Installing and Configuring Cisco Access Registrar, 4.2

November 2008

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-17221-02

Installing and Configuring Cisco Access Registrar, 4.2

CONTENTS

About This Guide

The Installing and Configuring Cisco Access Registrar, 4.2, provides information about installing, configuring, and customizing CAR 4.2. This guide is intended to be used by experienced network administrators with working knowledge of the Solaris UNIX operating system.

This guide contains the following chapters:

- Chapter 1, "Overview," provides an overview of the installation process and dialog, information about downloading Cisco Access Registrar 4.1 software, and information about Cisco AR licensing.
- Chapter 2, "Installing Cisco Access Registrar 4.2," provides information about installing the CAR using CD-ROM or downloaded software.
- Chapter 3, "Upgrading Cisco Access Registrar Software," provides information to help you upgrade your Cisco
- Chapter 4, "Configuring Cisco Access Registrar 4.2," describes how to configure a site. Cisco Access Registrar 4.1 is very flexible. You can choose to configure it in many different ways. In addition, you can write scripts that can be invoked at different points during the processing of incoming requests and/or outgoing responses.
- Chapter 5, "Customizing Your Configuration," provides an introduction to many of the Cisco Access Registrar 4.1 objects and their properties.

This guide also includes an index.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can submit comments about Cisco documentation by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you will find information about how to:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories, security notices, and security responses for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you have identified a vulnerability in a Cisco product, contact PSIRT:

- For Emergencies only—security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- For Nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.*x* through 9.*x*.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT at the aforementioned e-mail addresses or phone numbers before sending any sensitive material to find other means of encrypting the data.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Note Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command

output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests, or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—An existing network is down, or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of the network is impaired, while most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco offerings. To order and find out more about the Cisco Product Quick Reference Guide, go to this URL:

  http://www.cisco.com/go/guide

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

  or view the digital edition at this URL:

  http://ciscoiq.texterity.com/ciscoiq/sample/

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/ipj

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

  http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

CHAPTER 1

Overview

This chapter provides an overview of the software installation process. You can install the CAR 4.2 software on a machine for the first time, or you can upgrade the existing Cisco AR software on a workstation to CAR 4.2.

You might receive the Cisco AR software in a packaged CD-ROM or you can download the software from the Cisco.com web site. "Downloading Cisco Access Registrar Software" section on page 1-3 provides detailed information about downloading the CAR 4.2 software.

Before you install the CAR 4.2 software, you must copy a license file to the workstation where you will install the software. You will receive the license file as an e-mail attachment.
"Cisco Access Registrar 4.2 Licensing" section on page 1-4 provides detailed information about the new licensing mechanism in Cisco AR.

Note Before you begin the software installation, ensure that your server has up to date OS software including all relevant or recommended patches.

Installation Dialog Overview

You use the **pkgadd** command to install CAR 4.2 software on Solaris 9 and Solaris 10 workstations. The Linux version of CAR 4.2 uses the RedHat Package Manager (RPM) and installs as a script. When you begin the software installation, the install process uses a dialog to determine how to install the software.

Note CAR 4.2 can be used with Solaris 9, Solaris 10, or Red Hat Enterprise Linux 4.0 32-bit operating system using kernel 2.6.9-22.0.2.EL or later, and Glibc version: glibc-2.3.4-2.13 or later.

Installation Type

The first question for you to consider is the type of installation to perform. Your choices are full or configuration only. The default and most common installation type is a full install.

The Full installation installs all parts of the CAR 4.2 software including the server components, the example configuration, and the configuration utility, **aregcmd**.

The Config only installation only installs the example configuration and the configuration utility, **aregcmd**. You can use one instance of **aregcmd** to maintain other servers running the server software.

Installation Location

The next question in the installation dialog asks, "Where do you want to install?" The default location to install the software is **/opt/CSCOar**. You can choose to specify another location by entering it at this point. That directory would then be the base install directory, sometimes referred to as **$INSTALL** or **$BASEDIR**.

License File Location

The installation dialog asks for the location of the license file.

```
Access Registrar requires FLEXlm license file to operate.  A list
of space delimited license files or directories can be supplied as
input; license files must have the extension ".lic".

Where are the FLEXlm license files located? [] [?,q]
```

Cisco AR uses a licensing mechanism that requires a file to be copied from a directory on the Cisco AR workstation. Earlier versions of Cisco AR used a license key. You should copy the license file to the Cisco AR workstation before you begin the software installation. You can copy the license file to **/tmp** or another directory you might prefer. The installation process will copy the license file from the location you provide to **/opt/CSCOar/license**.

See "Cisco Access Registrar 4.2 Licensing" section on page 1-4 for more detailed information about the Cisco AR license file requirements.

Java 2 Runtime Environment

The installation dialog asks for the location of the Java 2 Runtime Environment (J2RE). Cisco AR provides a web-based GUI that requires J2RE version 1.4.*X* to be installed on the Cisco AR server.

```
Where is the J2RE installed?
```

If you already have a Java 2 platform installed, enter the directory where it is installed. If you need the J2RE, you can download it from:

http://java.sun.com

Open Database Connectivity

The installation dialog asks for the location of the Oracle installation directory, required for Open Database Connectivity (ODBC) configuration. The installation process uses this information to set the ORACLE_HOME variable in the **/opt/CSCOar/bin/arserver** script.

If you are not using ODBC, press **Enter** to skip this step.

Note Oracle 8i client and 8g server are no longer supported in CAR 4.2. However, Oracle 9i and 10g client and Oracle 9i, 10g, and 11g servers are supported in AR4.2.

Example Configuration

The installation dialog asks if you want to install the example configuration. You can use the example configuration to learn about Cisco AR and to refer to the examples that appear later in this document.

You can delete the example configuration at any time by running the command:

/opt/CSCOar/bin/aregcmd -f /opt/CSCOar/examples/cli/delete-example-configuration.rc

Base Directory

The installation process asks "where do you want to install [/opt/CSCOar]?"

If the base directory does not exist, the installation process asks if you want to create the selected base directory.

```
The selected base directory </opt/CSCOar> must exist before
installation is attempted.

Do you want this directory created now [y,n,?,q]
```

The base directory must be created before you can install the software. If you do not agree to create the base directory at this point, the installation process terminates and no changes are made to the system. The default base directory is **/opt/CSCOar**.

setuid and setgid Permissions

The installation process asks before installing the following files with setuid and setgid permissions:

- **/opt/CSCOar/.system/screen <setuid root>**
- **/opt/CSCOar/bin/aregcmd <setgid staff>**
- **/opt/CSCOar/bin/radclient <setgid staff>**

If you do not agree to install these files, the installation will continue, but you will only be able to run **aregcmd** as user **root**. Cisco recommends that you answer **Yes** to this question.

Continue with Installation

The final question asked by the installation process dialog is, "Do you want to continue with the installation of <CSCOar>?" Enter **Y** or **yes** to continue with the installation. No further user input is required.

Downloading Cisco Access Registrar Software

Cisco AR software is available for download from **http://www.cisco.com** at the following URL:

http://www.cisco.com/cgi-bin/tablebuild.pl/access-registrar-encrypted?sort=release

The page at this URL lists all available versions of Cisco AR software available for download. The current versions are:

- **CSCOar-4.2.1-sol9-k9.tar.gz** for Solaris 9

- **CSCOar-4.2.1-sol10-k9.tar.gz** for Solaris 10
- **CSCOar-4.2.1-lnx26-install-K9.sh** for RedHat Enterprise Linux (RHEL) 4.0

Complete the following steps to download the software.

Step 1 Create a temporary directory, such as **/tmp**, to hold the downloaded software package.

Step 2 Enter the URL to the Cisco.com web site for Cisco AR software:

http://www.cisco.com/cgi-bin/tablebuild.pl/access-registrar-encrypted?sort=release

Step 3 Click on the link for Cisco AR software:

CSCOar-4.2.1-sol9-k9.tar.gz for the Solaris 9 version, or
CSCOar-4.2.1-sol10-k9.tar.gz for the Solaris 10 version, or
CSCOar-4.2.1-lnx26-install-K9.sh for the RedHat Enterprise Linux version**.**

The Software Center Download Rules page displays. You should read these rules carefully.

Warning **Before downloading this software please ensure that each of the following licenses and agreements are in place with Cisco Systems or a Cisco Systems authorized reseller.**

These rules require you to acknowledge the following:

- A software license
- A valid service agreement

By clicking **Agree**, you confirm that the download of this file by you is in accordance with the requirements listed and that you understand and agree that Cisco Systems reserves the right to charge you for, and you agree to pay for, any software downloads to which you are not entitled. All Cisco Systems Operating System and application software licenses and downloads are governed by Cisco Systems' applicable End User License Agreement/Software License Agreement. By clicking **Agree** you further agree to abide by the terms and conditions set forth in Cisco Systems' End User License agreement/Software License Agreement and your service agreement.

If you click Agree, the End User License Agreement / Software License Agreement displays.

Step 4 Read the End User License Agreement / Software License Agreement carefully, and if you accept the terms, click **Accept**.

The software Download page appears. In few seconds, a File Download dialog box appears. If it does not appear, click the link provided in the page.

Step 5 Click **Save** and indicate where to save the file on your computer, such as **/tmp**, then click **Save** again.

Cisco Access Registrar 4.2 Licensing

CAR 4.2 uses a new licensing mechanism that enables you to activate all features in Cisco AR. During system initialization, the Cisco AR server sets up the licensing data model and activates all features.

In CAR 4.2, licensing is based on transactions per second(TPS). Every license will cover all features, but with restrictions enforced on the TPS. TPS is calculated based on the number of packets flowing into CAR irrespective of the feature.

CAR can be deployed in a two-tier architecture—front-end and back-end server. The front-end server performs AAA functions and it needs the base license and the TPS license. The back-end server performs session management functions and it needs the secondary license.

CAR can be deployed in an active/stand-by server combination (with Sun clustering solution). Active server performs all the functionality and it needs the base license and the TPS license. Only if the active server goes down, sun cluster will trigger the stand-by server. The stand-by server needs secondary license.

License Slabs

The license slabs available in CAR 4.2 are listed in Table 1.

Table 1 CAR 4.2 License Slabs

Product	Description
AR-4.2-BASE-K9=	CAR base license. Limited to 100 transactions per second.
AR-4.2-100TPS=	CAR additional license per server. Limited to 100 transactions per second.
AR-4.2-200TPS=	CAR additional license per server. Limited to 200 transactions per second.
AR-4.2-500TPS=	CAR additional license per server. Limited to 500 transactions per second.
AR-4.2-1000TPS=	CAR additional license per server. Limited to 1,000 transactions per second.
AR-4.2-2000TPS=	CAR additional license per server. Limited to 2,000 transactions per second.
AR-4.2-3000TPS=	CAR additional license per server. Limited to 3,000 transactions per second.
AR-4.2-5000TPS=	CAR additional license per server. Limited to 5,000 transactions per second.
AR-4.2-SECONDARY=	CAR secondary license. Required for each secondary server—back-end or stand-by.
AR-4.2-UP-3.X-K9=	CAR upgrade license for R3.x Customers, with or without SAS contract. Limited to 1000 transactions per second.
AR-4.2-UP-4.X-K9=	CAR upgrade license for R4.0 and R4.1 Customers, without SAS contract. Limited to 1000 transactions per second.

Getting Cisco Access Registrar 4.2 License

When you order the CAR 4.2 product, a text license file will be sent to you in e-mail. If you are evaluating the software, Cisco will provide you with an evaluation license.

If you decide to upgrade your Cisco AR software, a new text license file will be sent to you in e-mail.

Note While upgrading, the licenses of previous versions cannot be used with CAR 4.2. Backward compatability support in terms of license will not be available in this version.

If you receive a Software License Claim Certificate, you can get your Cisco AR license file at one of the two following URLs:

- www.cisco.com/go/license

  Use this site if you are a registered user of Cisco Connection Online.

- www.cisco.com/go/license/public

  Use this site if you are not a registered user of Cisco Connection Online.

Within one hour of registration at either of the above web sites, you will receive your license key file and installation instructions in e-mail.

Installing Cisco Access Registrar 4.2 Licenses

You must have a license in a directory on the Cisco AR machine before you attempt to install Cisco AR software. If you have not installed the Cisco AR license file before beginning the software installation, the installation process will fail.

You can store the Cisco AR license file in any directory on the Cisco AR machine. During the installation process, you will be asked the location of the license file, and the installation process will copy the license file to the **/opt/CSCOar/license** directory, or **$INSTALL/license** if you are not using the default installation location.

The license file might have the name **ciscoar.lic**, but it can be any filename with the suffix **.lic**. To install the Cisco AR license file, you can copy and paste the text into a file, or you can simply save the file you receive in e-mail to an accessible directory.

Adding Additional Cisco Access Registrar 4.2 Licenses

If you add additional licenses, you can open the file in **/opt/CSCOar/license** and add additional lines to the license file, or you can create an additional license file to hold the new lines. If you add a new file, remember to give it a **.lic** suffix. You must restart the Cisco AR server for the new license to take effect. To restart the Cisco AR server, enter the following on the server command line:

/opt/CSCOar/bin/arserver restart

Sample License File

The following is an example of a CAR 4.2 license file.

```
INCREMENT AR-BASE-100TPS cisco 4.2 30-nov-2008 uncounted
        HOSTID=ANY \
        NOTICE="<LicFileID>2008090307</LicFileID><LicLineID>0</LicLineID> \
        <PAK>dummyPak</PAK>" SIGN=ABCDEF123456
INCREMENT AR-ADD-TPS cisco 4.2 30-nov-2008 uncounted \
        VENDOR_STRING=<count>100</count> HOSTID=ANY \
        NOTICE="<LicFileID>2008090307</LicFileID><LicLineID>1</LicLineID> \
        <PAK>dummyPak</PAK>" SIGN=ABCDEF123456
```

Displaying License Information

Cisco AR provides two ways of getting license information using **aregcmd**:

- **aregcmd** command-line option
- Launching **aregcmd**

aregcmd Command-Line Option

Cisco AR provides a new **-l** command-line option to **aregcmd**. The syntax is:

aregcmd -l directory_name

where *directory_name* is the directory where the Cisco AR license file is stored. The following is an example of the **aregcmd -l** command:

```
aregcmd -l /opt/CSCOar/license
Licensed Application: Cisco Access Registrar (Standard Version)

 Following are the licensed components:

                              NAME     VERSION          EXPIRY_INFO       COUNT
                              ====     =======          ===========       =====
                    AR-Base-100TPS         4.2          30-Nov-2008         100
                        AR-ADD-TPS         4.2          30-Nov-2008         100
```

Launching aregcmd

The Cisco AR server displays license information when you launch **aregcmd**, as shown in the following:

aregcmd

```
Cisco Access Registrar 4.2.1 Configuration Utility
Copyright (C) 1995-2008 by Cisco Systems, Inc.  All rights reserved.
Logging in to localhost

[ //localhost ]
    LicenseInfo = AR-Base-100TPS 4.2 (expires on 30-Nov-2008)
                  AR-ADD-TPS 4.2 (expires on 30-Nov-2008)
    Radius/
    Administrators/

Server 'Radius' is Running, its health is 10 out of 10
```

CHAPTER 2

Installing Cisco Access Registrar 4.2

This chapter provides information about installing CAR 4.2 software. The software is available in CD-ROM form and can also be downloaded from the Cisco.com website. The installation instructions differ slightly depending on whether you install the software from the Cisco AR CD-ROM or from downloaded software.

Note CAR 4.2 can be used with Solaris 9, Solaris 10, or the Red Hat Enterprise Linux 4.0 32-bit operating system using kernel 2.6.9-22.0.2.EL or later, and Glibc version: glibc-2.3.4-2.13 or later.

This chapter contains the following sections:

Installing the Cisco Access Registrar 4.2 License File

You must have a license file in a directory on the Cisco AR machine before you attempt to install Cisco AR software. After purchasing Cisco AR, you will receive a license file in an e-mail attachment. Save or copy this license file to a directory on the Cisco AR workstation. If you have not installed the Cisco AR license file before beginning the software installation, the installation process will fail.

You can store the Cisco AR license file in any directory on the Cisco AR machine. During the installation process, you will be asked the location of the license file, and the installation process will copy the license file to the **/opt/CSCOar/license** directory or to the base installation directory you specify when you install the software if you are not using the default installation location.

The license file might have the name **ciscoar.lic**, but it can be any filename with the suffix **.lic**. To install the Cisco AR license file, you can copy and paste the text into a file, or you can simply save the file you receive in e-mail to an accessible directory.

Installing Cisco Access Registrar 4.2 Software on Solaris

This section describes the software installation process when installing Cisco AR software on a Solaris workstation for the first time.

This section includes the following subsections:

Tips Before you begin to install the software, check your workstation's **/etc/group** file and make sure that group ***staff*** exists. The software installation will fail if group staff does not exist before you begin.

Deciding Where to Install

Before you begin the software installation, you should decide where you want to install the new software. The default installation directory for CAR 4.2 software is **/opt/CSCOar**. You can use the default installation directory, or you can choose to install the Cisco AR software in a different directory.

Installing Cisco Access Registrar Software from CD-ROM

The following steps describe how to begin the software installation process when installing software from the CAR 4.2 CD-ROM. If you are installing downloaded software, proceed to Installing Downloaded Software.

Step 1 Place the Cisco AR software CD-ROM in the Cisco AR workstation CD-ROM drive.

Step 2 Log in to the Cisco AR workstation as a root user, and enter one of the following command lines:

For Solaris 9:

pkgadd -d /cdrom/cdrom0/kit/solaris-2.9 CSCOar

For Solaris 10:

pkgadd -d /cdrom/cdrom0/kit/solaris-2.10 CSCOar

Step 3 Proceed to Common Solaris Installation Steps.

Installing Downloaded Software

This section describes how to uncompress and extract downloaded Cisco AR software and begin the software installation.

Step 1 Log in to the Cisco AR workstation as a root user.

Step 2 Change directory to the location where you have stored the uncompressed tarfile.

cd /tmp

Step 3 Use the following command line to uncompress the tarfile and extract the installation package files.

zcat CSCOar-4.2.1-sol9-K9.tar.gz | tar xvf -

Note These instructions are for the Solaris 9 package. There is no difference in download or installation procedures for Solaris 9 or Solaris 10 other than the package name.

Step 4 Enter the following command to begin the installation:

pkgadd -d /tmp CSCOar

where ***/tmp*** is the temporary directory where you stored and uncompressed the installation files.

Step 5 Proceed to Common Solaris Installation Steps.

Common Solaris Installation Steps

This section describes the installation process immediately after you have issued the **pkgadd** command installing from CD-ROM or from downloaded software.

```
Processing package instance <CSCOar> from </tmp>

Cisco Access Registrar 4.2.1 [SunOS-5.9, official]
(sparc) 4.2.1
Copyright (C) 1998-2008 by Cisco Systems, Inc.
This program contains proprietary and confidential information.
All rights reserved except as may be permitted by prior written consent.

    This package contains the Access Registrar Server and the
    Access Registrar Configuration Utility.  You can choose to
    perform either a Full installation or just install the
    Configuration Utility.


What type of installation: Full, Config only [Full] [?,q]
```

Step 6 For a full install, press **Enter**.

```
Where do you want to install <CSCOar>? [/opt/CSCOar] [?,q]
```

Step 7 Press **Enter** to accept the default location of **/opt/CSCOar**, or enter a different directory to be used as the base installation directory.

```
    Access Registrar requires FLEXlm license file to operate.  A list
    of space delimited license files or directories can be supplied as
    input; license files must have the extension ".lic".

Where are the FLEXlm license files located? [] [?,q]
```

Step 8 Enter the directory where you have stored the CAR 4.2 license file.

```
    Access Registrar provides a  Web GUI. It requires J2RE version
    1.4.* to be installed on the server.

    If you already have a compatible version J2RE installed, please
    enter the directory where it is installed.  If you do not, the
    compatible J2RE version can be downloaded from:
```

```
    http://java.sun.com/

Where is the J2RE installed?  [?,q] /nfs/insbu-cnstools/java
```

The J2RE is required to use the Cisco AR GUI. If you already have a Java 2 platform installed, enter the directory where it is installed.

Note If you do not provide the J2RE path, or if the path is empty or unsupported, the installation process exits.

Step 9 Enter the directory or mount point where the J2RE is installed.

```
    If you are not using ORACLE, press Enter/Return to skip this step.
    ORACLE installation directory is required for ODBC configuration.
    ORACLE_HOME variable will be set in /etc/init.d/arserver script

Where is ORACLE installed? [] [?,q]
```

Step 10 If you plan to use Oracle accounting, enter the location where you have installed Oracle; otherwise press **Enter**.

```
    If you want to learn about Access Registrar by following the
    examples in the Installation and Configuration Guide, you need to
    populate the database with the example configuration.

Do you want to install the example configuration now [n] [y,n,?,q]
```

Step 11 When prompted whether to install the example configuration now, enter **Y** or **N** to continue.

```
    You can add the example configuration at any time by
    running the command:

    /opt/CSCOar/bin/aregcmd -f /opt/CSCOar/examples/cli/add-example-configuration.rc
```

Note You can delete the example configuration at any time by running the command **/opt/CSCOar/usrbin/aregcmd -f /opt/CSCOar/examples/cli/delete-example-configuration.rc**.

```
## Executing checkinstall script.

The selected base directory </opt/CSCOar> must exist before
installation is attempted.

Do you want this directory created now [y,n,?,q] y
```

Step 12 Enter **Y** to enable the installation process to create the **/opt/CSCOar** directory.

```
Using </opt/CSCOar> as the package base directory.
## Processing package information.
## Processing system information.
## Verifying package dependencies.
## Verifying disk space requirements.
## Checking for conflicts with packages already installed.
## Checking for setuid/setgid programs.

The following files are being installed with setuid and/or setgid
permissions:
  /opt/CSCOar/.system/screen <setuid root>
 /opt/CSCOar/bin/aregcmd <setgid staff>
 /opt/CSCOar/bin/radclient <setgid staff>
```

```
Do you want to install these as setuid/setgid files [y,n,?,q]
```

Step 13 Enter **Y** to install the **setuid/setgid** files.

```
This package contains scripts which will be executed with super-user
permission during the process of installing this package.

Do you want to continue with the installation of <CSCOar> [y,n,?]
```

Step 14 Enter **Y** to continue with the software installation.

No further interaction is required; the installation process should complete successfully and the **arservagt** is automatically started.

```
Installing Cisco Access Registrar 4.2.1 [SunOS-5.9, official] as <CSCOar>

## Installing part 1 of 1.
/opt/CSCOar/.system/add-example-config
/opt/CSCOar/.system/run-ar-scripts
/opt/CSCOar/.system/screen
/opt/CSCOar/README
/opt/CSCOar/bin/arbug
/opt/CSCOar/bin/nasmonitor
/opt/CSCOar/bin/share-access
/opt/CSCOar/bin/xtail
/opt/CSCOar/java/javadoc.tar.gz
/opt/CSCOar/lib/getopts.tcl
.
.
.
# setting up product configuration file /opt/CSCOar/conf/car.conf
# linking /etc/init.d/arserver to /etc/rc.d files
# setting ORACLE_HOME and JAVA_HOME variables in arserver
# removing old session information
# flushing old replication archive
# creating initial configuration database
Rollforward recovery using "/opt/CSCOar/data/db/vista.tjf" started Fri Nov 07 13:54:54
2008
Rollforward recovery using "/opt/CSCOar/data/db/vista.tjf" finished Fri Nov 07 13:54:54
2008

# installing example configuration
We will now generate an RSA key-pair and self-signed certificate that
may be used for test purposes
Generating a 1536 bit RSA private key
.....++++
..............++++
writing new private key to '/cisco-ar/certs/tomcat/server-key.pem'
-----
Server self-signed certificate now resides in /cisco-ar/certs/tomcat/server-cert.pem
Server private RSA key now resides in /cisco-ar/certs/tomcat/server-key.pem

Remember to install additional CA certificates for client verification
Tomcat private RSA key now resides in /cisco-ar/certs/tomcat/server-key.pem
Starting Access Registrar Server Agent...
completed.
The Radius server is now running.
# done with postinstall.

Installation of <CSCOar> was successful

hostname root /tmp##
```

Configuring SNMP

If you choose not to use the SNMP features of CAR, the installation process is completed. To use SNMP features, complete the configuration procedure described in Configuring SNMP, page 4-14.

RPC Bind Services

The Cisco AR server and the **aregcmd** CLI requires RPC services to be running before the server is started. If the RPC services are stopped, you must restart RPC services, then restart the Cisco AR server. Use the following commands to restart RPC services:

/opt/CSCOar/bin/arserver stop

/etc/init.d/rpc start

/opt/CSCOar/bin/arserver start

If RPC services are not running, the following message is displayed when you attempt to start aregcmd:

```
Login to aregcmd fails with the message:
400 Login failed
```

Installing Cisco Access Registrar on LDoms

Server virtualization is partitioning of network servers into several independent execution environments. Server virtualization allows a data center to be viewed and managed as a set of compute resources rather than a room of individual systems.

Server virtualization feature in CAR will enable maximum resource utilization with dynamic resource allocation between LDoms.

Note To know about configuration of CAR on LDoms, see White Paper under CAR Collateral in http://wwwin-nmbu.cisco.com/fieldportal/products/car/summary.cfm?Prod=car&tsession.

Installing Cisco Access Registrar 4.2 Software on Linux

This section describes the software installation process when installing Cisco AR software on a Linux workstation for the first time. This section includes the following subsections:

- Deciding Where to Install
- Installing Cisco Access Registrar Software from CD-ROM
- Common Linux Installation Steps

Tips Before you begin to install the software, check your workstation's **/etc/group** file and make sure that group ***staff*** exists. The software installation will fail if group staff does not exist before you begin.

Deciding Where to Install

Before you begin the software installation, you should decide where you want to install the new software. The default installation directory for CAR 4.2 software is **/opt/CSCOar**. You can use the default installation directory, or you can choose to install the Cisco AR software in a different directory.

Installing Cisco Access Registrar Software from CD-ROM

The following steps describe how to begin the software installation process when installing software from the CAR 4.2 CD-ROM. If you are installing downloaded software, proceed to Installing Downloaded Software.

Step 1 Place the CAR 4.2 software CD-ROM in the Cisco AR workstation CD-ROM drive.

Step 2 Log in to the Cisco AR workstation as a root user and find a temporary directory, such as **/tmp**, to store the Linux installation file.

Note The temporary directory requires at least 70 MB of free space.

Step 3 Change directory to the CD-ROM.

```
cd /cdrom/cdrom0/kit/linux-2.4
```

Step 4 Copy the **CSCOar-4.2.1-lnx26-install-K9.sh** file to the temporary directory.

```
cp CSCOar-4.2.1-lnx26-install-K9.sh /tmp
```

Step 5 Change the permissions of the CSCOar-4.1.4-lnx24-install-k9.sh file to make it executable.

```
chmod 777 CSCOar-4.2.1-lnx26-install-K9.sh
```

To continue the installation, proceed to Common Linux Installation Steps.

Common Linux Installation Steps

This section describes how to install the downloaded Cisco AR software for Linux and begin the software installation.

Note The Cisco AR Linux installation automatically installs **aregcmd** and **radclient** as setgid programs in group **adm**.

Step 1 Log in to the Cisco AR workstation as a root user.

Step 2 Change directory to the location where you have stored the **CSCOar-4.1.4-lnx26-install-K9.sh** file.

```
cd /tmp
```

Step 3 Enter the name of the script file to begin the installation:

./CSCOar-4.2.1-lnx26-install-k9.sh

```
Name        : CSCOar                       Relocations: /opt/CSCOar
Version     : 4.2.1                        Vendor: Cisco Systems, Inc.
Release     : 1140764415                    Build Date: Mon Nov 03 23:55:51 2008
Install date: (not installed)               Build Host: spencer.cnslab.cisco.com
Summary     : Access Registrar, a carrier-class RADIUS server
build_tag: [Linux-2.6.20, official]

Copyright (C) 1998-2008 by Cisco Systems, Inc.
This program contains proprietary and confidential information.
All rights reserved except as may be permitted by prior written consent.

    This package contains the Access Registrar Server and the Access
    Registrar Configuration Utility.  All the Client, Server, and
    Configuration utilities will be installed.

Where do you want to install <CSCOar>? [/opt/CSCOar] [?,q]
```

Step 4 Press **Enter** to accept the default location of **/opt/CSCOar**, or enter a different directory to be used as the base installation directory.

```
    Access Registrar requires FLEXlm license file to operate.  A list
        of space delimited license files or directories can be supplied as
        input; license files must have the extension ".lic".

    Where are the FLEXlm license files located? [] [?,q]
```

Step 5 Enter the directory where you have stored the Cisco AR license file.

```
    Access Registrar provides a Web GUI. It requires J2RE version 1.4.*
    to be installed on the server.

    If you already have a compatible version of J2RE installed, please
    enter the directory where it is installed.  If you do not, the
    compatible J2RE version can be downloaded from:

            http://java.sun.com/

    Where is the J2RE installed? [] [?,q]
```

The J2RE is required to use the CAR 4.2 GUI. If you already have a Java 2 platform installed, enter the directory where it is installed.

Note If you do not provide the J2RE path, or if the path is empty or unsupported, the installation process exits.

```
    If you are not using ORACLE, press Enter/Return to skip this step.
    ORACLE installation directory is required for ODBC configuration.
    ORACLE_HOME variable will be set in /etc/init.d/arserver script

    Where is ORACLE installed? [] [?,q]
```

Step 6 Enter the location where you have installed Oracle, otherwise press **Enter**.

```
    If you want to learn about Access Registrar by following the examples
    in the Installation and Configuration Guide, you need to populate
    the database with the example configuration.

Do you want to install the example configuration now? [n]: [y,n,?,q] y
```

Step 7 When prompted whether to install the example configuration now, enter **Y** or **N** to continue.

Note You can delete the example configuration at any time by running the command **/opt/CSCOar/usrbin/aregcmd -f /opt/CSCOar/examples/cli/delete-example-configuration.rc**.

```
unpack the rpm file done
Preparing...                ########################################### [100%]
   1:CSCOarui-add           ########################################### [100%]
Archive:  ./jakarta-tomcat-4.0.6.zip
   creating: /opt/CSCOar/jakarta-tomcat-4.0.6/bin/
  inflating: /opt/CSCOar/jakarta-tomcat-4.0.6/bin/bootstrap.jar
  inflating: /opt/CSCOar/jakarta-tomcat-4.0.6/bin/catalina.bat
  inflating: /opt/CSCOar/jakarta-tomcat-4.0.6/bin/catalina.sh
  inflating: /opt/CSCOar/jakarta-tomcat-4.0.6/bin/cpappend.bat
  inflating: /opt/CSCOar/jakarta-tomcat-4.0.6/bin/digest.bat
  inflating: /opt/CSCOar/jakarta-tomcat-4.0.6/bin/digest.sh
  inflating: /opt/CSCOar/jakarta-tomcat-4.0.6/bin/jasper.bat
  inflating: /opt/CSCOar/jakarta-tomcat-4.0.6/bin/jasper.sh
.
.
.
Rollforward recovery using "/opt/CSCOar/data/db/vista.tjf" finished Fri Nov 07 15:30:40
2008

# add-example-config y
calling gen-tomcat
We will now generate an RSA key-pair and self-signed certificate that
may be used for test purposes
Generating a 1536 bit RSA private key
.....................++++
.......................................++++
writing new private key to '/cisco-ar/certs/tomcat/server-key.pem'
-----
Server self-signed certificate now resides in /cisco-ar/certs/tomcat/server-cert.pem
Server private RSA key now resides in /cisco-ar/certs/tomcat/server-key.pem

Remember to install additional CA certificates for client verification
Tomcat private RSA key now resides in /cisco-ar/certs/tomcat/server-key.pem
Starting Access Registrar Server Agent..completed.
The Radius server is now running.

hostname root /tmp###
```

Configuring SNMP

If you choose not to use the SNMP features of Cisco AR, the installation process is completed. To use SNMP features, complete the configuration procedure described in Configuring SNMP, page 4-14.

CHAPTER 3

Upgrading Cisco Access Registrar Software

CAR 4.2 supports software upgrades from your previously installed Cisco AR software while preserving your existing configuration database. Cisco AR supports an upgrade path for both the Solaris or Linux versions of Cisco AR software.

Note Configuration for Prepaid billing servers in Cisco AR 3.0 will no longer work in CAR 4.2. If you have been using a Prepaid billing server in Cisco AR 3.0 and are upgrading your software to CAR 4.2, you must remove the Prepaid billing server configuration before installing the CAR 4.2 software. Chapter 15, "Using Prepaid Billing," provides detailed instructions for configuring Prepaid billing services for CAR 4.2.

Caution Running the command **mcdadmin -coi** to import configuration data will cause the CAR 4.2 server to lose all session information.

This chapter contains the following sections:

Solaris Software Upgrade Overview

This section describes the Solaris upgrade processes.

Step 1 Ensure that replication is disabled.

See Disabling Replication.

Step 2 If you have modified the **snmpd.conf** file in the **/cisco-ar/ucd-snmp/share/snmp** directory, you must back up this file before doing the upgrade process. The **pkgrm** removes the **snmpd.conf** file, even if it has been modified.

Step 3 Remove the old software using the **pkgrm** command.

See Using pkgrm to Remove Cisco Access Registrar Solaris Software.

Step 4 If you plan to use the Cisco AR SNMP features, disable the current Sun SNMP daemon and prevent the Sun SNMP daemon from restarting after a reboot.

Step 5 Decide where to install the CAR 4.2 software.

Step 6 Decide if you want to preserve your existing configuration database.

Preserving your existing configuration database is a compelling reason to upgrade rather than to start anew. The upgrade procedure in this chapter assumes you want to preserve your existing configuration.

If you are upgrading from Cisco AR 1.7 or an earlier version, the default installation directory is **/opt/AICar1**. The default installation directory for Cisco AR is **/opt/CSCOar**.

If your previous install directory was **/opt/AICar1**, you should use that directory to install CAR 4.2 You might also rename the old directory, as in the following:

```
cd /opt

mv AICar1  CSCOar
```

Step 7 Copy the CAR 4.2 license file to a location on the Cisco AR workstation directory such as **/tmp**.

For detailed information about the Cisco AR license and how to install the license, see Cisco Access Registrar 4.2 Licensing.

Step 8 Use the **pkgadd** command to install the CAR 4.2 software.

For detailed information about using the **pkgadd** command to install Cisco AR software, see Chapter 2, “Installing Cisco Access Registrar 4.2 Software on Solaris.”

Note Since you are upgrading, you will want to preserve your existing database.

Step 9 If you configured Cisco AR to use SNMP prior to upgrading, after installing CAR 4.2 software, you must copy the **snmpd.conf** file back to the **/cisco-ar/ucd-snmp/share/snmp** directory.

Step 10 Restart the Cisco AR server using the following command:

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

Linux Software Upgrade Overview

This section provides overview information of the Linux upgrade processes.

Step 1 Ensure that replication is disabled.

See Disabling Replication.

Step 2 If you have modified the **snmpd.conf** file in the **/cisco-ar/ucd-snmp/share/snmp** directory, you must back up this file before doing the upgrade process. The **pkgrm** removes the **snmpd.conf** file, even if it has been modified.

Note If you currently use the 3.5.2 Linux version, the **uninstall-ar** program removes **/opt/CSCOar/data**. Before you run the **uninstall-ar** program, copy the **/opt/CSCOar/data** directory to a temporary location such as **/tmp**. After you install the upgrade software, move the data directory back to **/opt/CSCOar/data**.

Step 3 Remove the old software using the **uninstall-ar** command.

For detailed information about using the **uninstall-ar** command to remove Cisco AR Linux software, see Using uninstall-ar to Remove Linux Software.

Step 4 If you plan to use the Cisco AR SNMP features, disable the current SNMP daemon and prevent the SNMP daemon from restarting after a reboot.

Step 5 Decide where to install the CAR 4.2 software.

The default installation directory for CAR 4.2 software is **/opt/CSCOar**.

Step 6 Decide if you want to preserve your existing configuration database.

Preserving your existing configuration database is a compelling reason to upgrade rather than to start anew. The upgrade procedure in this chapter assumes you want to preserve your existing configuration.

Step 7 Copy the CAR 4.2 license file to a location on the Cisco AR workstation directory such as **/tmp**.

Step 8 Install the Linux version of CAR 4.2 software.

Step 9 If you configured Cisco AR to use SNMP prior to upgrading, after installing CAR 4.2 software, you must copy the **snmpd.conf** file back to the **/cisco-ar/ucd-snmp/share/snmp** directory.

Step 10 Restart the Cisco AR server using the following command:

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

Software Upgrade Tasks

This section provides information about the tasks involved in the Cisco AR software upgrade process.

Disabling Replication

If you are using the Cisco AR replication feature, you must disable it before you begin the upgrade process of the upgrade will fail. When completed, see "Restarting Replication" section on page 3-19 for the correct way to restart replication.

To ensure that replication is disabled, complete the following steps:

Step 1 Login as admin and launch **aregcmd**.

Step 2 Change directory to /radius/replication and examine the RepType property.

```
cd /radius/replication
```

```
[ //localhost/Radius/Replication ]
RepType = None
RepTransactionSyncInterval = 60000
RepTransactionArchiveLimit = 100
RepIPAddress = 0.0.0.0
RepPort = 1645
RepSecret = NotSet
RepIsMaster = FALSE
RepMasterIPAddress = 0.0.0.0
RepMasterPort = 1645
Rep Members/
```

Make sure that RepType is set to None.

Step 3 If you made changes, issue the **save** command, then exit the **aregcmd** command interface.

Using pkgrm to Remove Cisco Access Registrar Solaris Software

There are two different Cisco AR Solaris software packages, **AICar1** and **CSCOar**. The **AICar1** package was used for Cisco AR 1.7 and earlier versions. The **CSCOar** package has been used for Cisco AR 3.0 and later versions.

Removing the AICar1 Package

The following steps describe how to remove the **AICar1** software package.

Step 1 Log in to the Cisco AR workstation as a root user, and enter the following command line:

pkgrm AICar1

```
The following package is currently installed:
   AICar1          Access Registrar 1.7R7 [SunOS-5.8, ns40, gcc-O, official]
                   (sparc) 1.7R7

Do you want to remove this package?
```

Step 2 Enter **y** or **yes** to continue removing the AICar1 package.

```
## Removing installed package instance <AICar1>

This package contains scripts which will be executed with super-user
permission during the process of removing this package.

Do you want to continue with the removal of this package [y,n,?,q]
```

Step 3 Enter **y** to continue removing the AICar1 package.

After you enter **y**, the AICar1 package should be removed without further interaction.

```
## Verifying package dependencies.
## Processing package information.
## Executing preremove script.
Waiting for these processes to die (this may take some time):
  AR MCD lock manager  (pid: 2971)
  AR MCD server        (pid: 2967)
  AR RADIUS server     (pid: 2973)
  AR Server Agent      (pid: 2965)
2967: terminated
```

```
2973: terminated
2971: terminated, wait status 0x000f
2965: terminated

Access Registrar Server Agent shutdown complete.
# removing /etc/rc.d files
# done with preremove.
## Removing pathnames in class <snmp>
/opt/AICar1/ucd-snmp/share/snmp/snmpd.conf
.
. <several hundred lines deleted>
.
/opt/AICar1/bin/screen
/opt/AICar1/bin
/opt/AICar1/README
## Removing pathnames in class <none>
## Updating system information.

Removal of <AICar1> was successful.
hostname root /scratch##
```

Removing the CSCOar Package

The following steps describe how to remove the **CSCOar** software package.

Step 1 Log in to the Cisco AR workstation as a root user, and enter the following command line:

pkgrm CSCOar

```
The following package is currently installed:
   CSCOar          Cisco Access Registrar 3.0R7 [SunOS-5.8, official]
                   (sparc) 3.0R7

Do you want to remove this package?
```

Step 2 Enter **y** or **yes** to continue removing the CSCOar package.

```
## Removing installed package instance <CSCOar>

This package contains scripts which will be executed with super-user
permission during the process of removing this package.

Do you want to continue with the removal of this package [y,n,?,q]
```

Step 3 Enter **y** to continue removing the CSCOar package.

After you enter **y**, the CSCOar package should be removed without further interaction.

```
## Verifying package dependencies.
## Processing package information.
## Executing preremove script.
Waiting for these processes to die (this may take some time):
  AR Server Agent      (pid: 28352)
  AR MCD server        (pid: 28354)
  AR RADIUS server     (pid: 28372)
  AR MCD lock manager  (pid: 28355)
28354: terminated, wait status 0x0000
28372: terminated, wait status 0x0000
28355: terminated, wait status 0x000f
28352: terminated, wait status 0x0000
```

```
Access Registrar Server Agent shutdown complete.
# removing /etc/rc.d files
# done with preremove.
## Removing pathnames in class <snmp>
/opt/CSCOar/ucd-snmp/share/snmp/snmpd.conf
/opt/CSCOar/ucd-snmp/share/snmp/snmpconf-data/snmptrapd-data/traphandle
.
.
. <several hundred lines deleted>
.
.
/opt/CSCOar/README
/opt/CSCOar/.system/screen
/opt/CSCOar/.system
## Removing pathnames in class <none>
## Updating system information.

Removal of <CSCOar> was successful.
hostname root ~##
```

Using uninstall-ar to Remove Linux Software

The Linux version of Cisco AR software includes the **uninstall-ar** program in **/opt/CSCOar/bin** that you use to remove Cisco AR software on Linux machines.

Note If you currently use the 3.5.2 Linux version, the **uninstall-ar** program removes **/opt/CSCOar/data**. Before you run the **uninstall-ar** program, copy the **/opt/CSCOar/data** directory to a temporary location such as **/tmp**. After you install the upgrade software, move the data directory back to **/opt/CSCOar/data**.

Step 1 Log in to the Cisco AR workstation as a root user.

Step 2 To remove the Linux version of Cisco AR software, change directory to **/opt/CSCOar/bin** and start the **uninstall-ar** program as follows:

cd /opt/CSCOar/bin

uninstall-ar

```
uninstall-ar
Are you sure you want to remove CSCOar-3.5.4-1101360135? [y/n]:
```

Step 3 Enter **Yes** or **Y** to continue removing the Linux software.

```
Are you sure you want to remove CSCOar-3.5.4-1101360135? [y/n]: y
Waiting for these processes to die (this may take some time):
AR RADIUS server running       (pid: 15492)
AR Server Agent running        (pid: 27288)
AR MCD lock manager running    (pid: 27295)
AR MCD server running          (pid: 27294)
```

```
4 processes left.3 processes left.......2 processes left.......k0 processes left.0
processes left

Access Registrar Server Agent shutdown complete.
```

Installing the Cisco Access Registrar License File

CAR 4.2 uses a new licensing mechanism that enables you to activate all features in Cisco AR. During system initialization, the Cisco AR server sets up the licensing data model and activates all features.

You must have a license in a directory on the Cisco AR machine before you attempt to install Cisco AR software. If you have not installed the Cisco AR license file before beginning the software installation, the installation process will fail.

You can store the Cisco AR license file in any directory on the Cisco AR machine. During the installation process, you will be asked the location of the license file, and the installation process will copy the license file to the **/opt/CSCOar/license** directory or to the base installation directory you specify when you install the software (if you are not using the default installation location).

The license file might have the name **ciscoar.lic**, but it can be any filename with the suffix **.lic**. To install the Cisco AR license file, you can copy and paste the text into a file, or you can simply save the file you receive in e-mail to an accessible directory.

Upgrading Cisco Access Registrar Solaris Software

This section describes the software installation process when installing CAR 4.2 software on a Solaris workstation for the first time. This section includes the following subsections:

Tips Before you begin to install the software, check your workstation's **/etc/group** file and make sure that group ***staff*** exists. The software installation will fail if group staff does not exist before you begin.

Note While upgrading, the licenses of previous versions cannot be used with CAR 4.2.1. Backward compatibility support in terms of license will not be available in this version.

Deciding Where to Install

Before you begin the software installation, you should decide where you want to install the new software. The default installation directory for CAR 4.2 software is **/opt/CSCOar**. You can use the default installation directory, or you can choose to install the Cisco AR software in a different directory.

Installing Cisco Access Registrar Software from CD-ROM

The following steps describe how to begin the software installation process when installing software from the CAR 4.2 CD-ROM. If you are installing downloaded software, proceed to Installing Downloaded Software.

Step 1 Place the CAR 4.2 software CD-ROM in the Cisco AR workstation CD-ROM drive.

Step 2 Log in to the Cisco AR workstation as a root user, and enter the following command line for (Solaris 9):

pkgadd -d /cdrom/cdrom0/kit/solaris-2.9 CSCOar

Step 3 Proceed to Common Solaris Installation Steps.

Installing Downloaded Software

This section describes how to uncompress and extract downloaded CAR 4.2 software and begin the software installation.

Step 1 Log in to the Cisco AR workstation as a root user.

Step 2 Change directory to the location where you have stored the uncompressed tarfile.

cd /tmp

Step 3 Use a command like the following to uncompress the tarfile and extract the installation package files.

zcat CSCOar-4.2.1-sol9-k9.tar.gz | tar xf -

Note These instructions are for the Solaris 9 package. There is no difference in download or installation procedures for Solaris 9 or Solaris 10 other than the package name.

Step 4 Enter the following command to begin the installation:

pkgadd -d /tmp CSCOar

where ***/tmp*** is the temporary directory where you stored and uncompressed the installation files.

Step 5 Proceed to Common Solaris Installation Steps.

Common Solaris Installation Steps

This section describes the installation process immediately after you have issued the **pkgadd** command installing from CD-ROM or from downloaded software.

```
Processing package instance <CSCOar> from </tmp>

Cisco Access Registrar 4.2.1 [SunOS-5.9, official]
```

```
(sparc) 4.2.1
Copyright (C) 1998-2008 by Cisco Systems, Inc.
This program contains proprietary and confidential information.
All rights reserved except as may be permitted by prior written consent.

    This package contains the Access Registrar Server and the
    Access Registrar Configuration Utility.  You can choose to
    perform either a Full installation or just install the
    Configuration Utility.

What type of installation: Full, Config only [Full] [?,q]
```

Step 1 For a full install, press **Enter**.

```
Where do you want to install <CSCOar>? [/opt/CSCOar] [?,q]
```

Step 2 Press **Enter** to accept the default location of **/opt/CSCOar**, or enter a different directory to be used as the base installation directory.

```
    Access Registrar requires FLEXlm license file to operate.  A list
    of space delimited license files or directories can be supplied as
    input; license files must have the extension ".lic".

Where are the FLEXlm license files located? [] [?,q]
```

Step 3 Enter the directory where you have stored the CAR 4.2 license file.

```
    Access Registrar provides a  Web GUI. It requires J2RE version
    1.4.* to be installed on the server.

    If you already have a compatible version J2RE installed, please
    enter the directory where it is installed.  If you do not, the
    compatible J2RE version can be downloaded from:

    http://java.sun.com/

Where is the J2RE installed?  [?,q]
```

The J2RE is required to use the Cisco AR GUI. If you already have a Java 2 platform installed, enter the directory where it is installed.

Note If you do not provide the J2RE path, or if the path is empty or unsupported, the installation process exits.

Step 4 Enter the directory or mount point where the J2RE is installed.

```
    If you are not using ORACLE, press Enter/Return to skip this step.
    ORACLE installation directory is required for ODBC configuration.
    ORACLE_HOME variable will be set in /etc/init.d/arserver script

Where is ORACLE installed? [] [?,q]
```

Step 5 If you plan to use Oracle for one of authentication, authorization, or accounting, enter the location where you have installed Oracle; otherwise press **Enter**.

```
    A local database from previous installation of the Access
    Registrar Server has been detected. It contains:

    * session information
    * all server object definitions
    * local UserLists
```

```
Do you want to preserve the local database in /opt/CSCOar [y]: [y,n,?,q] y
```

Step 6 Enter **Y** to preserve the local database.

```
The upgrade procedure needs administrator access to your
configuration so that it can upgrade it.
Enter an AR administrator username and password:

User:
```

Step 7 Enter the administrator userID and password.

```
User: admin
Password:
Retype password:

Remove old sessions in /opt/CSCOar/data/radius [n] [y,n,?,q]
```

Step 8 Press Enter to retain old sessions, or enter Y to remove them.

```
## Executing checkinstall script.

The selected base directory </opt/CSCOar> must exist before
installation is attempted.

Do you want this directory created now [y,n,?,q] y
Using </opt/CSCOar> as the package base directory.
## Processing package information.
## Processing system information.
## Verifying package dependencies.
## Verifying disk space requirements.
## Checking for conflicts with packages already installed.
## Checking for setuid/setgid programs.

The following files are being installed with setuid and/or setgid
permissions:
  /opt/CSCOar/.system/screen <setuid root>
 /opt/CSCOar/bin/aregcmd <setgid staff>
 /opt/CSCOar/bin/radclient <setgid staff>
Do you want to install these as setuid/setgid files [y,n,?,q]
```

Step 9 Enter `Y` to install the **setuid/setgid** files.

```
This package contains scripts which will be executed with super-user
permission during the process of installing this package.

Do you want to continue with the installation of <CSCOar> [y,n,?]
```

Step 10 Enter `Y` to continue with the software installation.

No further interaction is required; the installation process should complete successfully and the **arservagt** is automatically started.

```
Installing Cisco Access Registrar 4.2.1 [SunOS-5.9, official] as <CSCOar>

## Installing part 1 of 1.
/opt/CSCOar/.system/add-example-config
/opt/CSCOar/.system/run-ar-scripts
/opt/CSCOar/.system/screen
/opt/CSCOar/README
/opt/CSCOar/bin/arbug
/opt/CSCOar/bin/nasmonitor
.
.
.
```

```
inflating: /opt/CSCOar/jakarta-tomcat-4.0.6/webapps/tomcat-docs/RUNNING.txt
  inflating:
/opt/CSCOar/jakarta-tomcat-4.0.6/webapps/tomcat-docs/security-manager-howto.html
  inflating: /opt/CSCOar/jakarta-tomcat-4.0.6/webapps/tomcat-docs/ssl-howto.html
   creating: /opt/CSCOar/jakarta-tomcat-4.0.6/work/
# setting up product configuration file /opt/CSCOar/conf/car.conf
# linking /etc/init.d/arserver to /etc/rc.d files
# setting ORACLE_HOME and JAVA_HOME variables in arserver
# removing old session information
# flushing old replication archive
# creating initial configuration database
Rollforward recovery using "/opt/CSCOar/data/db/vista.tjf" started Fri Nov 07 13:54:54
2008
Rollforward recovery using "/opt/CSCOar/data/db/vista.tjf" finished Fri Nov 07 13:54:55
2008

# installing example configuration
We will now generate an RSA key-pair and self-signed certificate that
may be used for test purposes
Generating a 1536 bit RSA private key
.....++++
..............++++
writing new private key to '/cisco-ar/certs/tomcat/server-key.pem'
-----
Server self-signed certificate now resides in /cisco-ar/certs/tomcat/server-cert.pem
Server private RSA key now resides in /cisco-ar/certs/tomcat/server-key.pem

Remember to install additional CA certificates for client verification
Tomcat private RSA key now resides in /cisco-ar/certs/tomcat/server-key.pem
Starting Access Registrar Server Agent..
completed.
The Radius server is now running.
# done with postinstall.

Installation of <CSCOar> was successful.
hostname root /tmp##
```

Configuring SNMP

If you choose not to use the SNMP features of CAR, the installation process is completed. To use SNMP features, complete the configuration procedure described in Configuring SNMP.

Back-up Copy of Original Configuration

The upgrade process displays a message like the following to indicate where a copy of your original configuration has been stored.

Note Running the command **mcdadmin -coi** to import configuration data will cause the CAR 4.2 server to lose all session information.

Note Configuration files like the tcl script files are replaced with a new one. Hence, before upgrading, backup the existing file to prevent any loss of data. After upgrading, replace the /opt/CSCOar/scripts/radius/tcl/tclscript.tcl with the backup file.

```
################################################################
#
#  A backup copy of your original configuration has been
#  saved to the file:
#
#    /opt/CSCOar/temp/10062.origconfig-backup
#
#  If you need to restore the original configuration,
#  enter the following command:
#
#    mcdadmin -coi /opt/CSCOar/temp/10062.origconfig-backup
#
################################################################
```

Removing Old VSA Names

The upgrade process provides an analysis of the configuration database, addition of new database elements, and a search for obsolete VSA names. When this is complete, a message like the following is displayed:

```
############################################################
#
#   Sometimes VSAs get renamed from version to version of AR.
#   The upgrade process does not automatically remove the
#   old names. The upgrade process has generated a script
#   to remove the old names. The script is located in:
#
#       /opt/CSCOar/temp/10062.manual-deletes
#
#   Review the script to make sure you are not using any of
#   these old VSAs. Modify your configuration and your
#   scripts to use the new names before you attempt to run
#   the script.
#
#   To run the removal script, type:
#
#       aregcmd -sf /opt/CSCOar/temp/10062.manual-deletes
#
############################################################
```

At this point, you should examine the script produced by the upgrade process to make sure that your site is not using any of the old VSAs. In the example above, the script can be found at **/opt/CSCOar/temp/10062.manual-deletes**.

Note The number preceding **manual.deletes** is produced from the PID of the upgrade process.

Modify your configuration and your scripts to use the new names before you attempt to run the script generated by the upgrade process.

VSA Update Script

The upgrade process builds a script you can use to update VSAs in your system.

```
############################################################
#
#   VSAs for the old AR version are not updated
#   automatically. The upgrade process generated a script
```

```
#   to perform the update. The script is located in:
#
#       /opt/CSCOar/temp/10062.manual-changes
#
#   Review the script to make sure it does not conflict with
#   any of your VSA changes. Make sure you modify the script,
#   if necessary, before you attempt to run it.
#
#   To run the update script, type:
#
#       aregcmd -sf /opt/CSCOar/temp/10062.manual-changes
#
################################################################
```

Step 11 Review the script and make sure that the changes it will make do not conflict with any changes you might have made to the VSAs. Modify the script if necessary.

Step 12 Record the location of the upgrade messages for future reference.

```
################################################################
#
#  These upgrade messages are saved in:
#
#      /opt/CSCOar/temp/10062.upgrade-log
#
################################################################
```

Upgrading Cisco Access Registrar Linux Software

This section describes the software installation process when upgrading to CAR 4.2 software on a Linux workstation. This section includes the following subsections:

Using uninstall-ar to Remove Linux Software

The Linux version of Cisco AR software includes the **uninstall-ar** program in **/opt/CSCOar/bin** that you use to remove Cisco AR software on Linux machines.

Note If you currently use the 3.5.2 Linux version, the **uninstall-ar** program removes **/opt/CSCOar/data**. Before you run the **uninstall-ar** program, copy the **/opt/CSCOar/data** directory to a temporary location such as **/tmp**. After you install the upgrade software, move the data directory back to **/opt/CSCOar/data**.

Step 1 Log in to the Cisco AR workstation as a root user.

Step 2 To remove the Linux version of Cisco AR software, change directory to **/opt/CSCOar/bin** and stop the server.

cd /opt/CSCOar/bin

arserver stop

```
Waiting for these processes to die (this may take some time):
AR RADIUS server running       (pid: 1403)
AR Server Agent running        (pid: 29310)
AR MCD lock manager running    (pid: 29320)
AR MCD server running          (pid: 29317)
AR GUI running                 (pid: 29441)
5 processes left.2 processes left.0 processes left

Access Registrar Server Agent shutdown complete.
```

Step 3 Run the **uninstall-ar** program as shown below:

uninstall-ar

```
Are you sure you want to remove CSCOar-3.5.4-1101360135? [y/n]:
```

Step 4 Enter **Yes** or **Y** to continue removing the Linux software.

```
Are you sure you want to remove CSCOar-3.5.4-1101360135? [y/n]: y
Nothing running, no need to shutdown.
host root bin###
```

Deciding Where to Install

Before you begin the software installation, you should decide where you want to install the new software. The default installation directory for CAR 4.2 software is **/opt/CSCOar**. You can use the default installation directory, or you can choose to install the Cisco AR software in a different directory.

Installing Cisco Access Registrar Software from CD-ROM

The following steps describe how to begin the software installation process when installing software from the CAR 4.2 CD-ROM. If you are installing downloaded software, proceed to Installing Downloaded Software.

Step 1 Place the CAR 4.2 software CD-ROM in the Cisco AR workstation CD-ROM drive.

Step 2 Log in to the Cisco AR workstation as a root user and find a temporary directory, such as **/tmp**, to store the Linux installation file.

Note The temporary directory requires at least 1GB of free space.

Step 3 Change directory to the CD-ROM.

cd /cdrom/cdrom0/kit/linux-2.6

Step 4 Copy the **CSCOar-4.2.1-lnx26-install-k9.sh** file to the temporary directory.

cp CSCOar-4.2.1-lnx26-install-k9.sh /tmp

Step 5 Change the permissions of the CSCOar-4.2.1-lnx26-install-k9.sh file to make it executable.

chmod 777 CSCOar-4.2.1-lnx26-install-k9.sh

To continue the installation, proceed to Common Linux Installation Steps.

Common Linux Installation Steps

This section describes how to install the downloaded CAR 4.2 software for Linux and begin the software installation.

Note The Cisco AR Linux installation automatically installs **aregcmd** and **radclient** as setgid programs in group **adm**.

Step 1 Log in to the Cisco AR workstation as a root user.

Step 2 Change directory to the location where you have stored the **CSCOar-4.2.1-lnx26-install-K9.sh** file.

cd /tmp

Step 3 Enter the name of the script file to begin the installation:

CSCOar-4.2.1-lnx26-install-K9.sh

```
Name        : CSCOar                       Relocations: /opt/CSCOar
Version     : 4.2.1                        Vendor: Cisco Systems, Inc.
Release     : 1140764415                    Build Date: Fri Nov 07 23:55:51 2008
Install date: (not installed)               Build Host: donald.cnslab.cisco.com
Summary     : Access Registrar, a carrier-class RADIUS server
build_tag: [Linux-2.6.20, official]

Copyright (C) 1998-2008 by Cisco Systems, Inc.
This program contains proprietary and confidential information.
All rights reserved except as may be permitted by prior written consent.

    This package contains the Access Registrar Server and the Access
    Registrar Configuration Utility.  All the Client, Server, and
    Configuration utilities will be installed.

Where do you want to install <CSCOar>? [/opt/CSCOar] [?,q]
```

Step 4 Press **Enter** to accept the default location of **/opt/CSCOar**, or enter a different directory to be used as the base installation directory.

```
    Access Registrar requires FLEXlm license file to operate.  A list
    of space delimited license files or directories can be supplied as
    input; license files must have the extension ".lic".

    Existing license files found.  To use the existing license files,
    just press ENTER to the prompt below.

    Note: To enable other features within this package, additional FLEXlm
    license files can be specified below.

Where are the FLEXlm license files located? [/opt/CSCOar/license] [?,q]
```

Step 5 Enter the directory where you have stored the CAR 4.2 license file.

```
    Access Registrar provides a Web GUI. It requires J2RE version 1.4.*
    to be installed on the server.

    If you already have a compatible version of J2RE installed, please
    enter the directory where it is installed.  If you do not, the
    compatible J2RE version can be downloaded from:

        http://java.sun.com/

    Where is the J2RE installed? [] [?,q]
```

The J2RE is required to use the Cisco AR GUI. If you already have a Java 2 platform installed, enter the directory where it is installed.

Note If you do not provide the J2RE path, or if the path is empty or unsupported, the installation process exits.

```
    If you are not using ORACLE, press Enter/Return to skip this step.
    ORACLE installation directory is required for ODBC configuration.
    ORACLE_HOME variable will be set in /etc/init.d/arserver script

Where is ORACLE installed? [] [?,q]
```

Step 6 Enter the location where you have installed Oracle, otherwise press **Enter**.

```
    A local database from previous installation of the Access
    Registrar Server has been detected. It contains:

    * session information
    * all server object definitions
    * local UserLists

Do you want to preserve the local database in /opt/CSCOar [y]: [y,n,?,q] y
```

Step 7 Enter**Y** to preserve the local database.

```
    The upgrade procedure needs administrator access to your configuration
    so that it can upgrade it.

Enter an AR administrator username and password:
```

Step 8 Enter the administrator userID and password.

```
    User: admin
    Password:
    Retype password:

    Remove old sessions in /opt/CSCOar/data/radius [n]: [y,n,?,q]
```

Step 9 Enter **Y** to remove old sessions or **N** to retain old sessions.

```
unpack the rpm file done
Preparing...                ########################################### [100%]
   1:CSCOarui-add           ########################################### [100%]
Archive:  ./jakarta-tomcat-4.0.6.zip
   creating: /opt/CSCOar/jakarta-tomcat-4.0.6/bin/
  inflating: /opt/CSCOar/jakarta-tomcat-4.0.6/bin/bootstrap.jar
  inflating: /opt/CSCOar/jakarta-tomcat-4.0.6/bin/catalina.bat
.
.
.
```

```
inflating:
/opt/CSCOar/jakarta-tomcat-4.0.6/webapps/tomcat-docs/security-manager-howto.html
  inflating: /opt/CSCOar/jakarta-tomcat-4.0.6/webapps/tomcat-docs/ssl-howto.html
   creating: /opt/CSCOar/jakarta-tomcat-4.0.6/work/
Preparing...                ########################################### [100%]
   1:CSCOar                 ########################################### [100%]
relink arserver
# flushing old replication archive
# creating initial configuration database
Rollforward recovery using "/opt/CSCOar/data/db/vista.tjf" started Thu Nov 06 11:51:29
2008
Rollforward recovery using "/opt/CSCOar/data/db/vista.tjf" finished Thu Nov 06 11:51:29
2008

# add-example-config y
JAVA ROOT /nfs/insbu-cnstools/java-linux
JAVA_HOME /nfs/insbu-cnstools/java-linux
# setting ORACLE_HOME and JAVA_HOME variable in arserver
ORACLE_HOME
JAVA_HOME /nfs/insbu-cnstools/java-linux
set JAVA_HOME
calling gen-tomcat
/cisco-ar/certs/tomcat/server-cert.pem exists, no action taken.
unable to write 'random state'
Tomcat private RSA key now resides in /cisco-ar/certs/tomcat/server-key.pem
Starting Access Registrar Server Agent..completed.
The Radius server is now running.

hostname root /tmp###
```

Backup Copy of Original Configuration

The upgrade process displays a message like the following to indicate where a copy of your original configuration has been stored.

Note Running the command **mcdadmin -coi** to import configuration data will cause the CAR 4.2 server to lose all session information.

```
#################################################################
#
#  A backup copy of your original configuration has been
#  saved to the file:
#
#    /opt/CSCOar/temp/10062.origconfig-backup
#
#  If you need to restore the original configuration,
#  enter the following command:
#
#    mcdadmin -coi /opt/CSCOar/temp/10062.origconfig-backup
#
#################################################################
```

Removing Old VSA Names

The upgrade process provides an analysis of the configuration database, addition of new database elements, and a search for obsolete VSA names. When this is complete, a message like the following is displayed:

```
############################################################
#
#   Sometimes VSAs get renamed from version to version of AR.
#   The upgrade process does not automatically remove the
#   old names. The upgrade process has generated a script
#   to remove the old names. The script is located in:
#
#       /opt/CSCOar/temp/10062.manual-deletes
#
#   Review the script to make sure you are not using any of
#   these old VSAs. Modify your configuration and your
#   scripts to use the new names before you attempt to run
#   the script.
#
#   To run the removal script, type:
#
#       aregcmd -sf /opt/CSCOar/temp/10062.manual-deletes
#
############################################################
```

At this point, you should examine the script produced by the upgrade process to make sure that your site is not using any of the old VSAs. In the example above, the script can be found at **/opt/CSCOar/temp/10062.manual-deletes**.

Note The number preceding **manual.deletes** is produced from the PID of the upgrade process.

Modify your configuration and your scripts to use the new names before you attempt to run the script generated by the upgrade process.

VSA Update Script

The upgrade process builds a script you can use to update VSAs in your system.

```
############################################################
#
#   VSAs for the old AR version are not updated
#   automatically. The upgrade process generated a script
#   to perform the update. The script is located in:
#
#       /opt/CSCOar/temp/10062.manual-changes
#
#   Review the script to make sure it does not conflict with
#   any of your VSA changes. Make sure you modify the script,
#   if necessary, before you attempt to run it.
#
#   To run the update script, type:
#
#       aregcmd -sf /opt/CSCOar/temp/10062.manual-changes
#
############################################################
```

Step 10 Review the script and make sure that the changes it will make do not conflict with any changes you might have made to the VSAs. Modify the script if necessary.

Step 11 Record the location of the upgrade messages for future reference.

```
#################################################################
#
#  These upgrade messages are saved in:
#
#      /opt/CSCOar/temp/10062.upgrade-log
#
#################################################################
```

Configuring SNMP

If you choose not to use the SNMP features of CAR, the installation process is completed. To use SNMP features, complete the configuration procedure described in Configuring SNMP.

Configuring SNMP

If you choose not to use the SNMP features of CAR, the installation process is completed. To use SNMP features, complete the configuration procedure described in Configuring SNMP, page 4-14.

If you have modified the **snmpd.conf** file in the **/cisco-ar/ucd-snmp/share/snmp** directory, you must back up this file before doing the upgrade process. The **pkgrm** removes the **snmpd.conf** file, even if it has been modified.

After installing CAR 4.2 software with **pkgadd**, you must copy the **snmpd.conf** file back to the **/cisco-ar/ucd-snmp/share/snmp** directory. Restart the Cisco AR server using the following command:

/etc/init.d/arserver restart

Restarting Replication

Before you enable replication, you must first upgrade all replication slave servers to the same version of Access Registrar software as the master server. Do not enable replication on the master server until all slave servers have been upgraded.

Use the same process you used to upgrade the master server to upgrade any slave servers. If you retained your configuration on the master, retain the configuration on the slaves, too.

After the same version of Cisco AR software has been installed on all slave servers, you can enable replication on the master server again. After enabling replication on the master server, you can enable replication on each of the slave servers.

CHAPTER 4

Configuring Cisco Access Registrar 4.2

This chapter describes how to configure a site. Cisco Access Registrar 4.1 is very flexible. You can choose to configure it in many different ways. In addition, you can write scripts that can be invoked at different points during the processing of incoming requests and/or outgoing responses.

Before you can take advantage of this flexibility, it helps to configure a simple site. This chapter describes that process. It specifically describes a site that has the following characteristics:

- Uses a single user list for all of its users
- Writes all of its accounting information to a file
- Does not use session management to allocate or track dynamic resources

This chapter contains the following sections:

Using aregcmd

To configure Cisco AR, use the **aregcmd** commands, which are command-line based configuration tools. These commands allow you to set any Cisco AR configuration option, as well as, start and stop the Cisco AR RADIUS server and check its statistics.

General Command Syntax

Cisco AR stores its configuration information in a hierarchy. Using the **aregcmd** command **cd** (change directory), you can move through this information in the same manner as you would through a hierarchical file system. Or you can supply full pathnames to these commands to affect another part of the hierarchy, and thus avoid explicitly using the **cd** command to change to that part of the tree.

The **aregcmd** commands are case *insensitive*, which means that you can use upper or lowercase letters to designate elements. In addition, when you reference existing elements in the configuration, you only need to specify enough of the element's name to distinguish it from the other elements at that level. For example, instead of entering **cd Administrators**, you can enter **cd ad** if no other element at the current level begins with *ad*.

You can use CAR's command completion feature to see what commands are possible from your current directory location in the CAR server hierarchy by pressing the Tab key. You can also press the Tab key after entering a command to see which objects you might want to manage.

The **aregcmd** commands are command-line order dependent; that is, the arguments are interpreted based on their position on the command line. To indicate an empty string as a place holder on the command line, use either two single quotes ('') or two double quotes (""). In addition, if you use any arguments that contain spaces, make sure to quote the arguments.

aregcmd Commands

The **aregcmd** commands can be grouped into the following categories:

- Navigation commands—navigates within the Cisco AR hierarchy; commands include **cd**, **ls**, **pwd**, **next**, **prev**, **filter**, and **find**.
- Object commands—adds or deletes objects; commands include **add** and **delete**.
- Property commands—changes the value of properties; commands include **set**, **unset**, and **insert**.
- Server commands—manages the server; commands include **save**, **validate**, **start**, **stop**, **reload**, **status**, **stats**, and **trace**.
- Application commands—allows user access to the application; commands include **login**, **logout,** **exit**, **quit**, and **help**.
- Session management commands—queries the server about sessions, release active sessions, or count the number of sessions; commands include **query-sessions**, **release-sessions,** and **count-sessions.**.

This chapter uses only a few of the above commands to configure the Cisco AR RADIUS server. For more information about all the **aregcmd** commands, see Chapter 2, **Using the aregcmd Commands**, in the *Cisco Access Registrar User Guide*.

Configuring a Basic Site

The simplest RADIUS server configuration is a site that uses a single user list for all its users, writes its accounting information to a file, and does not use session management to allocate dynamic resources.

To configure such a site, do the following:

1. Run the **aregcmd** command on your Cisco AR machine.
2. Configure the Cisco AR RADIUS server settings, such as the server name and the server defaults.
3. Add users by copying the sample users.
4. Configure the Network Access Server(NAS) clients and proxies that communicate with Cisco AR.
5. Change profile attributes as needed.
6. Save your changes and reload your Cisco AR RADIUS server.

Running aregcmd

aregcmd is the command-line interface program used to configure the Cisco AR server. The **aregcmd** program is located in **$INSTALL/usrbin**.

Step 1 Run the **aregcmd** command:

aregcmd

Step 2 When asked for "Cluster," press **Enter**.

Step 3 Enter your administrator name and password.

When you install CAR software, the installation process creates a default administrator called **admin** with the password **aicuser**.

Changing the Administrator's Password

The administrator ID **admin** and password **aicuser** are default settings for all releases of CAR software. For security purposes, you should change the password for **admin** at your earliest convenience. To change the administrator's password, complete the following steps:

Step 1 Use the **cd** command to change to the **Administrators** level. Cisco AR displays the contents of the **Administrators** object.

cd //localhost/Administrators

Step 2 Use the **cd** command to change to **admin**:

cd admin

```
[ //localhost/Administrators ]
    Entries 1 to 1 from 1 total entries
    Current filter: <all>
    admin/
```

Step 3 Use the **set** command to change the administrator's password. You enter the password on the command line in readable form, however, Cisco AR displays it as encrypted.

The following example changes the password to `345`. You are asked to reenter it for confirmation.

set Password 345

Optionally, use the **set** command to change the description of the **admin** administrator.

set Description local

Step 4 Use the **ls** command to display the changed admin.

ls

Creating Additional Administrators

Use the **add** command to add additional administrators.

Step 1 Use the **cd** command to change to the **Administrators** level:

cd /Administrators

Step 2 Use the **add** command and specify the name of the administrator, an optional description, and a password.

The following example adds the administrator `jane`, description `testadmin`, and password `123`:

add jane testadmin 123

Step 3 Use the **ls** command to display the properties of the new administrator:

ls

Configuring the RADIUS Server

The top level of the Cisco AR RADIUS server is the Radius object itself. It specifies the name of the server and other parameters. In configuring this site, you only need to change a few of these properties.

```
[ //localhost/Radius ]
    Name = Radius
    Description =
    Version = 4.2.1
    IncomingScript~ =
    OutgoingScript~ =
    DefaultAuthenticationService~ = local-users
    DefaultAuthorizationService~ = local-users
    DefaultAccountingService~ = local-file
    DefaultSessionService~ =
    DefaultSessionManager~ = session-mgr-1
    UserLists/
    UserGroups/
    Policies/
    Clients/
    Vendors/
    Scripts/
    Services/
    SessionManagers/
    ResourceManagers/
    Profiles/
    Rules/
    Translations/
    TranslationGroups/
    RemoteServers/
    Advanced/
    Replication/
```

Checking the System-Level Defaults

Because this site does not use incoming or outgoing scripts, you do not need to change the scripts' properties (IncomingScript and OutgoingScript).

Since the default authentication and authorization properties specify a single user list, you can leave these unchanged as well (DefaultAuthenticationService and DefaultAuthorizationService). And because you have decided to use a file for accounting information, you can leave this property unchanged (DefaultAccountingService).

Session management, however, is on by default (DefaultSessionManager). As you do not want to use session management, you must disable it. Use the **set** command, enter *DefaultSessionManager*, then specify an empty string by entering a set of double quotes:

```
set DefaultSessionManager ""
```

Note When you do not want Cisco AR to monitor resources for user sessions, you should disable session management because using it affects your RADIUS server performance.

You have now configured some of the properties for the RADIUS server. The next step is to add users.

Checking the Server's Health

To check the server's health, use the **aregcmd** command **status**. The following issues decrement the server's health:

- Rejection of an Access-Request

Note One of the parameters in the calculation of the Cisco AR server's health is the percentage of responses to Access-Accepts that are rejections. In a healthy environment, the rejection percentage will be fairly low. An extremely high percentage of rejections could be an indication of a Denial of Service attack.

- Configuration errors
- Running out of memory
- Errors reading from the network
- Dropping packets that cannot be read (because the server ran out of memory)
- Errors writing to the network.

Cisco AR logs all of these conditions. Sending a successful response to any packet increments the server's health.

Selecting Ports to Use

By default, Cisco AR uses well-known ports 1645 and 1646 for TCP/IP communications. Access Registrar can be configured to use other ports, if necessary. If you add additional ports, however, Access Registrar will use the added ports and no longer use ports 1645 and 1646. These ports can still be used by adding them to the list of ports to use.

To configure Cisco AR to use ports other than the default ports, complete the following steps:

Step 1 Change directory to **/Radius/Advanced/Ports**.

cd /Radius/Advanced/Ports

```
[ //localhost/Radius/Advanced/Ports ]
    <no ports specified, will be using the well-known ports, 1645, 1646>
```

Step 2 Use the **add** command (twice) to add ports in pairs. (The **ls** is entered to show the results of the **add** command.)

add 1812

add 1813

ls

```
[ //localhost/Radius/Advanced/Ports ]
    Entries 1 to 2 from 2 total entries
    Current filter: <all>

    1812/
    1813/
```

Note After modifying Access Registrar's default ports setting, to continue using ports 1645 and 1646, you must add them to the list of ports in **/Radius/Advanced/Ports**.

Step 3 Enter the **save** and **reload** commands to affect, validate, and save your modifications to the CAR server configuration.

save

```
Validating //localhost...
Saving //localhost...
```

reload

```
Reloading Server 'Radius'...
Server 'Radius' is Running, its health is 10 out of 10
```

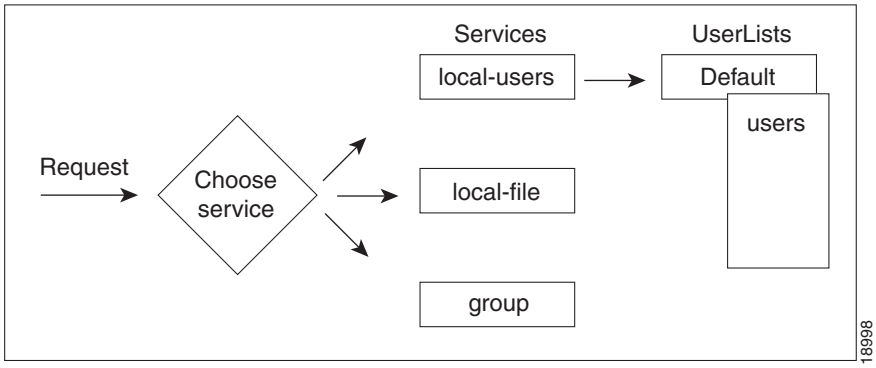
Displaying the UserLists

The first subobject in the RADIUS hierarchy that you can configure is the Userlists. The UserLists object contains all of the individual UserLists, which in turn contain the specific users.

When Cisco AR receives an Access-Request, it directs it to an authentication and/or authorization Service. If the Service has its type set to *local*, the Service looks up the user's entry in the specific **UserList**, and authenticates and/or authorizes the user.

Cisco AR, by default, specifies a Service called **local-users** that has the type **local** and uses the **Default** UserList (Figure 4-1).

Figure 4-1 Choosing Appropriate Services



Displaying the Default UserList

Step 1 Use the **cd** command to change to **UserLists/Default**:

cd /Radius/Userlists/Default

Step 2 Use the **ls -R** command to display the properties of the three users:

ls -R

Cisco AR displays the three sample users:

- `bob` who is configured as a PPP user
- `jane` who is configured as a Telnet user
- `joe` who is configured as either a PPP or Telnet user depending on how he logs in.

Adding Users to UserLists

Use the **aregcmd** command **add** to create a user under a UserList. The following lists the steps required to add a user:

Step 1 Use the **add** command to specify the name of a user and an optional description on one command line.

add jane

```
Added jane
```

Step 2 Change directory to **jane**.

cd jane

```
[ //localhost/Radius/UserLists/Default/jane ]
    Name = jane
```

```
Description =
Password = <encrypted>
Enabled = TRUE
Group~ = Telnet-users
BaseProfile~ =
AuthenticationScript~ =
AuthorizationScript~ =
UserDefined1 =
AllowNullPassword = FALSE
Attributes/
CheckItems/
```

Step 3 Use the **set** command to provide a password for user **jane**.

set password jane

```
Set Password <encrypted>
```

Note When using the **aregcmd** command, you can use the **add** command and specify all of the properties, or you can use the **add** command to create the object, and then use the **set** command and property name to set the property. For an example of using the **set** command, see the "Adding a NAS" section on page 4-9.

Deleting Users

To delete the sample users, or if you want to remove a user you have added, use the **delete** command.

From the appropriate UserList, use the **delete** command, and specify the name of the user you want to delete. For example, to delete user `beth` from the Default UserList, enter:

cd /Radius/UserLists/Default

delete beth

Displaying UserGroups

The UserGroups object contains the specific UserGroups. Specific UserGroups allow you to maintain common authentication and authorization attributes in one location, and then have users reference them. By having a central location for attributes, you can make modifications in one place instead of having to make individual changes throughout your user community.

Cisco AR has three default UserGroups:

- *Default*—uses the script **AuthorizeService** to determine the type of service to provide the user.

- *PPP-users*—uses the BaseProfile **default-PPP-users** to specify the attributes of PPP service to provide the user. The BaseProfile **default-PPP-users** contains the attributes that are added to the response dictionary as part of the authorization. For more information about Profiles, see the "Configuring Profiles" section on page 4-10.
- *Telnet-users*—uses the BaseProfile **default-Telnet-users** to specify the attributes of Telnet service to provide the user. The BaseProfile **default-Telnet-users** contains the attributes that are added to the response dictionary as part of the authorization.

For this basic site, you do not need to change these UserGroups. You can, however, use the **add** or **delete** commands to add or delete groups.

Configuring Clients

The Clients object contains all NAS and proxies that communicate directly with Cisco AR. Each client must have an entry in the Clients list, because each NAS and proxy share a secret with the RADIUS server, which is used to encrypt passwords and to sign responses.

Note If you are just testing Cisco AR with the **radclient** command, the only client you need is **localhost**. The **localhost** client is available in the sample configuration. For more information about using the **radclient** command, see the "Using radclient" section on page 4-12.

Adding a NAS

You must configure your specific NAS from both ends of the connection. That is, you must configure Cisco AR for your NAS, and you must configure your NAS for Cisco AR.

Step 1 Use the **cd** command to change to the **Clients** level:

cd /Radius/Clients

Step 2 Use the **add** command to add the NAS: `QuickExampleNAS`:

add QuickExampleNAS

Step 3 Use the **cd** command to change directory to the **QuickExampleNAS** directory:

cd /Radius/Clients/QuickExampleNAS

Step 4 Use the **set** command to specify the description `WestOffice`, the IP address `196.168.1.92`, the shared secret of `xyz`, the Type as `NAS`.

set Description WestOffice

set IPAddress 209.165.200.225

set SharedSecret xyz

set Type NAS

set Vendor USR

set IncomingScript ParseServiceHints

EnableDynamicAuthorization TRUE

EnableNotifications TRUE

The script, **ParseServiceHints**, checks the username for **%PPP** or **%SLIP**. It uses these tags to modify the request so it appears to the RADIUS server that the NAS requested that service.

Note When you are using a different NAS than the one in the example, or when you are adding NAS proprietary attributes, see the *Cisco Access Registrar User Guide* for more information about configuring Client and Vendor objects.

Configure your NAS, using your vendor's documentation. Make sure both your NAS and the Client specification have the same shared secret.

Configuring Profiles

The Profiles object allows you to set specific RFC-defined attributes that Cisco AR returns in the Access-Accept response. You can use profiles to group attributes that belong together, such as attributes that are appropriate for a particular class of PPP or Telnet user. You can reference profiles by name from either the UserGroup or the user properties. The sample users, mentioned earlier in this chapter, reference the following Cisco AR profiles:

- **default-PPP-users**—specifies the appropriate attributes for PPP service
- **default-SLIP-users**—specifies the appropriate attributes for SLIP service
- **default-Telnet-users**—specifies the appropriate attributes for Telnet service.

Setting RADIUS Attributes

When you want to set an attribute to a profile, use the following command syntax:

set <attribute> <value>

This syntax assigns a new value to the named attribute. The following example sets the attribute Service-Type to Framed:

Step 1 Use the **cd** command to change to the appropriate profile and attribute.

cd /Radius/Profiles/Default-PPP-users/Attributes

Step 2 Use the **set** command to assign a value to the named attribute.

set Service-Type Framed

When you need to set an attribute to a value that includes a space, you must double-quote the value, as in the following:

set Framed-Routing "192.168.1.0/24 192.168.1.1"

Adding Multiple Cisco AV Pairs

When you want to add multiple values to the same attribute in a profile, use the following command syntax:

set <attribute> <value1> < value2> < value3>

The AV pairs cannot be added one at a time or each subsequent command will overwrite the previous value. For example, consider the following command entry:

set Cisco-AVpair "vpdn:12tp-tunnel-password=XYZ" "vpdn:tunnel-type=12tp" "vpdn:tunnel-id=telemar" "vpdn:ip-addresses=209.165.200.225"

ls

```
Cisco-Avpair = vpdn:12tp-tunnel-password=XYZ
Cisco-Avpair = vpdn:tunnel-type=12tp
Cisco-Avpair = vpdn:tunnel-id=telemar
Cisco-Avpair = vpdn:ip-addresses=209.165.200.225
```

Note The example above is for explanation only; not all attributes and properties are listed.

Validating and Using Your Changes

After you have finished configuring your Cisco AR server, you must save your changes. Saving your changes causes Cisco AR to validate your changes and, if there were no errors, commit them to the configuration database.

Using the **save** command, however, does not automatically update your server. To update your server you must use the **reload** command. The **reload** command stops your server if it is running, and then restarts the server, which causes Cisco AR to reread the configuration database.

You must **save** and **reload** your configuration changes in order for them to take effect in the Cisco AR server.

Saving and Reloading

From anywhere in the radius object hierarchy, enter the **save** and **reload** commands.

Step 1 Use the **save** command to save your changes:

save

Step 2 Use the **reload** command to reload your server.

reload

Testing Your Configuration

Now that you have configured some users and a NAS, you are ready to test your configuration. There are two ways you can test your site:

1. You can act as a user and dial in to your NAS, and check that you can successfully log in.
2. You can run the **radclient** command, and specify one of the default users when making a request.

Using radclient

You can use the **radclient** command **simple** to create and send a packet. The following example creates an Access-Request packet for user `john` with password `john`, and the packet identifier `p001`. It displays the packet before sending it. It uses the **send** command to send the packet, which displays the response packet object identifier, `p002`. Then, the example shows how to display the contents of the response packet.

Step 1 Run the **radclient** command.

. /radclient -s

Step 2 The **radclient** command prompts you for the administrator's username and password (as defined in the Cisco AR configuration). Use **admin** for the admin name, and **aicuser** for the password.

```
Cisco Access Registrar 4.2.1 RADIUS Test Client
Copyright (C) 1995-2008 by Cisco Systems, Inc.  All rights reserved.
Logging in to localhost... done.
```

Step 3 Create a simple Access-Request packet for User-Name `john` and User-Password `john`. At the prompt, enter:

simple john john

```
p001
```

The **radclient** command displays the ID of the packet `p001`.

Step 4 Enter the packet identifier:

p001

```
Packet: code = Access-Request, id = 0, length = 0, attributes =
User-Name = john
User-Password = john
NAS-Identifier = localhost
NAS-Port = 0
```

Step 5 Send the request to the default host (**localhost**), enter:

p001 send

```
p002
```

Step 6 Enter the response identifier to display the contents of the Access-Accept packet:

p002

```
Packet: code = Access-Accept, id = 1,\
length = 38, attributes =
      Login-IP-Host = 196.168.1.94
      Login-Service = Telnet
      Login-TCP-Port = 541
```

Troubleshooting Your Configuration

If you are unable to receive an Access-Accept packet from the Cisco AR server, you can use the **aregcmd** command **trace** to troubleshoot your problem.

The **trace** command allows you to set the trace level on your server, which governs how much information the server logs about the contents of each packet. You can set the trace levels from zero to four. The system default is zero, which means that no information is logged.

Setting the Trace Level

Step 1 Run the **aregcmd** command.

aregcmd

Step 2 Use the **trace** command to set the trace level to 1-5.

trace 2

Step 3 Try dialing in again.

Step 4 Use the UNIX **tail** command to view the end of the **name_radius_1_trace** log.

host% **tail -f /opt/CSCOar/logs/name_radius_1_trace**

Step 5 Read through the log to see where the request failed.

Configuring Accounting

To configure Cisco AR to perform accounting, you must do the following:

1. Create a service
2. Set the service's type to file
3. Set the DefaultAccountingService field in **/Radius** to the name of the service you created

After you **save** and **reload** the CAR server configuration, the CAR server writes accounting messages to the **accounting.log** file in the **/opt/CSCOar/logs** directory. The CAR server stores information in the **accounting.log** file until a rollover event occurs. A rollover event is caused by the **accounting.log** file exceeding a pre-set size, a period of time transpiring, or on a scheduled date.

When the rollover event occurs, the data in **accounting.log** is stored in a file named by the prefix *accounting*, a date stamp (*yyyymmdd*), and the number of rollovers for that day. For example, **accounting-20081107-14** would be the 14th rollover on November 07, 2008.

The following shows the properties for a service called CiscoAccounting:

```
[ //localhost/Radius/Services/local-file ]
    Name = local-file
    Description =
    Type = file
    IncomingScript~ =
    OutgoingScript~ =
    OutagePolicy~ = RejectAll
    OutageScript~ =
    FilenamePrefix = accounting
    MaxFileSize = "10 Megabytes"
    MaxFileAge = "1 Day"
    RolloverSchedule =
    UseLocalTimeZone = FALSE
```

Configuring SNMP

Before you can perform SNMP configuration, you must first stop the SNMP master agent, then configure your local **snmpd.conf** file. The **snmpd.conf** file is the configuration file which defines how the CAR server's SNMP agent operates. The **snmpd.conf** file might contain any of the directives found in the DIRECTIVES section.

Enabling SNMP in the Cisco Access Registrar Server

To enable SNMP on the Cisco AR server, launch **aregcmd** and set the **/Radius/Advanced/SNMP/Enabled** property to TRUE.

aregcmd

cd /Radius/Advanced/SNMP

```
[ //localhost/Radius/Advanced/SNMP ]
    Enabled = FALSE
    TracingEnabled = FALSE
    InputQueueHighThreshold = 90
    InputQueueLowThreshold = 60
    MasterAgentEnabled = TRUE
```

set Enabled TRUE

Stopping the Master Agent

You stop the Cisco AR SNMP master agent by stopping the CAR server.

/opt/CSCOar/bin/arserver stop

Modifying the snmpd.conf File

The path to the **snmpd.conf** file is **/cisco-ar/ucd-snmp/share/snmp**. Use **vi** (or another text editor) to edit the **snmpd.conf** file.

There are three parts of this file to modify:

- Access Control
- Trap Recipient
- System Contact Information

Access Control

Access control defines who can query the system. By default, the agent responds to the ***public*** community for read-only access, if run without any configuration file in place.

The following example from the default **snmpd.conf** file shows how to configure the agent so that you can change the community names, and give yourself write access as well.

Complete the following steps to modify the **snmpd.conf** file.

Step 1 Look for the following lines in the **snmpd.conf** file for the location in the file to make modifications:

```
###############################################################################
# Access Control
###############################################################################
```

Step 2 First map the community name (COMMUNITY) into a security name that is relevant to your site, depending on where the request is coming from:

```
#       sec.name  source          community
com2sec local     localhost       private
com2sec mynetwork 10.1.9.0/24      public
```

The names are tokens that you define arbitrarily.

Step 3 Map the security names into group names:

```
#   sec.model  sec.name
group MyRWGroupv1local
group MyRWGroupv2clocal
group MyRWGroupusmlocal
group MyROGroupv1 mynetwork
group MyROGroupv2c mynetwork
group MyROGroupusmmynetwork
```

Step 4 Create a view to enable the groups to have rights:

```
#           incl/excl subtree                          mask
view all    included  .1                               80
```

Step 5 Finally, you grant the two groups access to the one view with different write permissions:

```
#               context sec.model sec.level match  read   write  notif
access MyROGroup ""      any       noauth    exact  all    none   none
access MyRWGroup ""      any       noauth    exact  all    all    none
```

Trap Recipient

The following example shows the default configuration that sets up trap recipients for SNMP versions v1 and v2c.

Note Most sites use a single NMS, not two as shown below.

```
# ------------------------------------------------------------------------------
trapcommunitytrapcom
trapsinkzubattrapcom162
trap2sinkponytatrapcom162
################################################################################
```

Note **trapsink** is used in SNMP version 1; **trap2sink** is used in SNMP version 2.

trapcommunity defines the default community string to be used when sending traps. This command must appear prior to **trapsink** or **trap2sink** which use this community string.

trapsink and **trap2sink** are defined as follows:

trapsink hostname community port

trap2sink hostname community port

System Contact Information

System contact information is provided in two variables through the **snmpd.conf** file, **syslocation** and **syscontact**.

Look for the following lines in the **snmpd.conf** file:

```
################################################################################
# System contact information
#
syslocation Your Location, A Building, 8th Floor
syscontact A. Person <someone@somewhere.org>
```

Restarting the Master Agent

You restart the CAR SNMP master agent by restarting the CAR server.

/opt/CSCOar/bin/arserver start

Configuring Dynamic DNS

Cisco AR supports the the Dynamic DNS protocol providing the ability to update DNS servers. The dynamic DNS updates contain the hostname/IP Address mapping for sessions managed by Cisco AR.

You enable dynamic DNS updates by creating and configuring new Resource Managers and new RemoteServers, both of type dynamic-dns. The dynamic-dns Resource Managers specify which zones to use for the forward and reverse zones and which Remote Servers to use for those zones. The dynamic-dns Remote Servers specify how to access the DNS Servers.

Before you configure Cisco AR you need to gather information about your DNS environment. For a given Resource Manager you must decide which forward zone you will be updating for sessions the resource manager will manage. Given that forward zone, you must determine the IP address of the primary DNS server for that zone. If the dynamic DNS updates will be protected with TSIG keys, you must find out the name and the base64 encoded value of the secret for the TSIG key. If the resource manager should also update the reverse zone (ip address to host mapping) for sessions, you will also need to determine the same information about the primary DNS server for the reverse zone (IP address and TSIG key).

If using TSIG keys, use aregcmd to create and configure the keys. You should set the key in the Remote Server or the Resource Manager, but not both. Set the key on the Remote Server if you want to use the same key for all of the zones accessed through that Remote Server. Otherwise, set the key on the Resource Manager. That key will be used only for the zone specified in the Resource Manager.

To configure Dynamic DNS, complete the following steps:

Step 1 Launch **aregcmd**.

Step 2 Create the dynamic-dns TSIG Keys:

cd /Radius/Advanced/DDNS/TSIGKeys

add foo.com

This example named the TSIG Key, **foo.com**, which is related to the name of the example DNS server we use. You should choose a name for TSIG keys that reflects the DDNS client-server pair (for example, **foo.bar** if the client is **foo** and the server is **bar**), but you should use the name of the TSIG Key as defined in the DNS server.

Step 3 Configure the TSIG Key:

cd foo.com

set Secret <base64-encoded string>

The Secret should be set to the same base64-encoded string as defined in the DNS server. If there is a second TSIG Key for the primary server of the reverse zone, follow these steps to add it, too.

Step 4 Use **aregcmd** to create and configure one or more dynamic-dns Remote Servers.

Step 5 Create the dynamic-dns remote server for the forward zone:

cd /Radius/RemoteServers

add ddns

This example named the remote server *ddns* which is the related to the remote server type. You can use any valid name for your remote server.

Step 6 Configure the dynamic-dns remote server:

cd ddns

set Protocol dynamic-dns

set IPAddress 10.10.10.1 (ip address of primary dns server for zone)

set ForwardZoneTSIGKey foo.com

set ReverseZoneTSIGKey foo.com

If the reverse zone will be updated and if the primary server for the reverse zone is different than the primary server for the forward zone, you will need to add another Remote Server. Follow the previous two steps to do so. Note that the IP Address and the TSIG Key will be different.

You can now use **aregcmd** to create and configure a resource manager of type dynamic-dns.

Step 7 Create the dynamic-dns resource manager:

cd /Radius/ResourceManagers

add ddns

This example named the service ddns which is the related to the resource manager type but you can use any valid name for your resource manager.

Step 8 Configure the dynamic-dns resource manager.

cd ddns

set Type dynamic-dns

set ForwardZone foo.com

set ForwardZoneServer DDNS

Finally, reference the new resource manager from a session manager. Assuming that the example configuration was installed, the following step will accomplish this. If you have a different session manager defined you can add it there if that is appropriate.

Step 9 Reference the resource manager from a session manager:

cd /Radius/SessionManagers/session-mgr-1/ResourceManagers

set 5 DDNS

Note The Property AllowAccountingStartToCreateSession must be set to TRUE for dynamic DNS to work.

Step 10 Save the changes you have made.

Testing Dynamic DNS with radclient

After the Resource Manager has been defined it must be referenced from the appropriate Session Manager. You can use **radclient** to confirm that dynamic DNS has been properly configured and is operational.

To test Dynamic DNS using **radclient**, follow these steps:

Step 1 Launch **aregcmd** and log in to the Cisco AR server.

cd /opt/CSCOar/bin

aregcmd

Step 2 Use the **trace** command to set the trace to level 4.

trace 4

Step 3 Launch **radclient**.

cd /opt/CSCOar/bin

radclient

Step 4 Create an Accounting-Start packet.

acct_request Start username

Example:

set p [acct_request Start bob]

Step 5 Add a Framed-IP-Address attribute to the Accounting-Start packet.

Step 6 Send the Accounting-Start packet.

$p send

Step 7 Check the **aregcmd** trace log and the DNS server to verify that the host entry was updated in both the forward and reverse zones.

CHAPTER 5

Customizing Your Configuration

After you have configured and tested a basic site, you can begin to make changes to better address your own sites's needs. This chapter provides information that describes how to:

- Use groups to select the appropriate user service
- Use multiple user lists to separate users
- Performs authentication and authorization against data from an LDAP server
- Use a script to determine which remote server to use for authentication and authorization
- Use session management to allocate and account for dynamic resources such as the number of concurrent user sessions.

The examples in this chapter provides an introduction to many of the CAR 4.2 objects and their properties. See Chapter 4, "Cisco Access Registrar Server Objects," of the Cisco Access Registrar 4.2 User's Guide for more detailed information.

Configuring Groups

The first change you might want to make is to create distinct groups based on the type of service, and divide your user community according to these groups.

You can use Cisco AR UserGroups in two ways:

- You can create separate groups for each specific type of service. For example, you can have a group for PPP users and another for Telnet users.
- You can use a default group and, depending on how the user logs in, use a script to determine which service to provide.

The default Cisco AR installation provides examples of both types of groups.

Configuring Specific Groups

For users who always require the same type of service, you can create specific user groups, and then set the user's group membership to that group.

Table 5-1 provides an overview of the process. The following sections describe the process in more detail.

Table 5-1 Configuring UserGroups

Object	Action
UserGroups	Add a new UserGroup
UserLists	Set group membership

Creating and Setting Group Membership

Step 1 Run the **aregcmd** command:

aregcmd

Step 2 Use the **cd** command to change to the **UserGroups** object.

cd /Radius/UserGroups

Step 3 Use the **add** command to create a user group, specifying the name and optional description, BaseProfile, AuthenticationScript, or AuthorizationScript. The following example shows how to add the PPP-users group.

This example sets the BaseProfile to `default-PPP-users`. When you set this property to the name of a profile, Cisco AR adds the properties in the profile to the response dictionary as part of the authorization process.

add PPP-users "Users who always connect using PPP" default-PPP-users

Step 4 Use the **cd** command to change to the user you want to include in this group. The following example shows how to change to the user, jean:

cd /Radius/UserLists/Default/jean

Step 5 Use the **set** command to set the user's group membership to the name of the group you have just created.

set group PPP-users

Step 6 Use the **save** command to save your changes.

save

Step 7 Use the **reload** command to reload the server.

reload

Note You must save whenever you have changed the configuration, either through adds, deletes, or sets. Before you exit, log out, or reload, Cisco AR prompts you to save. You must reload after all saves except when you have only made changes to individual users (either adds, deletes, or sets). Unlike all other changes, Cisco AR reads user records on demand; that is, when there is a request from that user.

Configuring a Default Group

If you allow users to request different Services based on how they specify their username, you can use a script to determine the type of Service to provide. For example, the user *joe* can request either PPP or Telnet Service by either logging in as `joe%PPP` or `joe%Telnet`.

This works because there are two scripts: **ParseServiceHints** and **AuthorizeService**.

- **ParseServiceHints**—checks the username suffix and if it corresponds to a service, it modifies the request so it appears as if the NAS requested that type of Service.
- **AuthorizeService**—adds a certain profile to the response based on the Service type. The script chooses the authentication and/or authorization Service, and the Service specifies the UserGroup which then specifies the UserList, which contains the user `joe`.

Table 5-2 provides an overview of the process. The following sections describe the process in more detail.

Table 5-2 Choosing Among UserGroups

Object	Action
UserGroups	Add a new UserGroup or use existing Default group.
	Set AuthorizationScript
Scripts	Add new Script.
UserLists	Set group membership.

Using a Script to Determine Service

The following instructions assume you have already created a UserGroup and you have written a script that performs this function. For some sample scripts, see the *Cisco Access Registrar User's Guide*.

Step 1 Use the **cd** command to change to the UserGroup you want to associate with the script. The following example changes to the **Default** group.

cd /Radius/UserGroups/Default

Step 2 Use the **set** command to set the AuthorizationScript to the name of the script you want run. The following example sets the script to **AuthorizeService**:

set AuthorizationScript AuthorizeService

Step 3 Use the **cd** command to change to **Scripts**:

cd /Radius/Scripts

Step 4 Use the **add** command to add the new script, specifying the name, description, language (in this case `Rex` which is short for RADIUS Extension), filename and an optional entry point. When you do not specify an entry point, Cisco AR uses the script's name.

add AuthorizeService "Authorization Script" Rex libAuthorizeService.so AuthorizeService

Step 5 Use the **cd** command to change to the user. The following example changes to the user `beth`:

cd /Radius/UserLists/Default/beth

Step 6 Use the **set** command to set the user's group membership to the name of that group. The following example sets `beth`'s group membership to the `Default` group.

set Group Default

Step 7 Use the **save** command to save your changes:

save

Step 8 Use the **reload** command to reload the server:

reload

Note To be able to save your changes and reload the server after following this example, you must have an actual script. Cisco AR displays a warning message when it detects missing configuration objects.

Configuring Multiple UserLists

The basic site contains a single userlist, *Default*, and uses group membership to determine the type of Service to provide each user. When all users are in the same UserList, each username must be unique.

You can, however, group your user community by department or location, and use separate UserLists to distinguish amongst them. In this case, the users names must be unique only within each UserList. Thus, you can allow a user `Jane` in the `North` UserList as well as one in the `South` UserList.

When you have more than one UserList, you must have an incoming script that Cisco AR can run in response to requests. The script chooses the authentication and/or authorization Service, and the Service specifies the actual UserList (Figure 5-1).

Figure 5-1 Using a Script to Choose a UserList

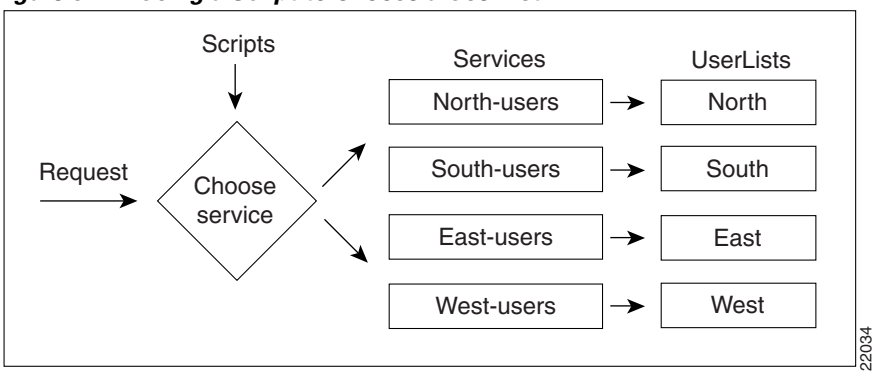


Table 5-3 provides an overview of the process. The following sections describe the process in more detail.

Table 5-3 Configuring Separate UserLists

Object	Action
UserLists	Add new UserLists.
Users	Add users.
Services	Add new Services.
	Set service type (local).
Radius	Set Incoming Script.
Scripts	Add a new Script.

Configuring Separate UserLists

Divide your site along organizational or company lines, and create a UserList for each unit.

Creating Separate UserLists

Step 1 Run the **aregcmd** command.

aregcmd

Step 2 Use the **cd** command to change to **UserLists**.

cd /Radius/UserLists

Step 3 Use the **add** command to create a UserList, specifying the name and optional description. The following example specifies the name `North` and the description `Users from the northern office`.

add North "Users from the northern office"

Step 4 Repeat for the other UserLists you want to add.

Configuring Users

After you have created multiple UserLists, you must populate them with the appropriate users.

Populating UserLists

Step 1 Use the **cd** command to change to the UserList you have created.

cd /Radius/UserLists/North

Step 2 Use the **add** command to add a user. Using the sample users as models, configure the appropriate group membership. The following example adds user `beth`, with the optional description `telemarketing`, the password `123`, Enabled set to `TRUE`, and group membership to `PPP-users`.

add beth telemarketing 123 TRUE PPP-users

Step 3 Repeat for the other users you want to add.

You can use the script, **add-100-users**, which is located in the **/opt/CSCOar/examples/cli** directory to automatically add 100 users.

Configuring Services

You must create a corresponding Service for each UserList. For example, when you create four UserLists, one for each section of the country, you must create four Services.

Creating Separate Services

Step 1 Use the **cd** command to change to **Services**:

cd /Radius/Services

Step 2 Use the **add** command to create a Service, specifying the name and optional description. The following example specifies the name `North-users` and the description `All users from the northern branch office`:

Caution **add North-users "All users from the northern branch office"**

Step 3 Use the **cd** command to change to **North-users**.

cd /Radius/Services/North-users

Step 4 Use the **set** command to set the type to *local. S*pecify the name of the UserList you want Cisco AR to use. You can accept the default Outage Policy and MultipleServersPolicy or you can use the **set** command to change them. The following example sets the type to `local` and the UserList to `North`:

set type local

set UserList North

Step 5 Repeat for each Service you must create.

Creating the Script

You must write a script that looks at the username and chooses the Service to which to direct the request.

For example, you create four UserLists (`North`, `South`, `East`, and `West`), with the Service based on the origin of the user. When a user requests a Service, your script can strip off the origin in the request and use it to set the environment dictionary variables **Authentication-Service** and/or **Authorization-Service** to the name or names of the appropriate Service.

In this situation, when `beth@North.QuickExample.com` makes an Access-Request, the script will strip off the word `North` and use it to set the value of the environment variable **Authentication-Service** and/or **Authorization-Service**. Note, the script overrides any existing default authentication and/or authorization specifications.

Note For more information about writing scripts and the role the dictionaries play in Cisco AR, see the *Cisco Access Registrar User Guide*. For examples of scripts, see the C*isco Access Registrar User's Guide.*

Client Scripting

Though, CAR allows external code (Tcl/C/C++/Java) to be used by means of a script, custom service, policy engine, and so forth, while processing request, response, or while working with the environment dictionaries, it shall not be responsible for the scripts used and will not be liable for any direct, indirect, incidental, special, exemplary, or consequential damages (including, but not limited to, procurement of substitute goods or services; loss of use, data, or profits; or business interruption) however caused and on any theory of liability, whether in contract, strict liability, or tort (including negligence or otherwise) arising in any way out of the use of the script.

Configuring the Script

When you have multiple UserLists, you need a script to determine which UserList to check when a user makes an Access-Request. When you want the script to apply to all users, irrespective of the NAS they are using, place the script at the **Radius** level. When, on the other hand, you want to run different scripts depending on the originating NAS, place the script at the **Client** level.

Client Scripting

Though, CAR allows external code (Tcl/C/C++/Java) to be used by means of a script, custom service, policy engine, and so forth, while processing request, response, or while working with the environment dictionaries, it shall not be responsible for the scripts used and will not be liable for any direct, indirect, incidental, special, exemplary, or consequential damages (including, but not limited to, procurement of substitute goods or services; loss of use, data, or profits; or business interruption) however caused and on any theory of liability, whether in contract, strict liability, or tort (including negligence or otherwise) arising in any way out of the use of the script.

Choosing the Scripting Point

Step 1 Use the **cd** command to change to the appropriate level. The following example sets the script for all requests.

cd /Radius

Step 2 Use the **set** command to set the incoming script. The following example sets the script, `ParseUserName`:

set IncomingScript ParseUserName

Step 3 Use the **cd** command to change to **Scripts**.

cd /Radius/Scripts

Step 4 Use the **add** command to add the new script, specifying the name, description, language, filename and an optional entry point. If you do not specify an entry point, Cisco AR uses the script's name.

The following example specifies the name `ParseUserName`, the language `Rex` (which is RADIUS Extension), the filename `LibParseUserName.so`, and the entry point `ParseUserName`.

add ParseUserName ""Rex libParseUserName.so ParseUserName

Step 5 Use the **save** command to save your changes:

save

Step 6 Use the **reload** command to reload the server.

reload

Handling Multiple Scripts

Cisco AR can run only one script from a given extension point. However, you can write a script that runs several scripts serially, one after the other. For example, the following **tcl** script, MasterScript, might look like the following:

```
## this MasterScript executes both tParseAAA and MyProcedure
# it assumes that tclscript.tcl and myscripts.tcl are in the same
#  directory as this file

source tclscript.tcl
source myscripts.tcl

proc MasterScript { request response environ } {
   tParseAAA $request $response $environ
   MyProcedure $request $response $environ
}
```

Save **tcl** scripts in the directory **/opt/CSCOar/scripts/radius/tcl**.

Configuring a Remote Server for AA

All the sites described so far in this chapter have used the Cisco AR RADIUS server for authentication and authorization. You might want to delegate either one or both of those tasks to another server, such as an LDAP server or another RADIUS server.

You can specify one of the following services when you want to use a particular remote server:

- radius—authentication and/or authorization
- ldap—authentication and/or authorization
- tacacs-udp—authentication only.

Note Although these services differ in the way they handle authentication and authorization, the procedure for configuring a remote server is the same independent of its type. For more information about the differences between these servers, see the *Cisco Access Registrar User Guide*.

Table 5-4 provides an overview of the process. The following sections describe the process in more detail.

Table 5-4 Configuring a Remote Server

Object	Action
RemoteServers	Add a new RemoteServer.
	Set the protocol (ldap).
	Set the properties.
Services	Add a new Service.
	Set the type (ldap).
	Set the RemoteServers property.
Radius	Set DefaultAuthentication.
	Set DefaultAuthorization.

Configuring the Remote Server

The RemoteServer object allows you to specify the properties of the remote server to which Services proxy requests. The remote servers you specify at this level are referenced by name from the RemoteServers list in the Services objects.

Creating a RemoteServer

Step 1 Run the **aregcmd** command:

aregcmd

Step 2 Use the **cd** command to change to the **RemoteServers** level:

cd /Radius/RemoteServers

Step 3 Use the **add** command to add the remote server you will reference in the Services level. The following example adds the remote server's hostname `QuickExample`.

add QuickExample

Step 4 Use the **cd** command to change to the **QuickExample RemoteServers** object level.

cd /Radius/RemoteServers/QuickExample

Step 5 Use the **set** command to specify the protocol `ldap`:

set protocol ldap

Step 6 Use the **set** command to specify the required LDAP properties.

At the very least you must specify:

- IPAddress—the IP address of the LDAP server (for example, `196.168.1.5`).
- Port—the port the LDAP server is listening on (for example, `389`).
- HostName—the hostname of the machine specified in the IP address field (for example, `ldap1.QuickExample.com`).
- SearchPath—the directory in the LDAP database to use as the starting point when searching for user information (for example, `o=Ace Industry, c=US`).
- Filter—the filter to use to find user entries in the LDAP database (for example, `(uid=%s)`).
- UserPasswordAttribute—the name of the LDAP attribute in a user entry that contains the user's password (for example, `userpassword`).
- BindName—specifies the distinguished name (DN) in the LDAP server for CAR to bind with the LDAP server (for example, `uid=admin,ou=administrators,ou=topologymanagement,o=netscaperoot`)
- BindPassword—Specifies the password for the distinguished name (for example, `cisco123`)

set IPAddress 196.168.1.5

set Port 389

set HostName ldap1.QuickExample.com

set SearchPath "o=Ace Industry, c=US"

set Filter (uid=%s)

set UserPasswordAttribute password

set BindName uid=admin,ou=administrators,ou=topologymanagement,o=netscaperoot

set BindPassword cisco123

See Table 19-1LDAP Service Properties, page 19-2 of the *Cisco Access Registrar User Guide* for descriptions of the other LDAP properties.

Configuring Services

To use LDAP for authorization and/or authentication, you must configure a Services object.

Creating Services

Step 1 Run the **aregcmd** command:

aregcmd

Step 2 Use the **cd** command to change to the **Services** level:

cd /Radius/Services

Step 3 Use the **add** command to add the appropriate LDAP service. The following example adds the `remote-ldap` service:

add remote-ldap "Remote LDAP Service"

Step 4 Use the **cd** command to change to the **remote-ldap** object:

cd /Radius/Services/remote-ldap

Step 5 Use the **set** command to set the type to `ldap`. You can accept the default Outage Policy and MultipleServersPolicy or you can use the **set** command to change them.

set type ldap

Step 6 Use the **cd** command to change to the **RemoteServers**:

cd /Radius/Services/remote-ldap/RemoteServers

Step 7 Use the **set** command to set the server number and name. By giving each server a number you tell Cisco AR the order you want it to access each server. Cisco AR uses this order when implementing the MultipleServersPolicy of Failover or RoundRobin.

The following example sets the first remote server to the server `QuickExample`:

set 1 QuickExample

The MultipleServersPolicy determines how Cisco AR handles multiple remote servers.

- When you set it to `Failover`, Cisco AR directs requests to the first server in the list until it determines the server is offline. At that time, Cisco AR redirects all requests to the next server in the list until it finds a server that is online.
- When you set it to `RoundRobin`, Cisco AR directs each request to the next server in the RemoteServers list in order to share the resource load across all the servers listed in the RemoteServers list.

Configuring the RADIUS Server

In the default Cisco AR configuration, authentication and authorization are handled through the local-users Service object. This causes Cisco AR to match requesting users with the names in its own database. When you select LDAP as a remote server for authentication and authorization, Cisco AR looks to that server for user information.

To have Cisco AR perform authentication and authorization against information from the LDAP server, you must change the DefaultAuthenticationService and DefaultAuthorizationService at the **Radius** level.

Changing the Authentication and Authorization Defaults

Step 1 Run the **aregcmd** command:

aregcmd

Step 2 Use the **cd** command to change to the **Radius** level:

cd /Radius

Step 3 Use the **set** command to change the **DefaultAuthentication**:

set DefaultAuthentication remote-ldap

Step 4 Use the **set** command to change the **DefaultAuthorization**:

set DefaultAuthorization remote-ldap

Step 5 Use the **save** command to save your changes:

save

Step 6 Use the **reload** command to reload the server:

reload

Configuring Multiple Remote Servers

All of the sites described so far in this chapter have used a single server for authentication and authorization; either the local RADIUS server or a remote LDAP server.

You can configure multiple remote servers to use the same Service, or multiple remote servers to use different Services. Figure 5-2 shows how to use multiple servers for authentication and authorization, and how to employ a script to determine which one to use.

Figure 5-2 Using a Script to Choose a Remote Server

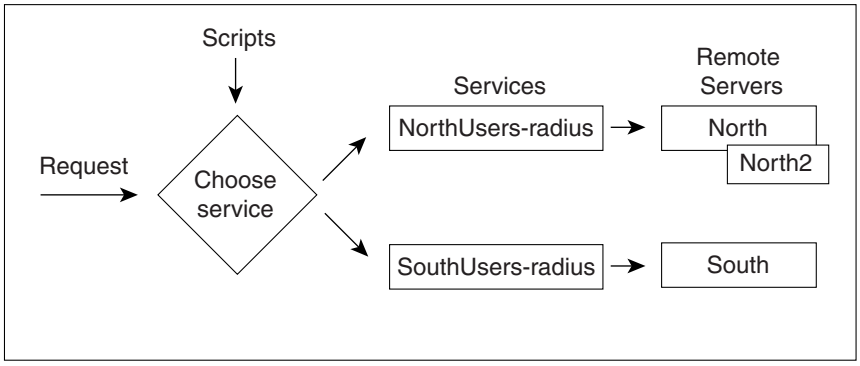


Table 5-5 provides an overview of the process. The following sections describe the process in more detail. Repeat for each RemoteServer you want to configure.

Table 5-5 Configuring Multiple Remote Servers

Object	Action
RemoteServers	Add a new RemoteServer.
	Set the protocol (radius).
	Set the shared secret.
Services	Add a new Service.
	Set the type (radius).
	Set the remote server name and number.
Scripts	Add a new Script.
Radius	Set the IncomingScript.

Configuring Two Remote Servers

Configure each remote server you want to use for authentication and authorization. The following example shows the `North` remote server.

Creating RemoteServers

Step 1 Run the **aregcmd** command:

aregcmd

Step 2 Use the **cd** command to change to the **RemoteServers** level:

cd /Radius/RemoteServers

Step 3 Use the **add** command to add the remote server you specified in the Services level. The following example adds the `North` remote server:

add North

Step 4 Use the **cd** command to change to the **North RemoteServers** level:

cd /Radius/RemoteServers/North

Step 5 Use the **set** command to specify the protocol `radius`*:*

set protocol radius

Step 6 Use the **set** command to specify the `SharedSecret 789`*:*

set SharedSecret 789

Step 7 Repeat these steps for the other remote servers.

Configuring Services

To use multiple remote servers for authorization and/or authentication you must configure the corresponding Services.

Creating the Services

Step 1 Run the **aregcmd** command:

aregcmd

Step 2 Change directory to **/Radius/Services**.

cd /Radius/Services

Step 3 Use the **add** command to add the appropriate Radius service. The following example adds the `NorthUsers-radius` object:

add NorthUsers-radius "NorthRemote server"

Step 4 Use the **cd** command to change the **NorthUsers-radius** object:

cd /Radius/Services/NorthUsers-radius

Step 5 Use the **set** command to set the type to `radius`*:*

set type radius

Step 6 Use the **set** command to set the remote server number and name. By giving each server a number, you tell Cisco AR the order you want it to access each server. Cisco AR uses this order when implementing the MultipleServersPolicy of Failover or RoundRobin.

The following example sets the first remote server to the server `North` and the second remote server to `North2`:

set RemoteServers/1 North

set RemoteServers/2 North2

Step 7 Create another Service (SouthUsers-radius) for the South remote server.

Configuring the Script

When you have multiple RemoteServers, you need a script that determines the authentication and/or authorization Service, which in turn specifies the RemoteServer to check when a user makes an Access-Request. If you want the script to apply to all users, irrespective of the NAS they are using, place the script at the **Radius** level.

Note See Determining the Goal of the Script, page 10-2 in the C*isco Access Registrar User's Guide* for sample scripts you can use as a basis for your own scripts.

Choosing the Scripting Point

Step 1 Run the **aregcmd** command:

> aregcmd

Step 2 Use the **cd** command to change to the **Scripts** object:

cd /Radius/Scripts

Step 3 Use the **add** command to add the new script, specifying the name, description, language, filename and an optional entry point. If you do not specify an entry point, Cisco AR uses the script's name.

The following example specifies the name ParseRemoteServers, the language `Rex`, the filename libParseRemoteServers.so, and the entry point ParseRemoteServers:

add ParseRemoteServers "Remote Server Script" RexlibParseRemoteServers.so ParseRemoteServers

Step 4 Use the **cd** command to change to the appropriate object level. The following example changes to the server level:

cd /Radius

Step 5 Use the **set** command to set the incoming script. The following example sets the script, **ParseRemoteServers**, at the server level:

set IncomingScript ParseRemoteServers

Step 6 Use the **save** command to save your changes:

save

Step 7 Use the **reload** command to reload the server.

reload

Configuring Session Management

You can use session management to track user sessions, and/or allocate dynamic resources to users for the lifetime of their sessions. You can define one or more Session Managers, and have each one manage the sessions for a particular group or company.

Configuring a Resource Manager

Session Managers use Resource Managers, which in turn manage a pool of resources of a particular type. The Resource Managers have the following types:

- *IP-Dynamic*—manages a pool of IP address and allows you to dynamically allocate IP addresses from that pool of addresses
- *IP-Per-NAS-Port*—allows you to associate NAS ports to specific IP addresses, and thus ensure specific NAS ports always get the same IP address
- *IPX-Dynamic*—manages a pool of IPX network addresses
- *Group-Session-Limit*—manages concurrent sessions for a group of users; that is, it keeps track of how many sessions are active and denies new sessions after the configured limit has been reached
- *User-Session-Limit*—manages per-user concurrent sessions; that is, it keeps track of how many sessions each user has, and denies the user a new session after the configured limit has been reached
- *USR-VPN*—allows you to set up a Virtual Private Network (VPN) using a US Robotics NAS. (A Virtual Private Network is a way for companies to use the Internet to securely transport private data.)
- IP address pool—allows you to manage pool of dynamic IP addresses
- On-Demand Address Pool—allows you to manage pool of IP dynamic subnet address
- Session Cache—allows you to cache additional attributes to existing session

Each Resource Manager is responsible for examining the request and deciding whether to allocate a resource for the user, pass the request through, or cause Cisco AR to reject the request.

Table 5-6 provides an overview of the process. The following sections describe the process in more detail.

Table 5-6 Configuring ResourceManagers

Object	Action
ResourceManagers	Add new ResourceManager
	Set type (Group-Session-Limit)
	Set value (100)
SessionManagers	Add new SessionManager
	Set ResourceManager
Radius	Set DefaultSessionManager

Creating a Resource Manager

You can use the default Resource Managers as models for any new Resource Managers you want to create. The following describes how to create a Resource Manager that limits the number of users to 100 or less at any one time.

Step 1 Run the **aregcmd** command:

aregcmd

Step 2 Use the **cd** command to change to the **ResourceManagers** level:

cd /Radius/ResourceManagers

Step 3 Use the **add** command to add a new ResourceManager. The following example adds the ResourceManager rm-100:

add rm-100

Step 4 Use the **cd** command to change to the ResourceManager you have just created:

cd rm-100

Step 5 Use the **set** command to set the type:

set type Group-Session-Limit

Step 6 Use the **set** command to set the number of GroupSessionLimit to 100:

set GroupSessionLimit 100

Configuring a Session Manager

Now that you have created a Resource Manager, you must associate it with the appropriate Session Manager.

Creating a Session Manager

Step 1 Run the **aregcmd** command:

aregcmd

Step 2 Use the **cd** command to change to the **SessionManagers** level:

cd /Radius/SessionManagers

Step 3 Use the **add** command to add a new SessionManager. The following example adds the SessionManager sm-1:

add sm-1

Step 4 Use the **cd** command to change to the **SessionManager/ResourceManagers** property:

cd sm-1/ResourceManagers

Step 5 Use the **set** command to specify the ResourceManagers you want tracked per user session. Specify a number and the name of the ResourceManager. Note, you can list the ResourceManager objects in any order.

set 1 rm-100

Enabling Session Management

Cisco AR, by default, comes configured with the sample SessionManagement **session-mgr-1**. You can modify it or change it to the new SessionManager you have created.

Note When you want the Session Manager to manage the resources for all Access-Requests Cisco AR receives, set the Radius DefaultSessionManager to this Session Manager. When you want a Session Manager to manage the resources of a particular object, or to use multiple Session Managers, then use an incoming script at the appropriate level.

Configuring Session Management

Step 1 Run the **aregcmd** command:

aregcmd

Step 2 Use the **cd** command to change to the **Radius** level:

cd /Radius

Step 3 Use the **set** command to set the **DefaultSessionManager** to the name you have just created:

set DefaultSessionManager sm-1

Step 4 Use the **save** command to save your changes:

save

Step 5 Use the **reload** command to reload the Cisco AR server.

reload

INDEX

Symbols

A

B

C

D

E

F

G

H

I

J

L

M

N

O

P

Q

R

S

T

U

V

W