Installing and Configuring Cisco Access Registrar, 3.5

October 2004

Corporate 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: 408 526-4100

Customer Order Number:
Text Part Number: OL-5983-03

Installing and Configuring Cisco Access Registrar, 3.5

CONTENTS

About This Guide

The Installing and Configuring Cisco Access Registrar, 3.5 provides information about installing, configuring, and customizing Cisco Access Registrar 3.5. 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 3.5 software, and information about Cisco AR licensing.
- Chapter 2, “Installing Cisco Access Registrar,” provides information about installing the Cisco AR 3.0 product 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 3.5,”
- Chapter 5, “Customizing Your Configuration,”

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/univercd/home/home.htm

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

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:

  http://www.cisco.com/en/US/partner/ordering/index.shtml

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 1 800 553-NETS (6387).

Documentation Feedback

You can send comments about technical documentation to bug-doc@cisco.com.

You can submit comments 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.

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

Cisco Technical Support Website

The Cisco Technical Support 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, 365 days a year, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support 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 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 TAC 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 TAC 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)—Your 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 operation 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 your network is impaired, but 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.

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

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

- The Cisco *Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the Cisco Product Catalog at this URL:

  http://cisco.com/univercd/cc/td/doc/pcat/

- *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

- *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

- 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 Cisco AR 3.5 software on a machine for the first time, or you can upgrade the existing Cisco AR software on a workstation to Cisco Access Registrar 3.5. Because Cisco AR 3.5.2 is the first release of Cisco AR for Linux, there is no upgrade path available.

You might receive the Cisco Access Registrar 3.5 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 1-4 provides detailed information about downloading the Cisco AR 3.5 software.

Note Cisco AR 3.5.2 for Linux is only available by downloading the software.

Before you install the Cisco AR 3.5 software, you must copy a license file to the workstation where you will install the software. You will receive the license file as an EMail attachment. "Cisco Access Registrar 3.5 Licensing" section on page 1-5 provides detailed information about the new licensing mechanism in Cisco Access Registrar 3.5.

Installation Dialog Overview

You use the **pkgadd** command to install Cisco AR 3.5 software on Solaris 8 or Solaris 9 workstations. The Linux version of Cisco AR 3.5.2 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.

Installation Type

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

The Full installation installs all parts of the Cisco AR 3.5 software including the server components, the example configuration, and the configuration utility, **aregcmd**.

The Server only installation only installs the server components and does not install the example configuration or 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. Cisco Access Registrar 3.5 uses a new 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, such as **/opt/CSCOar/license**. The installation process will copy the license file form the location you provide to **/opt/CSCOar/license**.

Refer to "Cisco Access Registrar 3.5 Licensing" section on page 1-5 for more detailed information about the Cisco Access Registrar 3.5 license file requirements.

Java Runtime Environment

The installation dialog asks for the location of the Java Runtime Environment (JRE). Cisco AR provides extensions that can be written in Java. If you intend to write or use Java extensions, the Java Runtime Environment (JRE) is required.

If you already have JRE installed, enter the directory where it is installed. If you need the JRE, you can download it from:

http://java.sun.com/products/archive

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

If you decide to use Java extensions after you have installed Cisco AR, you can specify the JRE location by entering the following at the Unix prompt:

ln -s <java-root> /cisco-ar/j2rel.4

After entering the **link** command, restart the Cisco AR server.

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.

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 if you want to create the selected base directory if it does not yet exist. 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.

If you are installing upgrade software over a previous version of Cisco AR, the base directory is detected by the installation process, and this question is not asked.

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 Access Registrar 3.5 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 version is named **CSCOar-3.5.3-sunos58-k9.tar.gz**. The RedHat Linux version of Cisco AR 3.5.2 is named **CSCOar-3.5.2-linux2420-install-k9.sh**.

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 Access Registrar 3.5 software:

CSCOar-3.5.3-sunos58-k9.tar.gz for the Solaris version or
CSCOar-3.5.2-linux2420-install-k9.sh for the RedHat 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
- A feature set upgrade license

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 displays with a link to the Cisco Access Registrar 3.5 software, **CSCOar-3.5.3-sunos58-k9.tar.gz**, and additional information about the software download package.

Step 5 Click the **Download: CSCOar-3.5.3-sunos58-k9.tar.gz** link to proceed with the software download.

A File Download dialog box displays indicating the file you are about to download.

Step 6 Click **Save** and indicate where to save the file on your computer, such as **/tmp**, then click **Save** again.

Cisco Access Registrar 3.5 Licensing

Cisco Access Registrar 3.5 uses a licensing mechanism that enables you to activate different features in Cisco AR using a combination of different license keys. During system initialization, the Cisco AR server sets up the licensing data model and activates any features that are properly licensed.

Licensed Features

Table 1lists the Cisco Access Registrar 3.5 names of the features that require licenses. As new licensed features are added to Cisco AR, new license files will also be required.

Table 1 Cisco Access Registrar 3.5 Licensed Features

Feature Name	Description
AR-STANDARD	Standard Cisco AR feature set
AR-HLR	HLR Proxy feature for EAP-SIM service
AR-PREPAID	Prepaid Billing feature for Prepaid service
AR-ADD-CACHE	Identity Caching feature
AR-CPU	Standard Cisco AR feature set for Cisco AR servers with multiprocessors

Getting Cisco Access Registrar 3.5 Feature Licenses

When you order the Cisco Access Registrar 3.5 product, a text license file will be sent to you in EMail. If you are evaluating the software, Cisco will provide you with an evaluation license.

If you decide to upgrade your Cisco Access Registrar 3.5 software and add a feature, a new text license file will be sent to you in EMail when you order the upgrade.

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 email.

Installing Cisco Access Registrar 3.5 Licenses

You must have a license in a directory on the Cisco AR machine before you attempt to install Cisco Access Registrar 3.5 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 EMail to an accessible directory.

Upgrading Your Cisco Access Registrar 3.5 License File

If you add additional features that require 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.

If you upgrade your Cisco AR license for additional features, 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 Cisco Access Registrar 3.5 license file.

```
INCREMENT AR-CPU cisco 3.5 permanent uncounted \
        VENDOR_STRING=<count>7</count> HOSTID=ANY \
        NOTICE="<LicFileID></LicFileID><LicLineID>1</LicLineID> \
        <PAK>dummyPak</PAK>" SIGN=ABCDEF123456

INCREMENT AR-STANDARD cisco 3.5 permanent uncounted \
        VENDOR_STRING=<count>5</count> HOSTID=ANY \
        NOTICE="<LicFileID></LicFileID><LicLineID>2</LicLineID> \
        <PAK>dummyPak</PAK>" SIGN=654321FEDCBA

INCREMENT AR-HLR cisco 3.5 permanent uncounted \
        VENDOR_STRING=<count>5</count> HOSTID=ANY \
        NOTICE="<LicFileID></LicFileID><LicLineID>3</LicLineID> \
        <PAK>dummyPak</PAK>" SIGN=GHIJKL123456

INCREMENT AR-PREPAID cisco 3.5 permanent uncounted \
        VENDOR_STRING=<count>5</count> HOSTID=ANY \
        NOTICE="<LicFileID></LicFileID><LicLineID>4</LicLineID> \
        <PAK>dummyPak</PAK>" SIGN=654321LMNOPQ
```

Displaying License Information

Cisco Access Registrar 3.5 provides two ways of getting license information using **aregcmd**:

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

aregcmd Command-Line Option

Cisco Access Registrar 3.5 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:
Licensed Application: Cisco Access Registrar (Standard Version)
Following are the licensed components:

          NAME         VERSION          EXPIRY_INFO
          ====         =======          ===========
          AR-Standard      3.5            permanent
          AR-CPU           3.5            permanent
          AR-HLR           3.5            permanent
          AR-Prepaid       3.5            permanent

 Following components are present but unlicensed (disabled):

         NAME           VERSION         EXPIRY_INFO
         ====           =======         ===========
         AR-Cache           3.5                 N/A
```

Launching aregcmd

The Cisco Access Registrar 3.5 server displays license information when you launch **aregcmd**, as shown in the following:

aregcmd

```
Cisco Access Registrar 3.5.1 Configuration Utility
Copyright (C) 1995-2004 by Cisco Systems, Inc.  All rights reserved.
Cluster:
User: admin
Password:
Logging in to localhost

[ //localhost ]
    LicenseInfo = AR-Standard + AR-CPU + AR-HLR + AR-Prepaid + AR-Cache
    Radius/
    Administrators/

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

CHAPTER 2

Installing Cisco Access Registrar

This chapter provides information about installing Cisco Access Registrar 3.5 software. The software is available in CD-ROM form and can also be downloaded from the Cisco.com Web site. The installation instructions differ slightly depending on whether you install the software from the Cisco Access Registrar 3.5 CD-ROM or from downloaded software.

Note This version of Cisco Access Registrar 3.5 can be used with Solaris 8, Solaris 9, or the Red Hat 7.3 Linux operating system using kernel version 2.4.20-24.7, glibc version 2.2.5-42.

Installing the Cisco AR License File

You must have a license file in a directory on the Cisco AR machine before you attempt to install Cisco Access Registrar 3.5 software. After purchasing Cisco Access Registrar 3.5, you will receive a license file in an EMail 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 EMail to an accessible directory.

Installing Cisco Access Registrar 3.5 Software on Solaris

This section describes the software installation process when installing Cisco Access Registrar 3.5 software on a Solaris workstation for the first time. This section includes the following subsections:

- Deciding Where to Install
- Installing Cisco AR Software from CD-ROM
- Installing Downloaded Software

- Common 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 Cisco AR 3.5 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 AR Software from CD-ROM

The following steps describe how to begin the software installation process when installing software from the Cisco Access Registrar 3.5 CD-ROM. If you are installing downloaded software, proceed to Installing Downloaded Software.

Note Only the Solaris 8 version of Cisco AR 3.5 is available on CD-ROM.

Step 1 Place the Cisco Access Registrar 3.5 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:

pkgadd -d /cdrom/cdrom0/kit/solaris-2.8 CSCOar

Step 3 Proceed to Common Installation Steps.

Installing Downloaded Software

This section describes how to uncompress and extract downloadedCisco Access Registrar 3.5 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-3.5.3-sunos58-k9.tar.gz | tar xvf -

Note These instructions are for the Solaris 8 package. There is no difference in download or installation procedures for Solaris 8 or Solaris 9 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 Installation Steps.

Common 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 3.5.3 [SunOS-5.8, official]
(sparc) 3.5.3
Copyright (C) 1998-2004 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.
```

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".

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.
```

Note The preceding lines display only when Cisco AR license files are detected in the **/opt/CSCOar/license** directory.

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

Step 8 Enter the directory where you have stored the Cisco Access Registrar 3.5 license file.

```
Access Registrar provides extensions that can be written in Java.
If you intend to write Java extensions, the Java Runtime
Environment (JRE) is required.

If you are not using Java, press Enter/Return to skip this step.
```

```
If you already have a JRE installed, please enter the directory
where it is installed.  If you do not, the JRE can be downloaded
from:
    http://java.sun.com/products/archive

You may specify or modify the location of the JRE, later on, by
entering the following command then restart the AR server.

# ln -s <java-root> /opt/CSCOar/j2re1.4

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

Step 9 If you plan to use Java, enter the directory location where the JRE is installed, otherwise press **Enter**.

(If you decide to use Java extensions after you have installed Cisco AR, you can specify the JRE location by entering the following at the Unix prompt:

ln -s <java-root> /cisco-ar/j2rel.4

After entering the **link** command, restart the Cisco AR server.)

```
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 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]

    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
```

Step 11 When prompted whether to install the example configuration now, reply **Yes** 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**.

```
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.

```
## Executing checkinstall script.
Using </opt/CSCOar> as the package base directory.
## Processing package information.
## Processing system information.
   8 package pathnames are already properly installed.
## 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>
/opt/CSCOar/bin/xmlclient <setgid staff>


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

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

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 part 1 of 1.
/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
.
.
.
/opt/CSCOar/ucd-snmp/share/snmp/snmpconf-data/snmptrapd-data/traphandle
/opt/CSCOar/ucd-snmp/share/snmp/snmpd.conf
[ verifying class <snmp> ]
## Executing postinstall script.
# setting up product configuration file /opt/CSCOar/conf/car.conf
# linking /etc/init.d/arserver to /etc/rc.d files
# setting ORACLE_HOME variable 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 May 14 13:23:32
2004
Rollforward recovery using "/opt/CSCOar/data/db/vista.tjf" finished Fri May 14 13:23:32
2004

# installing example configuration
```

```
Starting Access Registrar Server Agent..completed.
The Radius server is now running.

If SNMP needs to be reconfigured please follow the following
procedure:

(1) stop AR: /opt/CSCOar/bin/arserver stop
(2) edit: /cisco-ar/ucd-snmp/share/snmp/snmpd.conf
(3) restart AR: /opt/CSCOar/bin/arserver start

# done with postinstall.

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

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:

arserver stop

/etc/init.d/rpc start

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 3.5 Software on Linux

This section describes the software installation process when installing Cisco Access Registrar 3.5 software on a Linux workstation for the first time. This section includes the following subsections:

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 Cisco AR 3.5 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 Downloaded Software

This section describes how to install the downloadedCisco Access Registrar 3.5 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-3.5.3-linux2420-install-k9.sh** file.

cd /tmp

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

CSCOar-3.5.3-linux2420-install-k9.sh

```
CSCOar-3.5.3-linux2420-install-k9.sh
Name        : CSCOar                        Relocations: /opt/CSCOar
Version     : 3.5.3                              Vendor: Cisco Systems, Inc.
Release     : 1089750252                     Build Date: Tue Jul 13 14:17:55 2004
Install date: (not installed)                Build Host: muggle.cisco.com
Summary     : Access Registrar, a carrier-class RADIUS server
build_tag: [Linux-2.4.20, official]

Copyright (C) 1998-2004 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? [/opt/CSCOar/license] [?,q]
```

Step 5 Enter the directory where you have stored the Cisco Access Registrar 3.5 license file.

```
    Access Registrar provides extensions that can be written in Java.
    If you intend to write Java extensions, the Java Runtime Environment
    (JRE) is required.

    If you are not using Java, press Enter/Return to skip this step.

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

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

        You may specify or modify the location of the JRE, later on, by
        entering the following command then restart the AR server.

        # ln -s <java-root> /opt/CSCOar/j2re1.4

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

Step 6 If you plan to use Java, enter the directory location where the JRE is installed, otherwise press **Enter**.

(If you decide to use Java extensions after you have installed Cisco AR, you can specify the JRE location by entering the following at the Unix prompt:

ln -s <java-root> /cisco-ar/j2rel.4

After entering the **link** command, restart the Cisco AR server.)

```
    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 7 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 8 When prompted whether to install the example configuration now, reply **Yes** 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:CSCOar                 ########################################### [100%]
# setting ORACLE_HOME variable in arserver
# creating initial configuration database
Rollforward recovery using "/opt/CSCOar/data/db/vista.tjf" started Wed Jul 14 15:17:28
2004
Rollforward recovery using "/opt/CSCOar/data/db/vista.tjf" finished Wed Jul 14 15:17:28
2004

# installing example configuration

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 Access Registrar, 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

Cisco Access Registrar 3.5 supports software upgrades from your previously installed Cisco AR software while preserving your existing configuration database.

Note Configuration for Prepaid billing servers in Cisco AR 3.0 will no longer work in Cisco AR 3.5. If you have been using a Prepaid billing server in Cisco AR 3.0 and are upgrading your software to Cisco AR 3.5, you must remove the Prepaid billing server configuration before installing the Cisco AR 3.5 software. "Configuring Prepaid Billing" section on page 4-17 provides detailed instructions for configuring Prepaid billing services for Cisco AR 3.5.

This chapter contains the following sections:

Upgrade Overview

The following steps describe what you must do to perform the software upgrade process:

Step 1 Ensure that replication is disabled.

Refer to Disabling Replication.

Step 2 Remove the old software using the **pkgrm** command.

Refer to Using pkgrm to Remove Cisco AR Software.

Step 3 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 4 Decide where to install the Cisco Access Registrar 3.5 software.

The default installation directory for Cisco AR 3.5 software is **/opt/CSCOar**. If you are upgrading from Cisco AR version 1.7 or earlier, the default installation directory was **/opt/AICar1**.

Step 5 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 procedures in this chapter assume 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 3.0 and above is **/opt/CSCOar**.

If your previous install directory was **/opt/AICar1**, you should use that directory to install Cisco AR 3.5. You might also rename the old directory, as in the following:

cd /opt

mv AICar1 CSCOar

Step 6 Copy the Cisco Access Registrar 3.5 license file to a location on the Cisco AR workstation directory such as **/tmp**.

Step 7 Use the **pkgadd** command to install the Cisco Access Registrar 3.5 software.

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, refer to "Restarting Replication" section on page 3-12 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 AR Software

There are two different Cisco AR 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 ~##
```

Installing the Cisco AR License File

Cisco Access Registrar 3.5 uses a new licensing mechanism that enables you to activate different features in Cisco AR using a combination of different license keys. During system initialization, the Cisco AR server sets up the licensing data model and activates any features that are properly licensed.

You must have a license in a directory on the Cisco AR machine before you attempt to install Cisco Access Registrar 3.5 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 EMail to an accessible directory.

Installing Cisco AR Software

This section describes the software installation process and includes the following sections:

- Deciding Where to Install
- Installing Cisco AR Software from CD-ROM
- Installing Downloaded Software
- Common Installation Steps
- Configuring SNMP

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 Cisco AR 3.5 software is **/opt/CSCOar**. If you are upgrading from Cisco AR version 1.7 or earlier, the default installation directory was **/opt/AICar1**. You can preserve your existing configuration database by installing the new software in the old location, or you can rename the previous installation directory to the new package name before you begin the installation using commands like the following:

```
cd /opt

mv AICar1   CSCOar
```

Make this decision and take appropriate action before you proceed.

Installing Cisco AR Software from CD-ROM

The following steps describe how to begin the software installation process when installing software from the Cisco Access Registrar 3.5 CD-ROM.

Step 1 Place the Cisco Access Registrar 3.5 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:

pkgadd -d /cdrom/cdrom0/kit/solaris-2.8 CSCOar

Step 3 Proceed to Common Installation Steps.

Installing Downloaded Software

This section describes how to uncompress and extract downloadedCisco Access Registrar 3.5 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-3.5.3-sunos58.tar.gz | tar xvf -

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 Installation Steps.

Common 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 3.5.1 [SunOS-5.8, official]
(sparc) 3.5.1
Copyright (C) 1998-2004 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 Cisco Access Registrar Server and the
    Cisco Access Registrar Configuration Utility.  You can choose to
    perform a Full installation, just install the Server, or just
```

```
    install the Configuration Utility.

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

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

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

Step 7 Enter the location where the previous package was installed, or accept the default location of **/opt/CSCOar** if you moved the previous configuration database to the default directory.

```
The installation procedure requires the FLEXlm license file(s)
location. An individual file or a directory can be supplied as input.
License file(s) must have extension .lic

The file(s) will be copied to the installation license directory
  /opt/CSCOar/license

To enable other features within this package, additional FLEXlm
license files can be added to the license directory.

Enter FLEXlm license file(s) location? [/opt/CSCOar/license] [?,q]
```

Step 8 Enter the directory where you have stored the Cisco Access Registrar 3.5 license file.

```
Cisco AR provides extensions that can be written in Java.
If you intend to write Java extensions, the Java Runtime
Environment (JRE) is required.

If you are not using Java, press Enter/Return to skip this step.

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

    http://java.sun.com/products/archive

Where is the current JRE installed?  [?,q]
```

Step 9 If you are using Java, enter the directory location where the JRE is installed, otherwise press **Enter**.

```
If you are not using ODBC, 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 are using Open Database Connectivity, 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,n,?,q]
```

Step 11 Because you are upgrading, you will want to preserve your local database. Enter **y** or **yes**., then provide an administrator userID and password.

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

```
User: admin
Password:
Retype password:

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

Step 12 Enter **Y** to remove old sessions or **N** to save old sessions.

```
## Executing checkinstall script.
Using </opt/CSCOar> as the package base directory.
## Processing package information.
## Processing system information.
   14 package pathnames are already properly installed.
## 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 these 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. Sections that follow describe actions taken during the upgrade.

```
Installing Cisco Access Registrar 3.5.1 [SunOS-5.8, official] as <CSCOar>

## Installing part 1 of 1.
/opt/CSCOar/.system/screen
/opt/CSCOar/README
/opt/CSCOar/bin/arbug
.
. <several hundred lines deleted>
.
/opt/CSCOar/ucd-snmp/share/snmp/snmpd.conf
[ verifying class <snmp> ]
## Executing postinstall script.
# setting up product configuration file /opt/CSCOar/conf/car.conf
# linking /etc/init.d/arserver to /etc/rc.d files
# setting ORACLE_HOME variable in arserver

# Upgrade of the configuration db is in progress

# Password check in progress
# Wait.
# Password check complete

# flushing old replication archive

# Backup of configuration in progress
# Wait.....
```

```
# Backup complete

#################################################################
#
#  A backup copy of your original configuration has been
#  saved to the file:
#
#    /opt/CSCOar/temp/12661.origconfig-backup
#
#  If you need to restore the original configuration,
#  enter the following command:
#
#    mcdadmin -coi /opt/CSCOar/temp/12661.origconfig-backup
#
#################################################################


#################################################################
#
#  The upgrade process involves the use of mcdadmin and
#  aregcmd. First a small set of updates are performed
#  using mcdadmin. Then the vast majority of updates are
#  performed using aregcmd.
#
#################################################################

# Mcdadmin-level upgrade in progress
# Mcdadmin-level upgrade completed

# Aregcmd-level upgrade in progress
# Configuration DB analysis is in progress
# Wait....
# Analysis completed

# Deleting of obsolete tunnel attributes is in progress
# Wait..........
# Deletion completed


# Updating Port object definitions is in progress
# Wait.
# Update completed

# Add of new database elements is in progress
# Wait...................
# Add completed

# Search for obsolete VSA names is in progress
# Search completed

#################################################################
#
#   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/12661.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 -f /opt/CSCOar/temp/12661.manual-deletes
#
################################################################


################################################################
#
#   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/12661.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 -f /opt/CSCOar/temp/12661.manual-changes
#
################################################################


################################################################
#
#  These upgrade messages are saved in:
#
#      /opt/CSCOar/temp/12661.upgrade-log
#
################################################################

Starting Access Registrar Server Agent..completed.
The Radius server is now running.

If SNMP needs to be reconfigured please follow the following
procedure:

(1) stop AR: /opt/CSCOar/bin/arserver stop
(2) edit: /cisco-ar/ucd-snmp/share/snmp/snmpd.conf
(3) restart AR: /opt/CSCOar/bin/arserver start

# done with postinstall.

Installation of <CSCOar> was successful.
```

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.

```
################################################################
#
#  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 15 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 16 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 Cisco Access Registrar, the installation process is completed. To use SNMP features, complete the configuration procedure described in Configuring SNMP, page 4-14.

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.

Configuring Cisco Access Registrar 3.5

This chapter describes how to configure a site. Cisco Access Registrar 3.5 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 has the following major sections:

Using aregcmd

To configure Cisco Access Registrar 3.5, use the **aregcmd** commands, which are command-line based configuration tools. These commands allow you to set any Cisco Access Registrar 3.5 configuration option, as well as, start and stop the Cisco Access Registrar 3.5 RADIUS server and check its statistics.

General Command Syntax

Cisco Access Registrar 3.5 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 path names 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 typing **cd Administrators**, you can type **cd ad** if no other element at the current level begins with *ad*.

You can use Cisco AR's command completion feature to see what commands are possible from your current directory location in the Cisco AR 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 Access Registrar 3.5 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 or release active sessions; commands include **query-sessions** and **release-sessions**.

This chapter uses only a few of the above commands to configure the Cisco Access Registrar 3.5 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 Access Registrar 3.5 machine.
2. Configure the Cisco Access Registrar 3.5 RADIUS server settings, such as the server name and the server defaults.
3. Add users by copying the sample users.
4. Configure the clients, that is, the NASs and proxies that communicate with Cisco Access Registrar 3.5.
5. Change profile attributes as needed.
6. Save your changes and reload your Cisco Access Registrar 3.5 RADIUS server.

Running aregcmd

aregcmd is the command-line interface program used to configure the Cisco Access Registrar 3.5 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 Cisco AR 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 Cisco Access Registrar 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 Access Registrar 3.5 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. Note, you enter the password on the command line in readable form, however, Cisco Access Registrar 3.5 displays it as encrypted.

The following example changes the password to `345`. You are asked to retype 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 Access Registrar 3.5 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 = 1.3
    IncomingScript =
    OutgoingScript =
    DefaultAuthenticationService = local-users
    DefaultAuthorizationService = local-users
    DefaultAccountingService = local-file
    DefaultSessionManager = session-mgr-1
    UserLists/
    UserGroups/
    Clients/
    Vendors/
    Scripts/
    Services/
    SessionManagers/
    ResourceManagers/
    Profiles/
    RemoteServers/
    Advanced/
```

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, type *DefaultSessionManager*, then specify an empty string by typing a set of double quotes:

set DefaultSessionManager ““

Note When you do not want Cisco Access Registrar 3.5 to monitor resources for user sessions, you should disable session management, because using it affects your RADIUS server's 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 Access Registrar 3.5 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 AR server configuration.

save

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

reload

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

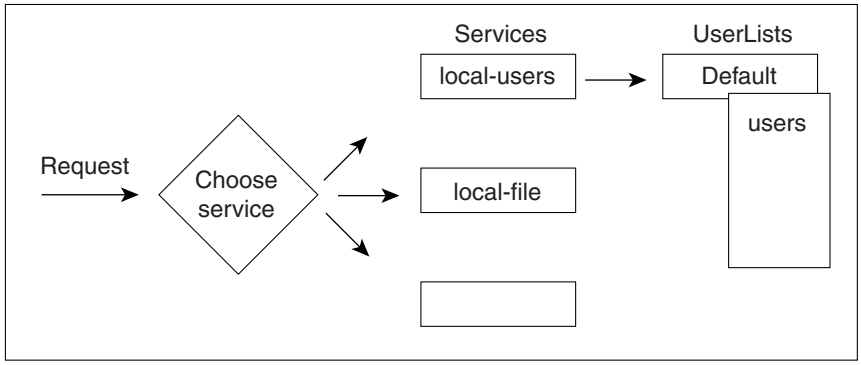
Displaying the UserLists

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 Access Registrar 3.5 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 Access Registrar 3.5, 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 If necessary, use the **cd** command to change to the **Radius /UserLists** level:

cd /Radius/Userl

```
[ //localhost/Radius/UserLists ]
    Entries x to x from x total entries
    Current filter: <all>

    localUsers
```

Step 2 Change directory to the UserList to which you want to add a user.

cd localUsers

```
[ //localhost/Radius/UserLists/localUsers ]
    Entries 0 to 0 from 0 total entries
    Current filter: <all>

    Name = localUsers
    Description =
```

Step 3 Use the **add** command to specify the name of a user and an optional description on one command line.

add jane

```
Added jane
```

Step 4 Change directory to **jane**.

cd jane

```
[ //localhost/Radius/UserLists/localUsers/jane ]
    Name = jane
    Description =
    Password =
    Enabled = TRUE
    Group~ =
    BaseProfile~ =
    AuthenticationScript~ =
    AuthorizationScript~ =
    UserDefined1 =
    AllowNullPassword = FALSE
```

Step 5 Use the **set** command to provide a password for user **jane**.

set p password

```
Retype password to confirm:
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, type:

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 Access Registrar 3.5 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 NASs and proxies that communicate directly with Cisco Access Registrar 3.5. 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 Access Registrar 3.5 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 Access Registrar 3.5 for your NAS, and you must configure your NAS for Cisco Access Registrar 3.5.

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`, and the Vendor as `USR`. Because you want to choose the service based on the user requests, set the IncomingScript as `ParseServiceHints`.

set Description WestOffice

set IPAddress 209.165.200.225

set SharedSecret xyz

set Type NAS

set Vendor USR

set IncomingScript ParseServiceHints

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 Access Registrar 3.5 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 Access Registrar 3.5 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-Telnet-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-Route “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 Access Registrar 3.5 server, you must save your changes. Saving your changes causes Cisco Access Registrar 3.5 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 Access Registrar 3.5 to reread the configuration database.

You must **save** and **reload** your configuration changes in order for them to take effect in the Cisco Access Registrar 3.5 server.

Saving and Reloading

From anywhere in the radius object hierarchy, type 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. It prompts you for the cluster name. Enter the cluster name.

radclient

Step 2 The **radclient** command prompts you for the administrator's username and password (as defined in the Cisco Access Registrar 3.5 configuration). Use **admin** for the admin name, and **aicuser** for the password.

```
Access Registrar RADIUS Test Client Version 1.3
Copyright (C) 1995-1998 by American Internet Corporation, and 1999 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, type:

simple john john

```
p001
```

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

Step 4 Type 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**), type:

p001 send

```
p002
```

Step 6 Type 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 Access Registrar 3.5 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 1-4.

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 Access Registrar 3.5 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 Cisco AR server configuration, the Cisco AR server writes accounting messages to the **accounting.log** file in the **/opt/CSCOar/logs** directory. The Cisco AR 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-20010619-14** would be the 14th rollover on June 19, 2001.

The following shows the properties for a service called CiscoAccounting:

```
[ //localhost/Radius/Services/CiscoAccounting ]
    Name = CiscoAccounting
    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 AR 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 AR 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 Cisco Access Registrar 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 MyRWGroup   v1         local
group MyRWGroup   v2c        local
group MyRWGroup   usm        local
group MyROGroup   v1         mynetwork
group MyROGroup   v2c        mynetwork
group MyROGroup   usm        mynetwork
```

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.

```
# ----------------------------------------------------------------------------
trapcommunity trapcom
trapsink      zubat    trapcom  162
trap2sink     ponyta   trapcom  162
##############################################################################
```

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 Cisco AR SNMP master agent by restarting the Cisco Access Registrar server.

/opt/CSCOar/bin/arserver start

Configuring Prepaid Billing

This section describes the configuration required before you can use the prepaid billing feature with Cisco Access Registrar 3.5. The *Cisco Access Registrar 3.5 Concepts and Reference Guide* provides detailed information about the prepaid billing feature.

Cisco Access Registrar 3.5 supports two types of prepaid billing, prepaid-is835c and prepaid-crb.

T o use the prepaid billing feature of Cisco Access Registrar 3.5, you must configure a new prepaid service type and reference a RemoteServer with its protocol set to either prepaid-is835c or prepaid-crb. The following lists the prepaid service properties:

```
[ //localhost/Radius/Services/prepaid-api ]
    Name = prepaid-api  (for example)
    Description =
    Type = prepaid
    IncomingScript~ =
    OutgoingScript~ =
    OutagePolicy~ = RejectAll
    OutageScript~ =
    MultipleServersPolicy = Failover
    RemoteServers/
```

Prepaid Billing Services

You can configure up to five services to use the prepaid billing feature:

- A service (type prepaid) to handle prepaid requests, for example **prepaid-api**
- A user authentication and authorization (AA) service, such as **local-users**, for authentication and authorization of local users
- An accounting service, such as **local-file,** for accounting requests
- Two group services that tie the AA and accounting services to the prepaid service

Prepaid Service

If you use the Cisco AR 3.5 server in your prepaid billing solution, you must configure a service of type prepaid as shown in Configuring Prepaid Billing, for example **prepaid-api**. The prepaid service is a new service type for Cisco AR 3.5 that mediates between the client NAS and the prepaid billing server.

The prepaid service must receive accounting requests to accurately charge the prepaid billing user. You can also set the prepaid service in a group service to log accounting requests locally or to proxy the accounting requests to another service or to both locations.

AA Service

If you use the Cisco AR 3.5 server for authentication and authorization in your prepaid billing solution, you might want to configure an AA service. For example, you might configure a service similar to **local-users** (in the example configuration) for authentication and authorization of local users.

If some of the users are non-prepaid users or if the prepaid users need to have RADIUS authorization attributes returned, you should configure an AA service to perform that authentication and authorization.

If all of the users in a realm are prepaid users and the prepaid billing client does not require normal RADIUS authorization attributes, an AA service is not necessary.

Accounting Service

If you want to use the Cisco AR 3.5 server to record the accounting records locally or to forward the accounting records to another RADIUS server, you must configure an accounting service. You might configure a service similar to **local-file** (in the example configuration) for accounting requests. Accounting requests can be logged locally (with an accounting service) or remotely (with a RADIUS service).

If you use the prepaid billing server to generate the accounting records, an accounting service is not necessary.

Group Services

Your prepaid billing solution might require a group service to tie together an AA service with a prepaid service, a group service to tie together an accounting service with a prepaid service, or both.

If you are using an AA service with your prepaid billing solution, you must configure a group service, for example **prepaid-users**, that ties the requests to the AA service (**local-users** in our example) with the prepaid service.

If you are using Cisco AR 3.5 for an accounting service with your prepaid billing solution, you must configure a group service, for example **prepaid-file**, that ties accounting requests to both the regular accounting service (**local-file** in our example) and the prepaid service.

Group Services for Prepaid User Authentication and Authorization

You must configure a **prepaid-users-**like service if you have some users who use prepaid billing and some users who are not. If this is the case, you can configure users by setting a user-specific attribute of Cisco-AVPair=crb-entity-type=2 if the subscriber is postpaid with no credit limit and Cisco-AVPair=crb-entity-type=3 if the subscriber is postpaid with a credit limit. In either case, Cisco Access Registrar does not call out to the prepaid billing server for the initial authentication.

Use the following steps to create and configure the **prepaid-users** service.

Step 1 Create the **prepaid-users** service, and set the service type to **group**.

```
[ //localhost/Radius/Services/prepaid-users ]
    Name = prepaid-users
    Description =
    Type =
    IncomingScript~ =
    OutgoingScript~ =
```

Step 2 Set the **prepaid-users** service to type group.

set type group

```
Set Type group
```

ls

```
[ //localhost/Radius/Services/prepaid-users ]
    Name = prepaid-users
    Description =
    Type = group
    IncomingScript~ =
    OutgoingScript~ =
    ResultRule = AND
    GroupServices/
```

Step 3 Change directory to **GroupServices** and set to **local-users** and **prepaid-api**.

cd groupservices

```
[ //localhost/Radius/Services/prepaid-users/GroupServices ]
```

set 1 local-users

```
Set 1 local-file
```

set 2 prepaid-api

```
Set 2 prepaid-api
```

ls

```
[ //localhost/Radius/Services/prepaid-users/GroupServices ]
    1. local-users
    2. prepaid-api
```

Group Services for Prepaid Accounting

You can configure a group service, such as **prepaid-file,** that directs requests to both the regular accounting service (**local-file** in this example) and the prepaid service. You must configure the **prepaid-file** service if you want to log accounting requests locally or to proxy the accounting requests to another service or to both locations.

Complete the following steps to create and configure the prepaid accounting group service.

Step 1 Create the **prepaid-file** service, and set the service type to **group**.

```
[ //localhost/Radius/Services/prepaid-file ]
    Name = prepaid-file
    Description =
    Type =
    IncomingScript~ =
    OutgoingScript~ =
```

Step 2 Set the **prepaid-file** service to type group.

set type group

```
Set Type group
```

ls

```
[ //localhost/Radius/Services/prepaid-file ]
    Name = prepaid-users
    Description =
    Type = group
    IncomingScript~ =
    OutgoingScript~ =
    ResultRule = AND
    GroupServices/
```

Step 3 Change directory to **GroupServices** and set to **local-file** and **prepaid-api**.

cd groupservices

```
[ //localhost/Radius/Services/prepaid-file/GroupServices ]
```

set 1 local-file

```
Set 1 local-file
```

set 2 prepaid-api

```
Set 2 prepaid-api
```

ls

```
[ //localhost/Radius/Services/prepaid-file/GroupServices ]
    1. local-file
    2. prepaid-api
```

RemoteServers

Prepaid billing also requires you to configure a RemoteServer with its protocol set to either prepaid-is835c or prepaid-crb.

Prepaid-CRB

The following is the default configuration of a prepaid-crb RemoteServer.

```
[ //localhost/Radius/RemoteServers/prepaid-crb ]
    Name = prepaid-crb
    Description =
    Protocol = prepaid-crb
    IPAddress =
    Port = 0
    Filename =
    Connections = 8
```

Prepaid-IS835C

The following is the default configuration of a prepaid-is835c RemoteServer.

```
[ //localhost/Radius/RemoteServers/prepaid-is835c ]
    Name = prepaid-is835c
    Description =
    Protocol = prepaid-is835c
    IPAddress =
    Port = 0
    Filename =
    Connections = 8
```

Configuring Packet of Disconnect

Cisco Access Registrar 3.5 adds support for the Packet of Disconnect (POD). The POD feature enables Cisco AR to send disconnect requests (PODs) to a NAS so that all the session information and the resources associated with the user sessions can be released. Cisco AR can also determine when to trigger and send the POD.

For example, when a PDSN handoff occurs during a mobile session, the new PDSN sends out a new access-request packet to Cisco AR for the same user. Cisco AR should detect this handoff by the change in NAS-Identifier in the new request and trigger sending a POD to the old PDSN if it supports POD. Cisco AR also provides an option for administrator to initiate sending POD requests through the command-line interface (CLI) for any user session. Cisco AR forwards POD requests from external servers to the destination NAS.

Configuring the Client Object

You should enable POD for each client object that might want to send disconnect requests to those clients. You enable POD in a client object using the EnablePOD property. This property is set to FALSE by default when you create a client object. The following example shows the default configuration for a new client object, NAS1.

```
[ //localhost/Radius/Clients/NAS1 ]
    Name = nas1
    Description =
    IPAddress =
    SharedSecret =
    Type = NAS
    Vendor =
    IncomingScript~ =
    OutgoingScript~ =
    EnablePOD = FALSE
```

If the Cisco AR server might send a POD to this client, set the EnablePOD property to TRUE. When you set this property to TRUE, the Cisco AR server creates a POD subdirectory under the client object. The following example shows a newly created POD subdirectory:

```
[ //localhost/Radius/Clients/NAS1/POD ]
    Port = 3799
    PODSecret =
    InitialTimeout = 5000
    MaxTries = 3
    AttributesToBeSent = Default
```

The default POD port is 3799. You can change the POD port, if desired.

The property PODSecret is initially set to the same as value as the client's SharedSecret property when you set EnablePOD to TRUE. You can chose to configure a different secret for POD in this subdirectory.

The InitialTimeout property represents the number of milliseconds used as a timeout for the first attempt to send a POD packet to a remote server. For each successive retry on the same packet, the previous timeout value used is doubled. You must specify a number greater than zero, and the default value is 5000 (or 5 seconds).

The MaxTries property represents the number of times to send a proxy request to a remote server before deciding the server is off-line. You must specify a number greater than zero, and the default is 3.

The AttributesToBeSent property points to a group of attributes to be included in a disconnect-request packet sent to this Client.

You can create and configure the POD attribute groups under PODAttributes subdirectory in **/Radius/Advanced**. The Default group contains commonly used POD attributes. The following is an example of the PODAttributes subdirectory:

```
[ //localhost/Radius/Advanced/PODAttributes/ ]

    Default/
        Name = Default
        Description =
        Attributes/
           1. Calling-Station-Id
           2. Framed-IP-Address
           3. Acct-Multi-Session-Id
```

Configuring a Resource Manager for POD

Cisco Access Registrar 3.5 adds a new resource manager type called *session-cache*. When you set a resource manager to session-cache, the resource manager's configuration contains a subdirectory called ***AttributesToBeCached***. The following is an example Resource Manager set to type session-cache:

```
[ //localhost/Radius/ResourceManagers/PODresourceMgr ]
    Name = PODresourceMgr
    Description =
    Type = session-cache
    OverwriteAttributes = FALSE
    AttributesToBeCached/
```

The attributes you configure under the **AttributesToBeCached** directory are cached in the session record during session management. The cached attributes are then sent in the disconnect-request for this session.

The OverwriteAttributes property indicates whether to overwrite the existing attributes if there are any in the session record. Since this resource manager can be invoked during Access-Request as well as Accounting-Start processing, the OverwriteAttributes can be used to control if the attributes cached during Access-Request processing can be overwritten with the attributes available during Accounting-Start processing.

The following is an example of a typical session-cache resource manager:

```
[ //localhost/Radius/ResourceManagers/RM-New ]
    Name = RM-New
    Description =
    Type = session-cache
    OverwriteAttributes = TRUE
    AttributesToBeCached/
        1. Framed-IP-Address
        2. CDMA-Correlation-ID
```

The attributes used in the example can be added as an indexed list using **add** or **set** commands (in any order).

Proxying POD Requests from External Servers

Cisco AR can also proxy the disconnect requests received from external servers. To make Cisco AR listen for external POD requests, the ListenForPOD property under **/Radius/Advanced** should be set to TRUE. The default value for this is FALSE. The default POD listening port is 3799. However this can be changed by configuring a new port of type *pod* under **/Radius/Advanced/Ports** and setting the new port number accordingly.

For security reasons, the source of a POD request should be configured as a remote server in Cisco AR and the remote server should be configured to accept PODs. The property AcceptPOD can be set to TRUE to do this. The default for this is FALSE. POD requests from unauthorized sources are silently discarded.

CLI Options for POD

Cisco Access Registrar 3.5 provides new options for the **query-sessions** and **release-sessions** CLI commands. One new option enables querying or releasing sessions based on the session's age. The other option enables for querying or releasing sessions based on any valid RADIUS attribute available in the user's session record.

query-sessions

The syntax for using **query-sessions** *with-Age* option is the following:

query-sessions <path> with-Age <value>

Where <path> is the path to the server, session-manager or resource manager and <value> is the minimum age of the session specified in minutes or hours with options M, Minutes, H or Hours. This command returns all sessions that are older than the given age value.

The syntax for using **query-sessions** *with-Attribute* option is the following:

query-sessions <path> with-Attribute <name> <value>

Where <name> is the RADIUS attribute name and <value> is the value of the attribute to be matched. This command returns the sessions where a session record contains and matches the attribute value specified in <value> field.

release-sessions

The syntax for using **release-sessions** *with-Age* option is the following:

release-sessions <path> with-Age <value>

Where <path> is the path to the server, session-manager or resource manager and <value> is the minimum age of the session specified in minutes or hours with options M, Minutes, H or Hours. This command returns all sessions that are older than the given age value.

The syntax for using **release-sessions** *with-Attribute* option is the following:

release-sessions <path> with-Attribute <name> <value>

Where <name> is the RADIUS attribute name and <value> is the value of the attribute to be matched. This command returns the sessions where a session record contains and matches the attribute value specified in <value> field.

A new option is also available for **release-sessions** command to enable an administrator to trigger sending a POD for a user after the session is released.

release-sessions <path> with-<type> <value> [send-pod]

Where <path> is the path to the server, Session Manager, or Resource Manager and with-<type> is one of the following: with-NAS, with-User, with-IP-Address with-ID, or with-Age. The **release-sessions** command with an optional [send-pod] at the end results in Cisco AR sending a POD to the NAS (as determined from the session record) after the session is actually released.

Configuring Dynamic DNS

Cisco Access Registrar 3.5 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 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 provide an introduction to many of the Cisco Access Registrar 3.5 objects and their properties. For more detailed descriptions, see the *Cisco Access Registrar 3.5 User's Guide.*

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 Access Registrar 3.5 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 Access Registrar 3.5 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 SLIP-users group.

This example sets the BaseProfile to `default-SLIP-users`. When you set this property to the name of a profile, Cisco Access Registrar 3.5 adds the properties in the profile to the response dictionary as part of the authorization process.

add SLIP-users "Users who always connect using SLIP" default-SLIP-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 SLIP-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 Access Registrar 3.5 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 Access Registrar 3.5 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, refer to 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), file name and an optional entry point. When you do not specify an entry point, Cisco Access Registrar 3.5 uses the script's name.

add AuthorizeService "" 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 In order to be able to save your changes and reload the server after following this example, you must have an actual script. Cisco Access Registrar 3.5 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 Access Registrar 3.5 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

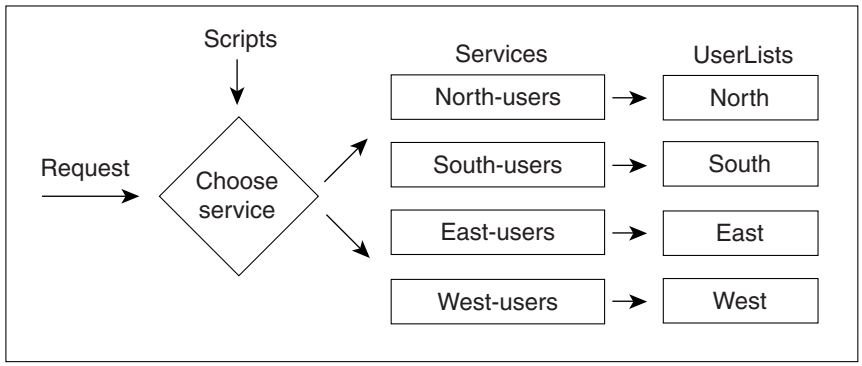


Table 5-3 provides an overview of the process. The following sections describe the process in more detail.

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 Access Registrar 3.5 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 Access Registrar 3.5, see the *Cisco Access Registrar User Guide*. For examples of scripts, refer to the C*isco Access Registrar User's Guide.*

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.

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, file name and an optional entry point. If you do not specify an entry point, Cisco Access Registrar 3.5 uses the script's name.

The following example specifies the name `ParseUserName`, the language `Rex` (which is RADIUS Extension), the file name `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 Access Registrar 3.5 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 Access Registrar 3.5 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.

Table 5-4 Configuring a Remote Server

Object	Action
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 host name `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 host name 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`).

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

For descriptions of the other LDAP properties, see the *Cisco Access Registrar User Guide.*

Configuring Services

In order 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 Access Registrar 3.5 the order you want it to access each server. Cisco Access Registrar 3.5 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 Access Registrar 3.5 handles multiple remote servers.

- When you set it to `Failover`, Cisco Access Registrar 3.5 directs requests to the first server in the list until it determines the server is off-line. At that time, Cisco Access Registrar 3.5 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 Access Registrar 3.5 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 Access Registrar 3.5 configuration, authentication and authorization are handled through the local-users Service object. This causes Cisco Access Registrar 3.5 to match requesting users with the names in its own database. When you select LDAP as a remote server for authentication and authorization, Cisco Access Registrar 3.5 looks to that server for user information.

To have Cisco Access Registrar 3.5 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

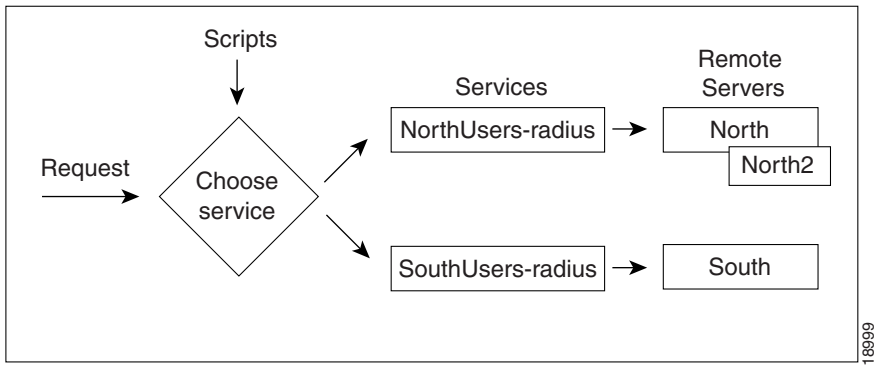


Table 5-5 provides an overview of the process. The following sections describe the process in more detail. Repeat for each RemoteServer you want to configure.

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 for the other remote servers.

Configuring Services

In order 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 Use the **cd** command to change to the **Services** level:

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 Access Registrar 3.5 the order you want it to access each server. Cisco Access Registrar 3.5 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 For sample scripts you can use as a basis for your own scripts, refer to the C*isco Access Registrar User's Guide.*

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, file name and an optional entry point. If you do not specify an entry point, Cisco Access Registrar 3.5 uses the script's name.

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

add ParseRemoteServers "" 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 once 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 once 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.)

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 Access Registrar 3.5 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 Access Registrar 3.5, 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 Access Registrar 3.5 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 Cisco Access Registrar 3.5:

reload

Symbols

A

B

C

D

E

F

G

H

I

J

L

M

N

O

P

Q

R

S

T

U

V

W