco Access Registrar extension points and the STUN server, enter **n** and press **Enter**.

The program prompts you to confirm the components that you want to install.

Step 5 Enter **y** and press **Enter** to continue.

The home directory prompt appears.

Step 6 Accept the default directory, /opt/CSCObac, by pressing **Enter**; or enter another directory.

Step 7 Confirm the directory location; enter **y** and press **Enter**.

The data directory prompt appears.

Step 8 Accept the default directory, /var/CSCObac, by pressing **Enter**; or enter another directory.

Step 9 Confirm the directory location; enter **y** and press **Enter**.

The program prompts you to enter the information related to the RDU, specifically the IP address and the listening port.

You must enter a value for the IP address and listening port. The listening port is the port number that the RDU uses to communicate with other Cisco BAC components, such as DPEs and Cisco Network Registrar extension points.

Step 10 Accept the default port number, 49187, by pressing **Enter**; or enter another port number.

Caution If you change the default listening port value, ensure that the new value does not conflict with any existing port assignments. Also, ensure that you configure all DPEs with the correct RDU port number. For details on configuring the DPE, see the *Cisco Broadband Access Center DPE CLI Reference, 3.7*.

Step 11 Confirm the listening port number; enter **y** and press **Enter** to continue.

The program prompts you to enter the shared secret password.

Step 12 Enter the shared secret password that you want to use for authentication between the Cisco BAC servers. You must use the same shared secret password for the RDU, all DPEs, Cisco Network Registrar extension points and in your network.

Step 13 Reenter the password for confirmation, and press **Enter**.

A message appears indicating that a response file has been created.

Step 14 After you generate the response file, start the installation program in noninteractive mode, using:

```
# install_bac.sh -r responsefile
```

After you run the above command, the program installs the DPE. After successful installation, a message appears.

Installing the Cisco Network Registrar Extensions in Noninteractive Mode

Install Cisco BAC extensions on all Cisco Network Registrar servers in your Cisco BAC environment. If you are deploying Cisco BAC in a failover environment, you also must install the extensions on the failover servers.

After you install extensions, you must configure them. This section explains how to install, configure, and validate these extensions.

Note We recommend that you configure the Cisco Network Registrar server to use a static IP address.

Before you install Cisco Network Registrar extensions, complete the initial installation described in Installation Checklist for Solaris, page 2-4. Also, ensure that Cisco Network Registrar is running.

Generating the Response File for Cisco Network Registrar Extensions

To generate a response file to install Cisco Network Registrar extensions:

Step 1 Enter:

```
# pkgask -r response -d install-path/BAC_37_SolarisK9/CSCObac.pkg CSCObac
```

where *install-path* specifies the complete path to the directory in which the BAC_37_SolarisK9 directory has been created.

The response file is created in the directory in which you run the **pkgask -r** command. If you want the response file to be generated in a specific location, enter:

```
# pkgask -r response-file-path -d CSCObac.pkg
```

where *response-file-path* specifies the path to the directory in which you want the response file to be generated; for example, */tmp/response*. You can also give the response file any name; for example, *outputFile*.

The installation program verifies that you have installed the required patches to the Solaris operating system. When the verification ends, the Welcome information appears.

Step 2 Press **Enter** to continue.

The installation program prompts you to select one or more components.

Step 3 Enter **y** and press **Enter** at the Cisco Network Registrar Extension Points prompt.

To skip installing the RDU, DPE, Cisco Access Registrar extension points and the STUN server, enter **n** and press **Enter**.

Note The installation program validates your Cisco Network Registrar installation. You must install Cisco Network Registrar 7.2 on your server. If the required version is not installed, the installation process terminates. You must upgrade to Cisco Network Registrar 7.2, before proceeding.

The program prompts you to confirm the components that you want to install.

Step 4 Enter **y** and press **Enter** to continue.

The home directory prompt appears.

Step 5 Accept the default directory, /opt/CSCObac, by pressing **Enter**; or enter another directory.

The program then prompts you to confirm the directory.

Step 6 Press **y** and **Enter** to continue.

The data directory prompt appears.

Step 7 Accept the default directory, /var/CSCObac, by pressing **Enter**; or enter another directory.

Note The installation program, by default, installs the data directory (*BPR_DATA*) on a different directory than the home directory (*BPR_HOME*). We recommend that the data directory be on a different physical disk than the home directory; for example, */var/disk0/CSCObac*.

Step 8 Enter **y** and press **Enter** to confirm the directory,

The program prompts you to enter information on the RDU required to install the extensions.

Step 9 Enter the IP address (or hostname) and the listening port of the host on which you have installed the RDU.

Step 10 Accept the default information, by pressing **Enter**; or enter alternative information.

You are prompted to enter the name of the extension point provisioning group.

Step 11 Enter the name of the Cisco Network Registrar extension point group.

Step 12 Enter **y** and press **Enter**.

Step 13 Enter the shared secret password that you want to use for authentication among Cisco BAC servers. You must use the same shared secret password for all Cisco BAC servers on your network.

Step 14 Press **Enter** to continue,

A message appears indicating that a response file has been created.

Step 15 After you generate the response file, start the installation program in noninteractive mode, using:

```
# install_bac.sh -r responsefile
```

After you run the above command, the program installs the DPE. After successful installation, a message appears.

After you install the extensions, you must configure and validate them. For details, see Configuring Extensions, page 3-8, and Validating Extensions, page 3-9.

Installing the Cisco Access Registrar Extensions in Noninteractive Mode

Install the Cisco Access Registrar Extensions on a server running Solaris 10 that meets the requirements described in Operating System Requirements, page 2-1.

To install the Cisco Access Registrar Extensions, complete the initial steps described in Installation Checklist for Solaris, page 2-4.

Generating the Response File for the Cisco Access Registrar Extensions

To generate a response file for Cisco Access Registrar Extensions installation:

Step 1 Enter:

```
# pkgask -r response -d install-path /BAC_37_SolarisK9/CSCObac.pkg CSCObac
```

where *install-path* specifies the complete path to the directory in which the BAC_37_SolarisK9 directory has been created.

The response file is created in the directory in which you run the **pkgask -r** command. If you want the response file to be generated in a specific location, enter:

```
# pkgask -r response-file-path -d CSCObac.pkg
```

where *response-file-path* specifies the path to the directory in which you want the response file to be generated; for example, */tmp/response*. You can also give the response file any name; for example, *outputFile*.

The installation program verifies that you have installed the required patches to the Solaris operating system. When the verification ends, the Welcome information appears.

Step 2 Press **Enter** to continue.

The program prompts you to add user name and user group name.

Step 3 Press **Enter** to continue.

The installation program prompts you to select one or more components.

Step 4 Enter **y** and press **Enter** at the CAR prompt.

To skip installing the RDU, DPE, Cisco Network Registrar extension points, and the STUN server, enter **n** and press **Enter**.

The program prompts you to confirm the components that you want to install.

Step 5 Enter **y** and press **Enter** to continue.

The home directory prompt appears.

Step 6 Accept the default directory, /opt/CSCObac, by pressing **Enter**; or enter another directory.

Step 7 Confirm the directory location; enter **y** and press **Enter**.

The data directory prompt appears.

Step 8 Accept the default directory, /var/CSCObac, by pressing **Enter**; or enter another directory.

Step 9 Confirm the directory location; enter **y** and press **Enter**.

The program prompts you to enter the information related to the RDU, specifically the IP address and the listening port.

You must enter a value for the IP address and listening port. The listening port is the port number that the RDU uses to communicate with other Cisco BAC components, such as DPEs and Cisco Network Registrar extension points.

Step 10 Accept the default port number, 49187, by pressing **Enter**; or enter another port number.

Caution If you change the default listening port value, ensure that the new value does not conflict with any existing port assignments. Also, ensure that you configure all DPEs with the correct RDU port number. For details on configuring the DPE, see the *Cisco Broadband Access Center DPE CLI Reference, 3.7*.

Step 11 Confirm the listening port number; enter **y** and press **Enter** to continue.

Step 12 After you generate the response file, start the installation program in noninteractive mode, using:

```
# install_bac.sh -r responsefile
```

After you run the above command, the program installs the Cisco Access Registrar. After successful installation, a message appears.

Installing the STUN Server in Noninteractive Mode

Install the STUN server on a server running Solaris 10 that meets the requirements described in Operating System Requirements, page 2-1.

To install the STUN server, complete the initial steps described in Installation Checklist for Solaris, page 2-4.

Generating the Response File for the STUN Server

To generate a response file for STUN server installation:

Step 1 Enter:

```
# pkgask -r response -d install-path/BAC_37_SolarisK9/CSCObac.pkg CSCObac
```

where *install-path* specifies the complete path to the directory in which the BAC_37_SolarisK9 directory has been created.

The response file is created in the directory in which you run the **pkgask -r** command. If you want the response file to be generated in a specific location, enter:

```
# pkgask -r response-file-path -d CSCObac.pkg
```

where *response-file-path* specifies the path to the directory in which you want the response file to be generated; for example, */tmp/response*. You can also give the response file any name; for example, *outputFile*.

The installation program verifies that you have installed the required patches to the Solaris operating system. When the verification ends, the Welcome information appears.

Step 2 Press **Enter** to continue.

The program prompts you to add the user name and user group name.

Step 3 Press **Enter** to continue.

The installation program prompts you to select one or more components.

Step 4 Enter **y** and press **Enter** at the STUN prompt.

To skip installing the RDU, DPE, Cisco Network Registrar extension points, and the Cisco Access Registrar extension points, enter **n** and press **Enter**.

The program prompts you to confirm the components that you want to install.

Step 5 Enter **y** and press **Enter** to continue.

The home directory prompt appears.

Step 6 Accept the default directory, /opt/CSCObac, by pressing **Enter**; or enter another directory.

Step 7 Confirm the directory location; enter **y** and press **Enter**.

The data directory prompt appears.

Step 8 Accept the default directory, /var/CSCObac, by pressing **Enter**; or enter another directory.

Step 9 Confirm the directory location; enter **y** and press **Enter**.

The program prompts you to enter the STUN HTTP listening port.

Step 10 Accept the default information, by pressing **Enter**; or enter alternative information.

The program prompts you to enter the STUN UDP listening port.

Step 11 Accept the default information, by pressing **Enter**; or enter alternative information.

The program prompts you to enter the STUN HTTP user name.

Step 12 Accept the default information, by pressing **Enter**; or enter alternative information.

The program prompts you to enter the STUN HTTP password.

Step 13 Accept the default information, by pressing **Enter**; or enter alternative information.A message appears indicating that a response file has been created.

Step 14 After you generate the response file, start the installation program in noninteractive mode, using:

```
# install_bac.sh -r responsefile
```

After you run the above command, the program installs the STUN server. After successful installation, a message appears.

Reinstalling Broadband Access Center

This section describes the procedures to reinstall Cisco Broadband Access Center (Cisco BAC). Reinstallation in Cisco BAC is enabled only for the purpose of restoring an installation that is corrupted.

This release does not support reinstalling the Regional Distribution Unit (RDU), the Device Provisioning Engine (DPE) and Cisco Network Registrar that are already installed on your system. If you need to reinstall them, first uninstall the RDU and DPE, and then reinstall them.

Caution You cannot retrieve a corrupted database after a reinstallation. You must have a backup of the database before it was corrupted.

Reinstalling from the CLI

To reinstall Cisco BAC from the CLI:

Step 1 Back up your database by running the *BPR_HOME*/**rdu/bin/backupDb.sh** command, where *BPR_HOME* is the home directory. The default directory is /opt/CSCObac.

To use this command, you must provide the target directory in which to place the backup files. This directory should be on a disk or partition that has available disk space equivalent to 120% of the current database file size.

For detailed information, see the *Cisco Broadband Access Center Administrator's Guide, Release 3.7*.

Caution You must back up your database before proceeding with the reinstallation procedure. If you do not save your database before uninstalling Cisco BAC (the next step in the procedure), you will lose the information in the database because the BPR_HOME directory is deleted during an uninstallation.

Step 2 Uninstall Cisco BAC from your system (see Uninstalling Cisco BAC, page 3-33 for Solaris and Uninstalling Cisco BAC, page 4-9 for Linux).

Step 3 Install Cisco BAC as described in Uninstalling Cisco BAC, page 3-33 for Solaris and Installing Cisco BAC, page 4-1 for Linux.

Step 4 After you install Cisco BAC 3.7 on your system, restore the database from the backup, and copy the recovered database to the database location that the RDU uses. For detailed information, see the *Cisco Broadband Access Center Administrator's Guide, Release 3.7*.

Adding Components in Solaris

This section describes how you can add one component of Cisco BAC to a system on which other components have already been installed. This situation arises mainly in a deployment similar to a lab installation, where, for the purposes of testing, more than one component is installed on a single machine. The definitions file (bpr_definitions.sh) is updated whenever you add new components.

Note Before you add components, ensure that all the components belong to the Cisco BAC 3.7 version.

When the installation program detects the presence of one component on your system, it does not allow you to add that particular component. It prompts you to add or install only other components.

For example, if you have installed a DPE on a system and then rerun the installation program, the program does not allow you to install the DPE.

The procedures for adding a component are similar to those for a fresh installation, except that the program does not allow you to add the component that you have already installed.

You cannot reinstall a component that you have already installed. If you must perform a reinstallation, first uninstall that component, and then re-install it.

Note Before you add the DPE, ensure that the RDU and the DPE belong to the BAC 3.7 version.

When the installation program detects the presence of an RDU on your system, it does not allow you to re-add the RDU. It prompts you to add or install only the DPE.

Note To ensure a smooth installation, we recommend that you install the RDU before you install the DPE.

Unlike the procedure in a fresh installation, while adding a DPE, you cannot install the home *BPR_HOME* and data *BPR_DATA* directories in a location of your choice. The directories are installed only in the location where you choose to install the RDU directories.

Note Adding the other components from the CLI is similar to Adding a DPE from the CLI, page 3-23.

Adding a DPE from the CLI

To add the DPE from the CLI:

Step 1 Log into the computer on which you intend to install Cisco BAC components, with *root* access. Use an X-Window client to log in.

Step 2 At the Solaris system prompt, change directory to your CD-ROM drive or other installation media. The installation program, pkgadd, is at the root of this drive.

Step 3 Enter the following command to start the installation program:

```
# install-path/BAC_3.7_SolarisK9/install_bac.sh
```

The installation program verifies that you have installed the correct patches to the Solaris operating system. When the verification is complete, the program displays the Welcome screen.

Step 4 Press **Enter** to continue.

The installation program prompts you to select one or more components,

Step 5 Enter **y** and press **Enter** at the DPE prompt.

The installation program prompts you to add only the DPE.

Step 6 Confirm the components that you want to install; enter **y** and press **Enter** to continue.

The program displays a message that it is starting individual component validation.

Step 7 Press **Enter** to continue.

When validation is complete, the program prompts you to enter the IP address and the listening port of the RDU.

Step 8 Press **Enter** to accept the hostname of the RDU.

Note The installation program obtains the IP address of the RDU automatically. You do not need to enter this value.

Step 9 Accept the default port number, 49187, by pressing **Enter**; or enter another port number.

Caution If you change the default listening port value, ensure that the new value does not conflict with any existing port assignments. Also, ensure that you configure all DPEs with the correct RDU port number. Refer to the *Cisco Broadband Access Center Administrator's Guide, Release 3.7,* for information on configuring the DPE.

Step 10 Confirm the IP address and the listening port number; enter **y** and press **Enter**.

The program prompts you to enter the shared secret password.

Step 11 Enter the password that you want to use for authentication between the Cisco BAC servers, and press **Enter**.

Note You must use the same shared secret password for all RDUs and DPEs in your network. The default password is **secret**.

Step 12 Press **Enter** to continue.

The installation parameters that you selected, appear.

Step 13 Enter **y** and press **Enter** to confirm the parameters, and add the DPE.

The Installation Summary appears when the installation is complete.

Step 14 Press **Enter** to exit the installation program.

The Installation Summary appears when the installation is complete.

Step 15 Press **Enter** to exit the installation program.

DPE Properties

The following is the list of DPE properties introduced in Cisco BAC 3.7.

Table 3-1 DPE Properties

Parameter	Description	Default	Property Name
Lease Query Client Port	The port for local end of the socket	68	/cnrQuery/clientPort
DHCP Server Port	This is the port to send the DHCP messages.	67	/cnrQuery/serverPort
Lease Query Threads	The maximum number of threads for lease query reads.	16	/cnrQuery/threads/maximum
GIADDR	The GIADDR to use when sending lease queries.	localhost	/cnrQuery/giaddr
Cisco Network Registrar Echo	A flag indicating that the DHCP lease query must use Cisco Network Registrar echo.	false	/cnrQuery/useEcho
Lease Query Timeout	The period of time that the LeaseQuery object will wait for a response from the DHCP server before giving up.	500ms	/dhcpLeaseQuery/timeout
Lease Query Retry	The number of times to attempt a retry with a DHCP server before giving up.	1	/dhcpLeaseQuery/retries
Lease Query client socket address	Local socket address for listening for DHCPv4 packets.	0.0.0.0:68	/cnrQuery/clientSocketAddress
Lease Query wait for all Responses	A flag to indicate if the first response should be returned or else wait for all DHCP servers to respond.	false	/dhcpLeaseQuery/requireAllAnswers
Cisco Access Registrar Shared Secret	The shared secret used between Cisco Access Registrar BAC extension and the DPE.	secret	/CAR/sharedSecret
DPE Auth Service IP Address	The address used by the auth service to authorize the incoming request.	127.0.0.1	/server/http/services/5
DPE Auth Service Port	The port used by the auth service.	7551	/server/http/services/5/port
Auth Service SSL	Enables or disables the use of SSL by the auth service	Disabled	/server/http/services/5/ssl/enable
Auth Service Authentication mode	Sets the HTTP authentication mode for the auth service	digest	/server/http/services/5/auth/mode
Enabling Auth Service	Enables or disables the auth service	enabled	/server/http/services/5/enable

Parameter	Description	Default	Property Name
Auth service SSL authentication mode	Sets Auth service SSL authentication mode.	none	/server/http/services/5/ssl/auth/mode
Auth service SSL store password	Sets Auth service SSL store password	110a110419150e0510	/server/http/services/5/ssl/storepassword
Auth service SSL key password	Sets Auth service SSL key password	500450560a14030d4f	/server/http/services/5/ssl/keypassword
Auth service SSL key store	Sets Auth service SSL key store	server-certs	/server/http/services/5/ssl/keystore
Auth service SSL cipher	Enables or disables Auth service SSL cipher suits	enabled	/server/http/services/5/ssl/cipher/all-cipher-suites
Auth service trace prefix	Sets Auth service trace prefix	/server/log/trace/auth/1/	/server/http/services/5/trace/prefix
Auth service all authentication trace log	Enables or disables Auth service all authentication trace log	disabled	/server/log/trace/auth/1/auth/all/enable
Auth service authentication failures trace log	Enables or disables Auth service authentication failures trace log	disabled	/server/log/trace/auth/1/auth/failures/enable
Auth service HTTP details trace log	Enables or disables Auth service HTTP details trace log	disabled	/server/log/trace/auth/1/http/details/enable
Auth service HTTP faults trace log	Enables or disables Auth service HTTP faults trace log	disabled	/server/log/trace/auth/1/http/faults/enable
Auth service HTTP headers trace log	Enables or disables Auth service HTTP headers trace log	disabled	/server/log/trace/auth/1/http/headers/enable
Auth service errors trace log	Enables or disables Auth service errors trace log	disabled	/server/log/trace/auth/1/errors/enable

Note Unless the property values are changed either in DPE properties or via DPE CLI, the default values will be used.

CNR Properties

See the *Cisco Broadband Access Center Administrator's Guide* for the Cisco Access Registrar property file. The property file is explained in the section *Using the changeARProperties.sh Tool.*

CAR Properties

See the *Cisco Broadband Access Center Administrator's Guide* for the Cisco Network Registrar property file. The property file is explained in the section *Using the changeNRProperties.sh Tool.*

STUN Properties

The following is the list of STUN properties introduced in Cisco BAC 3.7.

Table 3-2 STUN Properties

Parameter	Default	Property Name
Port for receiving the CXF connection requests from RDU.	888	/server/stun/http/port
UDP port for receiving the binding messages from the device.	3478	/stun/server/port
Shared secret for authenticating the binding messages.		/stun/sharedsecret
User name for accessing the STUN CXF service for sending connection requests.	bacadmin	/server/stun/http/username
User password for accessing the STUN CXF service for sending connection requests.		/server/stun/http/password
This flag will indicate if authorization is required for the binding messages. UDP authorization flag.	true	/stun/auth/required
Task which logs the STUN statistics such as binding requests, responses, failures, for the configured interval in a stunstatistics.log file under *STUN_DATA*/stun/logs directory.	900000	/stun/binding/statistics/interval
Number of connection request UDP message to be sent each time to the device.	3	/stun/number/udp/cr/packets
File to persist the binding mapping information.	/opt/CSCObac/stun/conf/bindinginfo	/bindinginfo/File
Task which persists the binding mapping information for the configured interval.	300000	/bindinginfo/persistor/time

Upgrading Cisco BAC

This section describes how to upgrade from an earlier version of Cisco BAC to Cisco BAC 3.7.

Before upgrading to Cisco BAC 3.7, ensure that you obtain the license file that this release supports. After the upgrade is complete, the installation program deletes all existing license keys. You must then install the license file that Cisco BAC 3.7 supports, using the administrator user interface.

For details on obtaining and installing the license file, see the *Release Notes for the Cisco Broadband Access Center 3.7*.

The Cisco BAC upgrade procedure requires that you upgrade the components as recommended in the following sections. Performing the upgrade in any other sequence results in error during provisioning.

1. Backing up the RDU, page 3-28
2. Upgrading the RDU, page 3-28
3. Upgrading the DPE, page 3-32

Backing up the RDU

Before upgrading Cisco BAC components, ensure that you backup the RDU database files. Throttling limits the I/O bandwidth used by the DB with backup utility. The Throttle option specifies the rate at which the backup tool reads the files it copies. While using this option, if the reading rate is high, the tool goes into Sleep mode till the rate comes down.

Note We recommend that you use the Throttle option always since it is not an I/O intensive operation.

To back up the RDU database, run the **backupDb.sh** script in the *BPR_HOME/rdu/bin* directory.

For example:

```
# backupDb.sh /var/backup -throttle 500/opt/
```

where */var/backup* identifies the database backup directory.

In this example, all backup database files are stored in a directory called */var/backup/rdu-backup-20071116-031028*. The last subdirectory (*rdu-backup-20070316-111028*) is automatically created with a current time stamp.

Note The time-stamped subdirectory format is *rdu-backup-yyyyMMdd-HHmmss*. In this example, the subdirectory would be *rdu-backup-20071116-031028*. This means that the directory contains a backup that was started at 3:10:28 a.m. on November 16, 2007.

For additional information on using the **backupDb.sh** tool, see the *Cisco Broadband Access Center Administrator Guide 3.7*.

Upgrading the RDU

Before upgrading the RDU, we recommend that you archive your files in the *BPR_HOME*/rdu/conf directory.

To upgrade the RDU:

Step 1 Upgrade to Cisco BAC 3.7,by running the following command:

```
# install-path/BAC_3.7_SolarisK9/install_bac.sh
```

a. When prompted, press **Enter** to continue, the upgrade message is displayed.

b. Enter **y** to start the upgrade process.

c. To verify whether the version information indicates Cisco BAC release 3.7, enter:

*# **pkgparam CSCObac** VERSION*

Step 2 Manually restart the RDU process to finish the upgrade process.

For example, from the command line, run:

```
# /etc/init.d/bprAgent start rdu
```

Note While upgrading from earlier version of Cisco BAC, the program displays warning messages for the properties that are already present in the DB. For example, `"A custom property with the name [/server/rdu/allow-unknown-cpe] already exists in the system."` Such warning messages can be ignored.

Migrating the RDU Database

About Backward Compatibility

The Cisco BAC 3.7 RDU with a migrated database can operate with earlier versions of Solaris DPEs and Cisco Network Registrar Extensions servers for gradual online migration.

Migration preserves the device record revision numbers used in DPE synchronization. As a result, DPE repopulation is not triggered after the RDU database upgrade. This ensures the least disruption until you upgrade the specific DPE.

Verifying Database Integrity

We recommend that you perform a dry run of the migration process on a staging (nonproduction) system, instead of on a live system, during RDU downtime. These steps may not be practical during a live migration, because in the case of a large database, verification can take an extended length of time.

To verify the database:

Step 1 Before migration, run the verifyDb.sh tool on a backup snapshot.

To verify the database before migration, use the verifyDb.sh tool from the Cisco BAC installation corresponding to the version of the database. You cannot verify a nonmigrated database with the Cisco BAC 3.7 version of verifyDb.sh.

For example, enter:

```
# /opt/BPR_HOME/rdu/internal/db/bin/verifyDb.sh -dbdir /disk1/backup
```

This pathname is specific to the Cisco BAC installation version that was installed before migrating to Cisco BAC 3.7.

Step 2 After migration and upgrade to Cisco BAC 3.7, run the Cisco BAC 3.7 versions of verifyDb.sh tool on the migrated database.

For example, enter:

```
# /opt/BPR_HOME/rdu/internal/db/bin/verifyDb.sh -dbdir /disk2/target
```

If any error occurs during the process, the log file, bpr-verify-db-log.xml, is generated in the path *BPR_HOME*/rdu/internal/db/bin, which contains the details of the error.

For details about the verifyDb.sh tool, see the *Cisco Broadband Access Center Administrator Guide 3.7*.

Using the RDU Migration Tool

This release of Cisco BAC consists of a migration tool that facilitates DB portability between platforms. You can also use this migration tool to migrate between different platforms. This tool contains JRE 1.6.0_27, Berkeley db 5.1.25 libraries and Cisco BAC 3.7 *bpr.jar*.

In Cisco BAC 3.7, Solaris to Solaris RDU database migration can be done using the Migration Tool (*BAC_37_MigrationTool.tar.gz*).

Before you start with the migration task, ensure you perform the steps explained in Using the RDU Migration Tool, page 3-30 section.

In the following section, steps 1 to 10 have to be done on the Solaris server that has the earlier version of Cisco BAC and steps 11 to 13 need to be done on the Linux server where Cisco BAC 3.7 needs to be installed.

To perform a database migration:

Step 1 Stop the brpAgent.

Step 2 Back up the existing Cisco BAC 3.x RDU database, using the backupDb.sh tool. For details, see the *Cisco Broadband Access Center Administrator Guide 3.7*.

For example:

```
# /BPR_HOME/rdu/bin/backupDb.sh -nosubdir /disk1/backup
```

- **-nosubdir**—Disables the automatic creation of a subdirectory. If you do not use this option, a subdirectory is created and reported to the console.
- */disk1/backup*—Identifies the location for the database backup files.

Note You must stop the brpAgent before taking a backup of the DB.

Step 3 Back up the following files. Backup is required only if you have customized these files.

- Files under *<BAC_HOME>/rdu/conf/*
  - *rdu.properties*
  - *api.properties*
  - Other xml files and dtd files
- MIB files under *<BAC_HOME>/rdu/mibs/*
- *.xml files under *<BAC_HOME>/snmp/conf/*

Step 4 Verify whether the database has been backed up by checking the history.log file, which resides in the *BPR_DATA* directory.

Step 5 Recover the database that you have backed up to a consistent state, using the recoverDb.sh tool. For details, see the *Cisco Broadband Access Center Administrator Guide 3.7*.

For example:

```
# /opt/CSCObpr/rdu/bin/recoverDb.sh /disk1/backup
```

where */disk1/backup* identifies the location of the database backup files.

Step 6 After recovering the database, verify it by running the command:

For example:

```
# /opt/CSCObpr/rdu/internal/db/bin/verifydb.sh -dbdir /disk1/backup
```

Note In case of any error while verifying the database, contact Cisco Support.

Step 7 Copy the *BAC_37_MigrationTool.tar.gz* from Cisco.com location.

Step 8 Go to the directory BAC_37_MigrationTool /migration.

Step 9 Run **migrationTool.sh** > help and follow the help instructions.

Step 10 After the migration is complete, copy the whole database directory and backed-up files to the Cisco BAC 3.7 setup machine.

Step 11 Restore the following files.

a. Files under *<BAC_HOME>/rdu/conf/*.

- *rdu.properties*
- *api.properties*
- Other xml files and dtd file

b. MIB files under *<BAC_HOME>/rdu/mibs/*

c. *.xml files under *<BAC_HOME>/snmp/conf/*

Note While restoring the files, make sure that you merge the changes without overwriting the newly installed files.

Step 12 Run restoreDB.sh on the newly copied directory.

Step 13 Start the bprAgent.

Upgrading the DPE

Before upgrading the DPE, we recommend that you archive your files in the *BPR_HOME/dpe/conf* directory.

To upgrade the DPE:

Step 1 Upgrade to Cisco BAC 3.7,by running the following command:

```
# install-path/BAC_3.7_SolarisK9/install_bac.sh
```

a. Press **Enter** to continue when you are prompted and the following message is displayed:

```
Upgrading BAC from <earlier version> to 3.7. Are you sure? (y/n) [n]:
```

b. Enter **y** to start the upgrade process.

where *file-path* specifies the complete path to the directory in which the BAC_3.7_SolarisK9 directory has been created.

To verify whether the version information indicates Cisco BAC release 3.7, enter:

*# **pkgparam CSCObac** VERSION*

Step 2 Restart the DPE process to complete the upgrade process.

For example, from the command line, run:

```
# /etc/init.d/bprAgent start dpe
```

Upgrading the CNR Extensions

Upgrading the CNR Extensions is similar to Upgrading the RDU, page 3-28.

Upgrading the CAR Extensions

Upgrading the CAR Extensions is similar to Upgrading the RDU, page 3-28.

Uninstalling Cisco BAC

This section describes how to uninstall Cisco BAC from the CLI.

Note You cannot uninstall the RDU and the DPE that are installed in a same server separately. Both components are uninstalled together.

The uninstall program removes all the DPE and RDU component files under the installation directory (the default installation directory is /opt/CSCObac) that are installed in the same server when the **uninstall** command is run. It also shuts down and removes these processes if they are detected: RDU, SNMP Agent, Tomcat, Watchdog, and DPE.

The uninstallation program does not remove files that were placed outside the installation directory. For example, a component installation places the database and database transaction logs directories under /var/CSCObac.

These files must be manually removed. However, if you choose to install the home, data, and database transaction log directories in the same location, the uninstallation program warns you that continuing the uninstallation will remove the data and log files.

If the program fails to uninstall Cisco BAC, error messages appear.

Note After uninstalling Cisco BAC, manually remove the Data and Database Transaction Logs directories (see the Post-Uninstallation Task, page 3-34).

Uninstalling from the CLI

This section describes the procedures to uninstall Cisco BAC.

After uninstalling Cisco BAC, manually remove the data and database logs directories. See Post-Uninstallation Task, page 3-34.

To uninstall Cisco BAC from the command line:

Step 1 Log in as root.

Step 2 Manually remove the configuration of the Cisco BAC extensions on the Cisco Network Registrar server. You can do this from any server that has nrcmd installed and has connectivity with Cisco Network Registrar.

- To uninstall the Cisco BAC extensions from your Cisco Network Registrar configuration, enter:

```
# NR_HOME/local/usrbin/nrcmd -N admin -P changeme -b <
BPR_HOME/cnr_ep/bin/bpr_cnr_disable_extpts.nrcmd
```

- To reload your DHCP server, enter:

```
# /etc/init.d/nwreglocal stop
# /etc/init.d/nwreglocal start
```

- To remove the Cisco BAC extensions from the Cisco Network Registrar extensions directory, enter:

```
# rm -rf NR_HOME/local/extensions/dhcp/dex/libbprextensions.so
```

Step 3 Manually remove the Cisco Access Registrar extensions on the Cisco Access Registrar server using this command.

```
rm -rf CAR_HOME/scripts/radius/java/dpeext.jar
```

Step 4 Restart the Cisco Access Registrar server by running:

```
# /etc/init.d/arserver restart
```

Step 5 At the CLI prompt, enter:

```
# pkgrm CSCObac
```

Step 6 Enter **y**, and press **Enter** to start uninstalling.

Step 7 Enter **y** and press **Enter**.

When uninstallation is complete, a message appears.

Post-Uninstallation Task

After uninstalling Cisco BAC, manually remove the data and database transaction logs directories. To remove these directories:

Step 1 Log in as root.

Step 2 Remove the data and the database transaction logs. (The default directory for both is */var/CSCObac*.)

For example, enter:

```
# rm -rf /var/CSCObac
```

The data and the database transaction logs directories are deleted.

CHAPTER 4

Installing and Uninstalling Cisco BAC on Linux

This chapter explains how to successfully install Cisco BAC on Linux 5.

The SELinux and iptable should be disabled. Also, ensure that before installing Cisco BAC, you install the sysstat package for the proper execution of the diagnostic scripts. This is an optional package which you might have not installed while installing Linux

Installing Cisco BAC

The initial steps in the Cisco BAC installation program are identical, regardless of the component you are installing. This section explains how to work with the installation program.

To install Cisco BAC:

Step 1 Log into the intended Cisco BAC with your user name and password.

Step 2 At the Linux system prompt, change directory to your CD-ROM drive or other installation media.

Step 3 Ensure that the **gzip** and **gtar** utilities are available on your system under /bin directory, to decompress and unpack the Cisco BAC installation file, and:

a. Change to the directory in which you will decompress and extract the installation file.

b. Decompress and unpack the file with the .gtar.gz extension. Enter:

```
gtar zxvf BAC_37_LinuxK9.gtar.gz
```

The utility creates the BAC_37_LinuxK9 directory into which the installation program is extracted.

Note If the program displays a checksum error while unpacking, specify the path to the GNU tar on your machine.

Step 4 After the installation program is extracted, you can choose to install the components.

Before you begin any of these procedures, you must complete the initial procedure described in Installing Cisco BAC, page 4-1.

To install the Cisco BAC components, see:

Installing the RDU

Install the RDU on a server running Linux that meets the requirements described in Cisco BAC Components, page 1-1.

Note We recommend that you configure the RDU server to use a static IP address.

To install the RDU, complete the initial installation described in Installing Cisco BAC, page 4-1. After you do this:

Step 1 Enter the following command to start the installation program in interactive mode:

```
# install-path/BAC_37_LinuxK9/install_bac.sh
```

where *install-path* specifies the complete path to the directory in which the BAC_37_LinuxK9 directory has been created.

The installation program verifies that you have installed the required patches on the Linux operating system. When the verification ends, the Welcome information appears.

Step 2 Press **Enter** to continue.

The program prompts you to choose the component that you want to install.

Step 3 Enter **y** and press **Enter** at the RDU prompt.

To skip installing the DPE, Cisco Network Registrar extension points, Cisco Access Registrar extension points and the STUN server, enter **n** and press **Enter**. You can choose to install these components later.

Step 4 Confirm the components that you want to install. To do this, enter **y** and press **Enter**.

The home directory prompt appears.

Step 5 Accept the default directory, /opt/CSCObac, by pressing **Enter**; or enter another directory.

Step 6 Confirm the directory location.To do this, enter **y** and press **Enter**.

The data directory prompt appears.

Step 7 Accept the default directory, /var/CSCObac, by pressing **Enter**; or enter another directory.

Step 8 Confirm the directory location.To do this, enter **y** and press **Enter**.

The database log directory prompt appears.

Step 9 Accept the default directory, /var/CSCObac, by pressing **Enter**; or enter another directory.

Step 10 Confirm the directory location.To do this, enter **y** and press **Enter**.

The program starts preparing the packages for the installation.

Step 11 Accept the default port number, 49187, by pressing **Enter**; or enter another port number.

Caution If you change the default listening port value, ensure that the new value does not conflict with any existing port assignments. Also, ensure that you configure all DPEs with the correct RDU port number. For details on configuring the DPE, see the *Cisco Broadband Access Center DPE CLI Reference, 3.7*.

Step 12 Confirm the listening port number. To do this, enter **y** and press **Enter** to continue.

The program prompts you to enter the shared secret password.

Step 13 Enter the shared secret password that you want to use for authentication among Cisco BAC servers, and confirm the password.

Note You must use the same shared secret password for the RDU, all DPEs, and Cisco Network Registrar extension points in your network.

Step 14 Press **Enter** to continue.

The program displays the parameters you have selected to install.

Step 15 Enter **y** and press **Enter** to confirm the installation parameters.

After a successful installation, the following message appears:

```
Installation of <CSCObac> was successful.
```

Installing the DPE

Install the DPE on a server running Linux that meets the requirements described in Cisco BAC Components, page 1-1.

Note We recommend that you configure the DPE server to use a static IP address. During DPE installation, if the program detects a TFTP server or a ToD server running on the same server as the DPE, the installation displays an error message and quits. To terminate the TFTP or ToD server, perform the steps that the error message lists.

To install the DPE, complete the initial installation described in Installing Cisco BAC, page 4-1. To start the installation program in interactive mode:

Step 1 Run:

```
# install-path/BAC_37_LinuxK9/install_bac.sh
```

where *install-path* specifies the complete path to the directory in which the BAC_37_LinuxK9 directory has been created.

The installation program verifies that you have installed the required patches on the Linux operating system. When the verification ends, the Welcome information appears.

Step 2 Press **Enter** to continue.

The program prompts you to choose the component that you want to install.

Step 3 Enter **y** and press **Enter** at the DPE prompt.

To skip installing the RDU, Cisco Network Registrar extension points, Cisco Access Registrar extension points and the STUN server, enter **n** and press **Enter**. You can choose to install these components later.

The home directory prompt appears.

Step 4 Accept the default directory, /opt/CSCObac, by pressing **Enter**; or enter another directory.

Step 5 Confirm the directory location. To do this, enter **y** and press **Enter**.

The data directory prompt appears.

Step 6 Accept the default directory, /var/CSCObac, by pressing **Enter**; or enter another directory.

The database log directory prompt appears.

Step 7 Accept the default directory, /var/CSCObac, by pressing **Enter**; or enter another directory.

Step 8 Confirm the directory location. To do this, enter **y** and press **Enter**.

The program prompts you to enter the shared secret password. Enter the shared secret password that you want to use for authentication between the Cisco BAC servers.

Step 9 Re-enter the password for confirmation, and press **Enter**.

The program prompts you to enter information on the RDU, required to install the extensions.

Step 10 Enter the IP address (or hostname) and the listening port of the host on which you have installed the RDU.

Step 11 Accept the default information, by pressing **Enter**; or enter alternative information.

Step 12 Confirm the information. To do this, enter **y** and press **Enter**.

The installation proceeds, and displays the following message after successful installation:

```
Installation of <CSCObac> was successful.
```

Installing the Cisco Network Registrar Extensions

Install the Cisco Network Registrar extension points on a Linux server that meets the requirements described in Cisco BAC Components, page 1-1.

To install the Cisco Network Registrar extension points, complete the initial installation described in Installing Cisco BAC, page 4-1. After you do this

Step 1 Enter the following command to start the installation program in interactive mode:

```
# install-path/BAC_37_LinuxK9/install_bac.sh
```

where *install-path* specifies the complete path to the directory in which the BAC_37_LinuxK9 directory has been created.

The installation program verifies that you have installed the required patches on the Linux operating system. When the verification ends, welcome information appears.

Step 2 Press **Enter** to continue.

The program prompts you to choose the component that you want to install.

Step 3 Enter **y** and press **Enter** at the Cisco Network Registrar extension prompt.

To skip installing the RDU, DPE, Cisco Access Registrar extension points and the STUN server, enter **n** and press **Enter**. You can choose to install these components later.

The home directory prompt appears.

Step 4 Accept the default directory, /opt/CSCObac, by pressing **Enter**; or enter another directory.

Step 5 Confirm the directory location. To do this, enter **y** and press **Enter**.

The data directory prompt appears.

Step 6 Accept the default directory, /var/CSCObac, by pressing **Enter**; or enter another directory.

The database log directory prompt appears.

Step 7 Accept the default directory, /var/CSCObac, by pressing **Enter**; or enter another directory.

Step 8 Confirm the directory location.To do this, enter **y** and press **Enter**.

The program prompts you to enter the shared secret password. Enter the shared secret password that you want to use for authentication between the Cisco BAC servers.

Step 9 Re-enter the password for confirmation, and press **Enter**.

The program prompts you to enter information on the RDU, required to install the extensions.

Step 10 Enter the IP address (or hostname) and the listening port of the host on which you have installed the RDU.

Step 11 Accept the default information, by pressing **Enter**; or enter alternative information.

Step 12 Confirm the information. To do this, enter **y** and press **Enter**.

The installation proceeds, and displays the following message after successful installation:

```
Installation of <CSCObac> was successful.
```

Configuring Extensions

After you install the Cisco BAC extensions on the Cisco Network Registrar server, you must configure the extensions. The procedure described in this section assumes that:

- The Cisco BAC component is installed in /opt/CSCObac.
- Cisco Network Registrar is installed in /opt/nwreg2.
- The Cisco Network Registrar username is **admin** and the password is **changeme**.

To configure extensions:

Step 1 Log into the Cisco Network Registrar server, with *root* access.

Step 2 At the command line, enter:

```
# NR_HOME/local/usrbin/nrcmd -N admin -P changeme -b <
BAC_HOME/cnr_ep/bin/bpr_cnr_enable_extpts.nrcmd
```

- To reload the Cisco Network Registrar server, enter:

```
# /etc/init.d/nwreglocal stop
# /etc/init.d/nwreglocal start
```

- To reload the DHCP server alone, enter:

```
# NR_HOME/local/usrbin/nrcmd -N admin -P changeme "dhcp reload"
```

Note Before you can use the Cisco Network Registrar server, you must configure client classes, scope-selection tags, policies, and scopes. See the *User Guide for Cisco Network Registrar 7.2*.

Validating Extensions

To validate the extensions installed on the Cisco Network Registrar server, from the Cisco Network Registrar Command Line Tool (**nrcmd**), run:

Depending on whether you installed a local or regional cluster, the **nrcmd** tool is located in:

- Local—/opt/nwreg2/local/usrbin
- Regional—/opt/nwreg2/regional/usrbin

```
nrcmd> extension list
100 Ok
dexdropras:
    entry = dexdropras
    file = libdexextension.so
    init-args =
    init-entry =
    lang = Dex
    name = dexdropras
preClientLookup:
    entry = bprClientLookup
    file = libbprextensions.so
    init-args = BPR_HOME=/opt/CSCObac,BPR_DATA=/var/CSCObac
    init-entry = bprInit
    lang = Dex
    name = preClientLookup
nrcmd>
```

Note The *BPR_HOME* and *BPR_DATA* values may be different in your installation.

Also, in the **nrcmd** program, run:

```
nrcmd> extension list
100 Ok
dexdropras:
    entry = dexdropras
    file = libdexextension.so
    init-args =
    init-entry =
    lang = Dex
    name = dexdropras
preClientLookup:
    entry = bprClientLookup
    file = libbprextensions.so
    init-args = BPR_HOME=/opt/CSCObac,BPR_DATA=/var/CSCObac
    init-entry = bprInit
    lang = Dex
    name = preClientLookup
nrcmd>
```

Note When you install all the components in the same Linux server, Cisco Network Registrar will not respond to the lease queries from RDU.

Installing the Cisco Access Registrar Extension Points

Install the Cisco Abstract Registrar on a Linux server that meets the requirements described in Cisco BAC Components, page 1-1.

To install the Cisco Abstract Registrar, complete the initial installation described in Installing Cisco BAC, page 4-1. After you do this

Step 1 Enter the following command to start the installation program in interactive mode:

```
# install-path/BAC_37_LinuxK9/install_bac.sh
```

where *install-path* specifies the complete path to the directory in which the BAC_37_LinuxK9 directory has been created.

The installation program verifies that you have installed the required patches on the Linux operating system. When the verification ends, the Welcome information appears.

Step 2 Press **Enter** to continue.

The program prompts you to choose the component that you want to install.

Step 3 Enter **y** and press **Enter** at the CAR prompt.

To skip installing the RDU, DPE, Cisco Network Registrar extension points and the STUN server, enter **n** and press **Enter**. You can choose to install these components later.

The home directory prompt appears.

Step 4 Accept the default directory, */opt/CSCObac*, by pressing **Enter**; or enter another directory.

Step 5 Confirm the directory location. To do this, enter **y** and press **Enter**.

The data directory prompt appears.

Step 6 Accept the default directory, */var/CSCObac*, by pressing **Enter**; or enter another directory.

Step 7 Confirm the directory location.To do this, enter **y** and press **Enter**.

The program prompts you to enter information on the RDU required to install the extensions.

Step 8 Enter the IP address (or hostname) and the listening port of the host on which you have installed the RDU.

Step 9 Accept the default information, by pressing **Enter**; or enter alternative information.

Step 10 Confirm the information. To do this, enter **y** and press **Enter**.

The installation proceeds, and displays the following message after successful installation:

```
Installation of <CSCObac> was successful.
```

Installing the STUN Server

Install the STUN on a server running Linux that meets the requirements described in Cisco BAC Components, page 1-1.

To install the STUN, complete the initial installation described in Installing Cisco BAC, page 4-1. After you do this:

Step 1 Enter the following command to start the installation program in interactive mode:

```
# install-path/BAC_37_LinuxK9/install_bac.sh
```

where *install-path* specifies the complete path to the directory in which the BAC_37_LinuxK9 directory has been created.

The installation program verifies that you have installed the required patches on the Linux operating system. When the verification ends, the Welcome information appears.

Step 2 Press **Enter** to continue.

The program prompts you to choose the component that you want to install.

Step 3 Enter **y** and press **Enter** at the STUN server prompt.

To skip installing the RDU, DPE, Cisco Network Registrar extension points and the Cisco Access Registrar extension points, enter **n** and press **Enter**. You can choose to install these components later.

The home directory prompt appears.

Step 4 Accept the default directory, /opt/CSCObac, by pressing **Enter**; or enter another directory.

Step 5 Confirm the directory location. To do this, enter **y** and press **Enter**.

The data directory prompt appears.

Step 6 Accept the default directory, /var/CSCObac, by pressing **Enter**; or enter another directory.

Step 7 Confirm the directory location.To do this, enter **y** and press **Enter**.

The program prompts you to enter information on the RDU required to install the extensions.

Step 8 Enter the IP address (or hostname) and the listening port of the host on which you have installed the RDU.

Step 9 Accept the default information, by pressing **Enter**; or enter alternative information.

Step 10 Confirm the information. To do this, enter **y** and press **Enter**.

The program prompts you to enter the STUN HTTP listening port.

Step 11 Accept the default information, by pressing **Enter**; or enter alternative information.

The program prompts you to enter the STUN UDP listening port.

Step 12 Accept the default information, by pressing **Enter**; or enter alternative information.

The program prompts you to enter the STUN HTTP user name.

Step 13 Accept the default information, by pressing **Enter**; or enter alternative information.

The program prompts you to enter the STUN HTTP password.

Step 14 Accept the default information, by pressing **Enter**; or enter alternative information.

The program prompts you to enter the password to be used for UDP CR authentication.

Step 15 Accept the default information, by pressing **Enter**; or enter alternative information

The program prompts you to enter the shared secret password.

Step 16 Enter the shared secret password that you want to use for authentication between the Cisco BAC servers.

Step 17 Re-enter the password for confirmation, and press **Enter**.

The installation proceeds, and displays the following message after successful installation:

```
Installation of <CSCObac> was successful.
```

Adding Components in Linux

Adding components in Linux is similar to that of Solaris. See Adding Components in Solaris, page 3-23 for details.

Upgrading Cisco BAC

This section describes how to upgrade a Cisco Broadband Access Center 3.x installation to Cisco Broadband Access Center 3.7.

You must stop the process watchdog (bprAgent) before upgrading. After the upgrade is complete, Cisco BAC does not restart the process watchdog automatically.

Upgrading Cisco BAC on Linux is similar to the upgrading of Cisco BAC on Solaris. See Upgrading Cisco BAC, page 3-27 for the details.

Migrating the RDU Database

Migrating the RDU database on Linux is similar to the RDU database migration on Solaris. See Migrating the RDU Database, page 3-29 for the details.

Uninstalling Cisco BAC

This section describes how to uninstall Cisco Broadband Access Center (Cisco BAC).

The procedure described in this section uninstalls the RDU, DPE, Cisco Access Registrar extension points and Cisco Network Registrar extensions but it does not uninstall the Cisco Network Registrar application. Before removing Cisco BAC, manually remove the Cisco BAC configuration on Cisco Network Registrar.

The uninstallation program removes all files found in the installation directory (the default directory is /opt/CSCObac). The program also shuts down and removes these processes, if they are detected: SNMP Agent, Tomcat, Cisco BAC agent, RDU, and DPE.

The uninstallation program does not remove files that were placed outside the installation directory.

For example, a component installation places the database and database logs directories under /var/CSCObac. These files must be removed manually. (Subsequent sections describe how to delete these files.) Also, the program does not remove any files found in the Cisco Network Registrar directory.

If you have installed Cisco BAC extensions on Cisco Network Registrar, you must uninstall those extensions to completely uninstall the Cisco BAC program; otherwise, an error message appears.

Note The path to the Cisco Network Registrar extensions differs based on the location where you have installed Cisco Network Registrar; the default location is /opt/nwreg2.

If the uninstallation program fails to uninstall Cisco BAC, error messages appear.

After uninstalling Cisco BAC, manually remove the data and database logs directories. See Post-Uninstallation Task, page 4-10.

To uninstall Cisco BAC from the command line:

Step 1 Log in using your user name and password.

Step 2 Manually remove the configuration of the Cisco BAC extensions on the Cisco Network Registrar server. You can do this from any server that has **nrcmd** installed and connectivity with Cisco Network Registrar.

- To uninstall the Cisco BAC extensions from your Cisco Network Registrar configuration, enter:

```
# NR_HOME/local/usrbin/nrcmd -N admin -P changeme -b <
BPR_HOME/cnr_ep/bin/bpr_cnr_disable_extpts.nrcmd
```

- To reload your DHCP server, enter:

```
# /etc/init.d/nwreglocal stop
# /etc/init.d/nwreglocal start
```

- To remove the Cisco BAC extensions from the Cisco Network Registrar extensions directory, enter:

```
# rm -rf NR_HOME/local/extensions/dhcp/dex/libbprextensions.so
```

Step 3 Run the following command to uninstall:

```
# # install-path/BAC_37_LinuxK9/uninstall_bac.sh
```

Step 4 Enter **y** to continue.

Step 5 Run the following commands to delete the previously installed directories.

```
rm -rf /opt/CSCObac
rm -rf /var/CSCObac
```

Post-Uninstallation Task

After you have uninstalled Cisco BAC, manually remove the data and database logs directories. To remove these directories:

Step 1 Log in as root.

Step 2 Remove the data and the database logs directories. (The default directory for both is /var/CSCObac.)

For example, enter:

```
# rm -rf /var/CSCObac
```

The data and the database logs directories are deleted.

CHAPTER 5

Configuring the Syslog Utility to Receive Cisco BAC Alerts

This chapter explains how to configure the syslog daemon after you install the Cisco Broadband Access Center (BAC). In case of a local data server, you can configure the syslog utility on any Cisco BAC component server to receive alerts from the system. For receiving the syslogs in a centralized server from all the BAC components, you can configure the syslog daemon either on any Cisco BAC component server or on a separate server.

Note Configuring the syslog file is an optional task.

Syslog is a client-server protocol that manages the logging of information on UNIX. Cisco BAC generates alerts through the syslog service. Cisco BAC syslog alerts are not a logging service; they notify that a problem exists, but do not necessarily define the specific cause of the problem.

The information related to the problem resides in the appropriate Cisco BAC log files, rdu.log and dpe.log. If you choose to configure the syslog file, syslog alerts are directed to a separate log file.

For more information on error messages and alerts, refer to the *Cisco Broadband Access Center 3.7 Administrator Guide*.

Configuring Syslogs on a Local Server

To configure the syslog utility on a local Cisco BAC RDU/DPE server (Solaris and Linux):

Step 1 Log in as *root* on the server.

Step 2 At the command line, create the log file.

For example:

```
# touch /var/log/bac.log
```

Step 3 Open the /etc/syslog.conf file with a text editor, such as *vi*.

Step 4 Add the following lines to the /etc/syslog.conf file:

```
local6.alert        /var/log/bac.log
local6.info         /var/log/bac.log
```

Note You must insert one or more tabs between the local6:info and */var/log/bac.log* information.

Step 5 Save and close the /etc/syslog.conf file.

Step 6 To force the syslog utility to take the new configuration, at the command line, enter:

```
# ps -ef  | grep syslogd
   root      217   1    0     Nov   26      ?    0:00      /usr/sbin/syslogd

   kill -HUP 217
```

Note The process ID (PID) in this example is 217, but may change when you run **ps -ef | grep syslogd**. Use the correct output from that command as the input to **kill -HUP**.

Syslog is now ready to receive alerts from Cisco BAC.

Configuring Centralized Solaris Server to Receive Syslogs

On Solaris machines, the LOG_FROM_REMOTE property specifies whether RDU/DPE server messages are logged. By default, this property is enabled.

To configure a centralized server to receive syslog alters from a RDU/DPE server:

Step 1 Login to the server as root.

Step 2 By default the LOG_FROM_REMOTE property is enabled. In case it is not, you can enable it by setting it's value to true as shown in the following commands.

```
# svccfg -s svc:/system/system-log setprop config/log_from_remote = true
# svcadm refresh svc:/system/system-log
```

Step 3 Create a dummy file.

```
# touch /var/log/messages
```

Step 4 Add the following configuration in /etc/syslog.conf file:

```
local6.info             @loghost
local6.info             /var/log/messages
```

Step 5 Restart the syslog daemon.

```
# svcadm restart system-log
# tail -f /var/log/messages
```

Note Always use Tab while modifying /etc/syslog.conf. Using the space bar shows errors while you restart syslogd.

Configuring RDU/DPE to Send Syslog to Centralised Server on Solaris

After you configure syslog daemon on a centralized server, you must configure the RDU/DPE server to send messages to the centralized server. To do this, edit the /etc/hosts file on the RDU/DPE server as explained below.

Step 1 Determine the IP address and fully qualified host name of the RDU/DPE server logging host.

Step 2 Login to the server as *root*.

Step 3 To enable the RDU/DPE server logging hostname, add the following entry in the /etc/hosts file:

For example;

```
IP-address    fully-qualified-domain-name    hostname    "loghost"
```

The /etc/hosts file has the nickname loghost, for the server.

Step 4 Edit the /etc/syslog.conf file to send the syslog messages to the server.

For example;

```
local6.info    ifdef(`LOGHOST', /var/log/messages, @loghost)
```

Step 5 Restart the syslog daemon to get the RDU/DPE server logging started.

```
# svcadm restart system-log
```

To test whether the syslog server is receiving the messages, stop the RDU server. The DPE and Cisco Network Registrar servers will send a message indicating the connection failure.

Configuring Centralized Linux Server to Receive Syslogs

By default, syslog daemon on a centralized server does not expect to receive messages from the Linux RDU/DPE servers. You must configure the centralized server for the syslog daemon to start listening to these messages.

The syslog daemon checks the /etc/syslog.conf file to determine the expected names and locations of the log files it should create. It also checks the /etc/sysconfig/syslog file to determine the various modes in which it should operate. The syslog daemon will not receive RDU/DPE server messages unless the SYSLOGD_OPTIONS variable in this file has a -r included in it as shown below:

```
# Options to syslogd
# -m 0 disables 'MARK' messages.
# -r enables logging from RDU/DPE server machines
# -x disables DNS lookups on messages received with -r
# See syslogd(8) for more details
 SYSLOGD_OPTIONS="-m 0 -r"
# Options to klogd
# -2 prints all kernel oops messages twice; once for klogd to decode, and
#    once for processing with 'ksymoops'
# -x disables all klogd processing of oops messages entirely
# See klogd(8) for more details
KLOGD_OPTIONS="-2"
```

You must restart the syslog daemon for the changes to take effect. The server listens on UDP port 514, which you can verify using one of the following netstat command variations:

- **# netstat -a | grep syslog**
  udp 0 0 *:syslog *:*

- **# netstat -an | grep 514**
  udp 0 0 0.0.0.0:514 0.0.0.0:*

Configuring RDU/DPE to Send Syslog to Centralised Server on Linux

After you configure syslog daemon on the centralized server, you must configure the RDU/DPE server to send messages to it. To do this, edit the /etc/hosts file on the RDU/DPE server.

Step 1 Determine the IP address and fully qualified hostname of the RDU/DPE server logging host.

Step 2 Log in as *root* on the server

Step 3 To enable the RDU/DPE server logging hostname, add the following entry in the /etc/hosts file:

For example:

```
IP-address    fully-qualified-domain-name    hostname    "loghost"
```

In the example, the /etc/hosts file has a nickname loghost, for the server.

Step 4 Edit the /etc/syslog.conf file to send the syslog messages to the server.

For example:

```
local6.info             @loghost
local6.info             /var/log/messages
```

Step 5 Restart the syslog daemon to start RDU/DPE server logging.

To test whether the syslog server is receiving the messages, stop the RDU server. The DPE and Cisco Network Registrar servers will send a message indicating the connection failure.

INDEX

H

I

L

M

N

O

P

R

S

T

U

W