Installation Guide for Cisco Network Registrar

Software Release 7.0

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

Text Part Number: OL-10274-01

CONTENTS

Preface

This guide describes how to install Cisco Network Registrar Release 7.0 on the supported operating systems: Windows, Solaris, and Linux. It is written for the system administrators who will be installing the software, and assumes that you understand your site configuration and the basic steps for installing software. (For information on configuring and managing Network Registrar, refer to the *Cisco Network Registrar User's Guide*.)

The guide is organized into these chapters and appendixes.

Chapter 1	Overview	Introduces Network Registrar and provides critical system information that must be read before installing the software.
Chapter 2	Installing and Upgrading Network Registrar	Describes how to install or upgrade Network Registrar; and how to uninstall it, stop and start servers, and troubleshoot the installation.
Appendix A	Performing a Silent Installation	Explains how to perform a silent installation, upgrade, or uninstallation of the Network Registrar product.
Appendix B	Lab Evaluation Installations	Explains how to install, upgrade, or uninstall Network Registrar if it is being used in a lab environment.

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

CHAPTER 1

Overview

This guide describes how to install Cisco Network Registrar Release 7.0 on Windows, Solaris, and Linux operating systems. You can also refer to these documents for important information about configuring and managing Network Registrar:

- For configuration and management procedures for Network Registrar, see the *Cisco Network Registrar User's Guide*.
- For details about commands available through the command line reference (CLI), see the *Cisco Network Registrar CLI Reference*.

About Network Registrar

Network Registrar is a network server suite that automates managing enterprise IP addresses. It provides a stable infrastructure that increases address assignment reliability and efficiency. It includes these servers (see Figure 1-1 on page 1-2):

- Dynamic Host Configuration Protocol (DHCP)
- Domain Name System (DNS)
- Router Interface Configuration (RIC)
- Simple Network Management Protocol (SNMP)
- Trivial File Transfer Protocol (TFTP)

You can control these servers by using the Network Registrar web-based user interface (web UI) or the command line interface (CLI). These user interfaces can also control server clusters that run on different platforms.

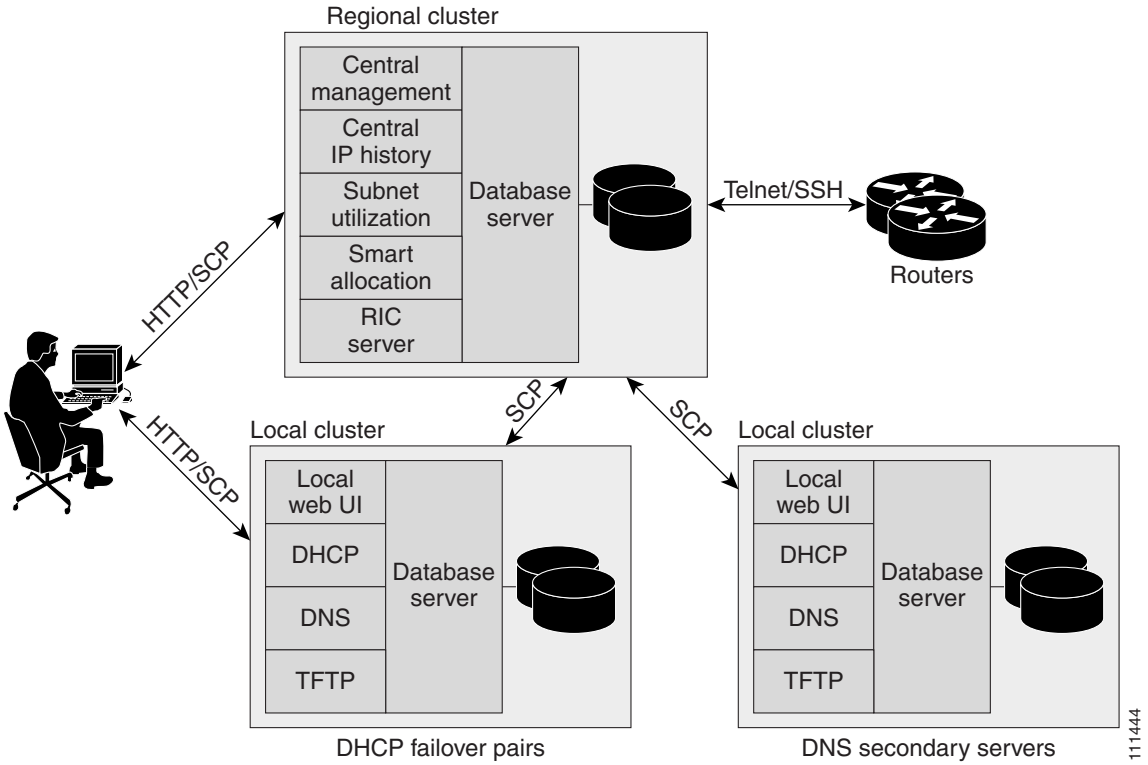
You can install Network Registrar in either local or regional mode:

- Local mode is used for managing local cluster protocol servers.
- Regional mode is used for managing multiple local clusters through a central management model.

A regional cluster centrally manages local cluster servers and their address spaces. The regional administrator can perform these operations:

- Push and pull configuration data to and from the local DNS and DHCP servers.
- Obtain subnet utilization and IP lease history data from the local clusters.
- Manage the router interface configuration (RIC) server that integrates with cable modem termination systems (CMTSs) directly from the regional cluster.

Figure 1-1 Network Registrar User Interfaces and the Server Cluster



System Requirements

Review these system requirements before installing the Network Registrar 7.0 software:

- Java—You must have the Java Runtime Environment (JRE) 5.0 (1.5.0_06) or later, or the equivalent Java Development Kit (JDK) installed on your system. (The JRE is available from Sun Microsystems on its website.)
- Operating system—Your Network Registrar machine must meet the minimum requirements on the Windows, Solaris, or Linux operating systems that are specified in Table 1-1 on page 1-3.)
- User Interface—Network Registrar currently includes two user interfaces: a web UI and a CLI:
  - The web UI runs on a minimum of Microsoft Internet Explorer 6.0 (Service Pack 2), Mozilla Firefox 1.5, or Netscape 7.0 and requires JRE 5.0 [1.5].
  - The CLI runs in a Windows, Solaris, or Linux command window.

Tip Include a network time service in your configuration to avoid time differences between the local and regional clusters. This method ensures that aggregated data at the regional server appears consistently.

Table 1-1 Network Registrar Server Minimum Requirements

Component	Windows	Solaris	Linux
CPU architecture	Intel Pentium III or its equivalent	Sun Netra AC200	Intel Pentium III or its equivalent
OS version	Windows 2003 server	Solaris 9 or Solaris 10	Red Hat Enterprise Linux ES 4.0
RAM	512 MB for all operating systems		
Disk space	18 GB recommended, minimum 310 MB required for installation		
Swap space	100 MB free swap space		

Installation Modes

The modes of installation that exist for the local and regional clusters are new installations and upgrades from a previous version with or without data migration. These installations or upgrades are performed by using operating-system-specific software installation mechanisms:

- Windows—InstallShield setup program
- Solaris—**pkgadd** command
- Linux—**install_cnr** script that uses RPM Package Manager (RPM)

License Files

Network Registrar now uses the FLEXlm licensing tool. Your license file defines the features of Network Registrar to which you have access. When you install the software, you are prompted to provide the name of the license file and its location. The name of the license file supported in Network Registrar 7.0 is ip-node.

An ip-node license gives you the right to manage a specified number of IP addresses. One license covers both IPv4 and IPv6 nodes. For example, to manage 24,000 IPv4 nodes and 10,000 IPv6 nodes in a local cluster, you must purchase an ip-node license that covers 34,000 total nodes.

This method also applies on a regional server. With a regional server, however, you must aggregate the licensed nodes from all managed local clusters. Consider the following scenario in which the regional server manages three local clusters:

- local cluster *A* has 24,000 IPv4 nodes and 10,000 IPv6 nodes
- local cluster *B* has 2,000 IPv4 nodes and 12,000 IPv6 nodes
- local cluster *C* has 48,000 IPv4 nodes and 1,000 IPv6 nodes

The regional cluster must have an ip-node license that covers 97,000 total nodes.

Backup Software and Virus Scanning Guidelines

If you have automatic backup or virus scanning software enabled on your system, exclude these Network Registrar directories and their subdirectories from being scanned. If they are not excluded, file locking issues can corrupt the databases or make them unavailable to the Network Registrar processes. If you are installing to the default locations, exclude the following directories and their subdirectories:

- Windows—

  install-path\data (for example, C:\Program Files\Network Registrar\Local\data and C:\Program Files\Network Registrar\Regional\data)
  install-path\logs (for example, C:\Program Files\Network Registrar\Local\logs and C:\Program Files\Network Registrar\Regional\logs)

- Solaris and Linux—

  install-path/data (for example, /var/nwreg2/local/data and /var/nwreg2/regional/data)
  install-path/logs (for example, /var/nwreg2/local/logs and /var/nwreg2/regional/logs)

Modifying ACLs in Windows Installations

The Network Registrar installation program for Windows does not try to modify ACLs to restrict access to installed files and directories. If you want to restrict access to these files and directories, use the native Microsoft utilities **cacls** and **icacls** to manually change file and directory permissions.

If you decide to manually change ACLs, Cisco recommends that you control the settings so that the contents of the entire installation area are read-only to everyone except those in the Administrators system group.

The following files and subdirectories are used to restrict access to the Administrators system group:

- *installdir***conf\cnr.conf**
- *installdir***tomcat\conf\server.xml**
- *installdir***conf\priv**
- *installdir***data**

  Modifying the ACLs is strictly optional, and Network Registrar will function normally without making any changes to them. Refer to documentation supplied by Microsoft for information about how to use the **cacls** and **icacls** utilities.

Server Event Logging

System activity begins logging when you start Network Registrar. The server maintains all the logs by default in these directories:

- Windows—Local cluster: C:\Program Files\Network Registrar\Local\logs;
  Regional cluster: C:\Program Files\Network Registrar\Regional\logs
- Solaris and Linux—Local cluster: /var/nwreg2/local/logs;
  Regional cluster: /var/nwreg2/regional/logs

  To monitor the logs, use the **tail -f** command.

Caution In Windows, to avoid losing the most recent system Application Event Log entries if the Event Log fills up, use the Event Viewer system application to click the **Overwrite Events as Needed** check box in Event Log Settings for the Application Log. If the installation process detects that this option is not set properly, it displays a warning message advising corrective action.

Running Performance Monitoring Software on Windows

On Windows systems only, if you uninstall Network Registrar and try to remove the associated data directories while having software installed that integrates with the Windows Performance Monitor, the software might take possession of certain shared libraries. This action prevents you from removing these files from the Network Registrar folder; hence, the directory itself. To keep this event from happening:

1. Stop the service that is associated with the performance monitoring software.
2. Delete the Network Registrar folder.
3. Restart the service.

Running Other Protocol Servers

You cannot run the Network Registrar DNS, DHCP, or TFTP servers concurrently with any other DNS, DHCP, and TFTP servers. In many Windows 2000 server systems, these services are enabled and running by default. If the Network Registrar installation process detects that a conflict exists, it displays a warning message.

Use one of these methods to change the Windows configuration from the Service Control Manager (**Control Panel > Administrative Tools > Services** in Windows 2000):

- Change the Microsoft servers from a Startup Type of Automatic to Manual or Disabled.
- Stop the Network Registrar protocol server that conflicts with the Microsoft one by using the Stop function in one of the user interfaces.

If you want to disable a protocol server and prevent the Network Registrar server from starting automatically after a system reboot, use the **server {dns | dhcp | tftp} disable start-on-reboot** command in the CLI.

Upgrading

Network Registrar 7.0 supports upgrades from releases 6.1.x, 6.2.x, and 6.3. The upgrade process differs slightly depending on the release from which you are upgrading. To preserve your existing configurations during the upgrade:

- From Network Registrar 5.5 or earlier, you must first upgrade to 6.1. You must then do a further upgrade to 6.2.1.
- You can upgrade to 6.2.1 while preserving the earlier configuration, or you can replace the configuration.

Improvements in the Network Registrar software database from release to release can result in important changes that affect the way that you use Network Registrar:

- The DHCP server's configuration changed substantially in 6.2. Attributes formerly set on a scope or DHCP server to configure DHCP failover, DNS updates and traps are now set separately and stored in new data objects. You cannot upgrade custom or vendor-specific DHCP options; you must reenter them using the new 6.2 functions.
- Beginning with Network Registrar 6.1.1, administrators and related data can be centrally managed, which allows administrators, groups, and roles to be defined centrally at one time and then populated throughout the system. To simplify central management, groups are used exclusively to associate administrators with roles. These groups now manage the role assignments.

  If you configured administrators with direct role assignments, the upgrade converts these role assignments to group assignments. Group names are created from role names by appending the suffix *-group*, with numbers appended as needed to avoid conflicting names. These groups are only created for the upgrade, but only for roles that have administrators associated with them.
- If you are upgrading from 6.0, a number of name changes to processes, utilities, and files occurred in 6.1 that can affect automated scripts that you have from previous releases.Table 1-2 summarizes these changes.

Table 1-2 Name Changes from Release 6.0

Previous Name	New Name	Change Action
AIC Server Agent 2.0	nwreglocal nwregregion Displays as Network Registrar Local (or Regional) Server Agent	Windows Network Registrar server name renamed to local and regional server names
/etc/init.d/aicservagt	/etc/init.d/nwreglocal /etc/init.d/nwregregion	Solaris and Linux start/stop script renamed
aicservagt.exe	cnrservagt.exe	Windows Network Registrar server agent executable file renamed
aicservagt	cnrservagt	Solaris and Linux Network Registrar server agent executable file renamed
mcdsvr.exe	ccmsrv.exe	Windows MCD server executable renamed to the CCM server
mcdsvr	ccmsrv	Solaris and Linux MCD server executable renamed to the CCM server
config_mcd_1_log	config_ccm_1_log	Server log file renamed
aicstatus	cnr_status	Solaris and Linux server status utility renamed

CHAPTER 2

Installing and Upgrading Network Registrar

This chapter describes how to install Network Registrar 7.0 on Windows, Solaris, or Linux systems. It includes these sections:

Checklist

Before you perform the installation or upgrade, ensure that you are prepared by reviewing this checklist:

- Does my operating system meet the minimum requirements to support Network Registrar 7.0? (See the "System Requirements" section on page 1-2.)
- Does my hardware meet the minimum requirements? (See the "System Requirements" section on page 1-2)
- If necessary, have I excluded Network Registrar directories and subdirectories from virus scanning? (See the "Backup Software and Virus Scanning Guidelines" section on page 1-4.)
- On Windows, are other applications closed, including any virus-scanning or automatic-backup software programs? Is the Debugger Users group included in the Local Users and Groups?
- Do I have the proper software license? (See the "License Files" section on page 1-3.)
- Am I authorized for the administrative privileges needed to install the software?
- Does the target installation server have enough disk space?
- Is this a new installation or an upgrade?
- Is the cluster mode of operation regional or local?
- Is this a full or client-only installation?
- Is the Java Runtime Environment (JRE) 5.0 (1.5.0_06) or later, or the equivalent Java Development Kit (JDK), installed on your system? If so, where?
- Is the Windows system set up to support 16-bit applications (short filenames)?

- Should the web UI use an HTTP or HTTPS connection, or both?
- Am I upgrading from an earlier version of Network Registrar? If so:
  - Are there any active user interface sessions?
  - Is my database backed up?
  - Is my Network Registrar task list empty?

Before You Begin

Verify that you are running a supported operating system and that your environment meets all other current system requirements (see the "System Requirements" section on page 1-2).

If you are running an unsupported operating system, back up your Network Registrar data and upgrade your operating system before installing this latest release:

Step 1 Use the currently installed Network Registrar release to complete any configuration changes in progress, so that the existing database is consistent before you perform the upgrade.

Step 2 Ensure that no pending database tasks result from recent edits. You can confirm that the task lists are empty by viewing the CCM and MCD Tasks pages under the Administration menu in the web UI. Wait until both lists are empty before proceeding with the update.

Step 3 Back up your database. The installation program tries to detect configuration data from an earlier installation and will upgrade the data.

Step 4 Upgrade your operating system.

About Network Registrar License Files

When you purchase Cisco Network Registrar 7.0, you receive a FLEXlm license file in an e-mail attachment from Cisco after you register the software.

You must copy the license file to a directory on the Network Registrar target machine before you attempt to install the software. Store the license file in any directory on the Network Registrar machine. The installation process asks you for the location of the license file.

To obtain a license file:

Step 1 Read the Software License Claim Certificate document packaged with the software.

Step 2 Note the Product Authorization Key (PAK) number printed on the certificate.

Step 3 Log in to one of the Web sites described on the certificate, and follow the registration instructions. The PAK number is required for the registration process.

You should receive the license file through e-mail within one hour of registration.

A typical license file might look like the following example:

```
FEATURE ip-node cisco 1.000 1-feb-2010 uncounted VENDOR_STRING=1000 \
    HOSTID=ANY SN=CNR12222006113344 NOTICE="<LicFileID>licenseFileName1 </LicFileID>
    SIGN=46764487EXMPL1
FEATURE ip-node cisco 1.000 3-mar-2037 uncounted VENDOR_STRING=50000 HOSTID=ANY \
    SN=CNR09082006112233 SIGN=776AB544EXMPL2
INCREMENT ipv6-node cisco 1.000 3-mar-2037 uncounted VENDOR_STRING=500000 HOSTID=ANY \
    SN=CNR09092006112233 SIGN=776AB544ZEXMPL3
```

Installation and Upgrade Procedure

Follow this procedure to install or upgrade Network Registrar. The procedure is essentially the same for a new installation or upgrade; except that the upgrade requires a few additional steps.

Note If you are upgrading to Network Registrar 7.0, be sure you have obtained license files to replace each license key. For more information, see the "About Network Registrar License Files" section on page 2-2.

Step 1 Log in to the target machine using an account that has administrative privileges:

- Windows—Account in the Administrators group
- Solaris and Linux—**su** (superuser) or root account

Windows—Close all open applications, including any antivirus software. Also ensure that the Dr. Watson visual notification setting is unchecked. This option prevents the servers from restarting automatically if a failure occurs until you respond to a pop-up dialog box. The Visual Notification check box in Dr. Watson is usually marked by default. Run **drwtsn32.exe** (in C:\WINDOWS\system32), uncheck the check box, then click **OK**. (Note that you can perform this step after the installation.)

Step 2 If you have not already done so, download and install the Java Runtime Environment (JRE) 5.0 (1.5.0_06) or later, or the equivalent Java Development Kit (JDK). These are available from Sun Microsystems at its Java download website.

Note On Windows, add the *\bin* subdirectory of your Java installation folder to your PATH environment variable.

Step 3 If you are not configuring secure login to the web UI, skip to Step 4. If you are configuring secure login, you must create a keystore file by using the Java **keytool** utility, which is located in the \bin subdirectory of the Java installation (see Step 2). Use the utility to define a self-signed certificate, or to request and later import a certificate from an external signing authority:

1. To create a keystore file containing a self-signed certificate, run this command and respond to the prompts:

```
> keytool -genkey -alias tomcat -keyalg RSA -keystore k-file
    Enter keystore password: password
    What is your first and last name? [Unknown]: name
    What is the name of your organizational unit? [Unknown]: org-unit
    What is the name of your organization? [Unknown]: org-name
    What is the name of your City or Locality? [Unknown]: local
    What is the name of your State or Province? [Unknown]: state
    What is the two-letter country code for this unit? [Unknown]: cc
    Is CN=name, OU=org-unit, O=org-name, L=local, ST=state, C=cc correct? [no]: yes
    Enter key password for <tomcat> (RETURN if same as keystore password):
```

The keystore filename (*k-file*) is its fully qualified path. You will be entering the keystore path and password in Step 13.

2. To create a Certificate Signing Request (CSR) that you will submit to the Certificate Authority (CA) when you request a certificate, create the keystore file as in the previous substep, then execute this command:

```
> keytool -certreq -keyalg RSA -alias tomcat -file certreq.cer -keystore k-file
  ...
```

Submit the resulting certreq.cer file to the CA. Once you receive the certificate from the CA, first download the Chain Certificate from the CA, then import the Chain Certificate and your new Certificate into the keystore file, as follows:

```
> keytool -import -alias root -keystore k-file -trustcacerts -file chain-cert-file
> keytool -import -alias tomcat -keystore k-file -trustcacerts -file new-cert-file
```

For details on the **keytool** utility, see the documentation at the Java website of Sun Microsystems. For details on the **keystore** file and Tomcat, see the documentation at the website of the Apache Software Foundation.

Caution The keystore password is stored in the server.xml file in the *install-path*\tomcat\conf directory, which is protected to have superuser access only. Because the password is visible as plain text in this file, do not change the file and directory permissions to make this file generally accessible.

Step 4 Load the installation CD, or browse to the network resource where the Network Registrar software is located. If you download a distribution file from the Cisco website, run it from a different directory than where you will install Network Registrar.

- Windows—The cnr_7_0-nt.exe file is a self-extracting executable file that places the setup file and other files in the directory where you run it. (If you are not configured for Autostart, run the setup.exe file in that directory.) The Welcome to Cisco Network Registrar window appears.

  Click **Next**. The second welcome window introduces the setup program and reminds you to exit all current programs, including virus scanning software. If any programs are running, click **Cancel**, close these programs, and return to the start of Step 4. If you already exited all programs, click **Next**.

- Solaris and Linux—Be sure that the **gzip** and **gtar** utilities are available to uncompress and unpack the Network Registrar installation files. See the GNU organization website for information on these utilities. Follow these steps:

  1. Download the distribution file.
  2. Navigate to the directory in which you will uncompress and extract the installation files.
  3. Uncompress and unpack the .gtar.gz file. Use **gtar** with the **–z** option:

     ```
     gtar -zxpf cnr_7_0-linux.gtar.gz
     ```

     To unpack the .gtar file that **gunzip** already uncompressed, omit the **–z** option:

     ```
     gtar -xpf cnr_7_0-linux.gtar
     ```

  4. Run this command or program:

     Solaris—Run the **pkgadd** command with the **–d** option that specifies the directory from which you are installing, with the **–a** option in case you want to upgrade from a previous release. The name of the Network Registrar package is **nwreg2**:

```
pkgadd -a install-path/solaris/nwreg2/install/cnradmin -d install-path/solaris nwreg2
```

Linux—Run the install_cnr script from the directory containing the installation files:

```
install-path # ./install_cnr
```

The *install-path* is the CD-ROM directory that contains the installation files or the directory that contains the extracted Network Registrar installation files, if they were downloaded electronically.

Step 5 Specify whether you want to install Network Registrar in the local or regional cluster mode (see the "About Network Registrar" section on page 1-1):

- Windows—Keep the default Network Registrar Local or choose Network Registrar Regional. Click **Next**. The Select Program Folder appears, where you determine the program folder in which to store the program shortcuts in the Start menu. Accept the default, enter another name, or choose a name from the Existing Folders list. Click **Next**.
- Solaris and Linux—Enter **1** for a local, or **2** for regional. The default mode is 1.

Note If you are upgrading, the upgrade process autodetects the installation directory from the previous release.

Step 6 Enter the filename, as an absolute or relative path, for your base license (see the "License Files" section on page 1-3).

Note Entering the filename during installation is optional. However, if you do not enter the filename now, you must enter it when you first log in to the web UI or the CLI.

Step 7 Note these Network Registrar installation directories and make any appropriate changes to meet your needs:

- Windows default locations:
  - Local cluster—C:\Program Files\Network Registrar\Local
  - Regional cluster—C:\Program Files\Network Registrar\Regional
- Solaris and Linux default locations:
  - Local cluster:

    Program files—/opt/nwreg2/local

    Data files—/var/nwreg2/local/data

    Log files—/var/nwreg2/local/logs

    Temporary files—/var/nwreg2/local/temp
  - Regional cluster:

    Program files—/opt/nwreg2/regional

    Data files—/var/nwreg2/regional/data

    Log files—/var/nwreg2/regional/logs

    Temporary files—/var/nwreg2/regional/temp

Step 8 Choose whether to archive the existing binaries and database in case this installation does not succeed. The default and recommended choice is **Yes** or **y**:

If you choose to archive the files, specify the archive directory. The default directories are:

Windows—Local cluster (C:\Program Files\Network Registrar\Local.sav); Regional cluster (C:\Program Files\Network Registrar\Regional.sav). Click **Next**.

Solaris and Linux—Local cluster (/opt/nwreg2/local.sav); Regional cluster (/opt/nwreg2/regional.sav)

Step 9 Choose the appropriate installation type: server and client (the default), or client-only:

- Windows—Choose **Both server and client (default)** or **Client only**. Click **Next.** The Select Port window appears.
- Solaris and Linux—Entering **1** installs the server and client (the default), or **2** installs the client only.

Note Choose **Client only** in a situation where you want the client software running on a different machine than the protocol servers. Be aware that you must then set up a connection to the protocol servers from the client.

Step 10 Choose the CCM management SCP port number. (You can change this port number on your target system.) These are the default port numbers:

- Local cluster—1234
- Regional cluster—1244

On Windows, click **Next**.

Step 11 Enter the location of the Java installation (JRE or JDK 1.5.0_06 selected in Step 2). (The installation or upgrade process tries to detect the location.)

- Windows—A dialog box reminds you of the Java requirements. Click **OK** and then choose the default Java directory or another one. Click **OK**. The Select Connection Type window appears.
- Solaris and Linux—Enter the Java installation location.

Note Do not include the bin subdirectory in the path. If you install a new Java version or change its location, rerun the Network Registrar installer, then specify the new location in this step.

Step 12 Choose whether to enable the web UI to use a nonsecure (HTTP) or secure (HTTPS) connection for web UI logins:

- Windows—Choose **Non-secure/HTTP (default)**, **Secure/HTTPS (requires JSSE)**, or **Both HTTP and HTTPS**.
- Solaris and Linux—Enter an HTTP port, a secure HTTPS port, or both HTTP and HTTPS ports.

Enabling the secure HTTPS port configures security for connecting to the Apache Tomcat web server (see Step 3 for configuration). (To change the connection type, rerun the installer, and then make a different choice at this step.)

- If you choose HTTPS, or HTTP and HTTPS, click **Next** and continue with Step 13.
- If you choose the default HTTP connection, click **Next**, and skip to Step 14.

Step 13 If you enabled HTTPS web UI connectivity, you are prompted for the location of the necessary .jar files:

- If you want to use a different JSSE installation than the default set in Step 2 for the .jar files, enter it.
- For the keystore location, specify the fully qualified path to the keystore file that contains the certificate(s) to be used for the secure connection to the Apache Tomcat web server. This is the keystore file that you created in Step 3.
- For the keystore password, specify the password given when creating the keystore file. On Windows, click **Next**.

Caution Do not include a dollar sign ($) in the keystore password as it will result in an invalid configuration on the Apache Tomcat web server.

Step 14 Enter a port number for the web UI connection. The defaults are:

- HTTP local cluster—8080
- HTTP regional cluster—8090
- HTTPS local cluster—8443
- HTTPS regional cluster—8453

On Windows, click **Next**.

The Network Registrar installation process begins. (Solaris prompts you to verify that you want to continue with the installation.) Status messages report that the installer is transferring files and running scripts. This process may take a few minutes:

- Windows—The Setup Complete window appears. Choose **Yes, I want to restart my computer now** or **No, I will restart my computer later** and then click **Finish**.
- Solaris and Linux—Successful completion messages appear.

Step 15 Verify the status of the Network Registrar servers:

- Windows—In the Services control panel, verify that the Network Registrar Local Server Agent or Network Registrar Regional Server Agent is running after rebooting the system when the installation has completed successfully.
- Solaris and Linux—Use the *install-path***/usrbin/cnr_status** command to verify status. See the "Starting and Stopping Servers" section on page 2-8.

Starting Network Registrar

To administer the local and regional clusters that you have installed, you must enter the contents of the appropriate license file (web UI) or the filename (CLI).

Follow this procedure to enter license information:

Step 1 Start the Network Registrar web UI or CLI:

- To access the web UI, open the Web browser and use the HTTP (nonsecure login) or HTTPS (secure login) website:

  http://*hostname***:***http-port*
  https://*hostname***:***https-port*

  where:

  – The *hostname* is the actual name of the target host.

  – The *http-port* and the *https-ports* are the default HTTP or HTTPS port that are specified during installation. (See the installation procedure, Step 14 on page 2-6).

On Windows, you can access the web UI from the Start menu from the local host:

- On a local cluster—Choose **Start > Programs > Network Registrar 7.0 > Network Registrar 7.0 local Web UI** (or **Network Registrar 7.0 local Web UI (secure)** if you enabled secure login).
- On a regional cluster—Choose **Start > Programs > Network Registrar 7.0 > Network Registrar 7.0 regional Web UI** (or **Network Registrar 7.0 regional Web UI (secure)** with secure login).

- To start the CLI:
  - Windows—Navigate to the *install-path*\bin directory and enter this command:

    ```
    nrcmd -C cluster-ipaddress -N admin -P changeme
    ```

  - Solaris and Linux—Navigate to the *install-path*\usrbin directory and enter this command:

    ```
    install-path/usrbin/nrcmd -C clustername -N admin -P changeme
    ```

Step 2 Enter the username **admin** and the password **changeme**.

Tip Cisco recommends that you change this password as soon as possible to maintain system security.

Step 3 If you did not enter license information during the installation procedure, you must do so now:

- Web UI—Enter the name of the license file on the Add License page. Optionally, click **Browse** to navigate to the license file.
- CLI—Enter an absolute or relative path for the license filename, as follows:

  ```
  nrcmd> license create filename
  ```

Starting and Stopping Servers

In Windows, you can stop and start the Network Registrar server agent from the Services feature of the Windows Control Panel. If the installation completed successfully and you enabled the servers, the Network Registrar DNS and DHCP servers start automatically each time you reboot the machine.

For the TFTP server, you must use this Network Registrar CLI command to enable it to restart on bootup:

```
nrcmd> tftp enable start-on-reboot
```

All servers in the cluster are controlled by the Network Registrar regional or local server agent. You can stop or start the servers by stopping or starting the server agent.

For details on stopping and starting servers, see the *Cisco Network Registrar User's Guide*.

Starting and Stopping Servers on Windows

Follow this procedure to start and stop servers on Windows:

Step 1 Choose **Start > Settings > Control Panel > Administrative Tools > Services**.

Step 2 From the Service list, choose **Network Registrar Local Server Agent** or **Network Registrar Regional Server Agent**.

Step 3 Click **Restart** or **Stop**, as required, and then click **Close**.

Starting and Stopping Servers on Solaris or Linux

In Solaris or Linux, the Network Registrar servers automatically start up after a successful installation or upgrade. You do not need to reboot the system. Follow this procedure to start and stop servers on Solaris or Linux:

Step 1 Log in as superuser.

Step 2 Start the server agent by running the nwreglocal or nwregregion script with the *start* argument:

```
# /etc/init.d/nwreglocal start ;for the local cluster
# /etc/init.d/nwregregion start ;for the regional cluster
```

Step 3 Enter the **cnr_status** command to check that the servers are running:

```
# install-path/usrbin/cnr_status
```

Step 4 Stop the server agent by running the nwreglocal or nwregregion script with the *stop* argument:

```
# /etc/init.d/nwreglocal stop ;for the local cluster
# /etc/init.d/nwregregion stop ;for the regional cluster
```

Troubleshooting the Installation

The Network Registrar installation process creates a log file, install_cnr_log, in the Network Registrar log file directory. For upgrades, two additional log files are created: mcdupgrade_log and lease_upgrade_log. The log directory is set to these locations by default:

- Windows:
  - Local cluster: C:\Program Files\Network Registrar\Local\logs
  - Regional cluster: C:\Program Files\Network Registrar\Regional\logs
- Solaris and Linux:
  - Local cluster: /var/nwreg2/local/logs
  - Regional cluster: /var/nwreg2/regional/logs

If the installation or upgrade does not complete successfully, first check the contents of these log files to help determine what might have failed. Some examples of possible causes of failure are:

- An incorrect version of Java is installed.
- Insufficient disk space is available.
- Inconsistent data exists for an upgrade.

If the log messages do not clearly indicate the failure, you can gather additional debug information by using the debug_install utility script. This script appears only if the installation failed and is located by default in the Network Registrar program files directory:

- Windows:
  - Local cluster: C:\Program Files\Network Registrar\Local\debug_install.cmd
  - Regional cluster: C:\Program Files\Network Registrar\Regional\debug_install.cmd
- Solaris and Linux:
  - Local cluster: /opt/nwreg2/local/debug_install.sh
  - Regional cluster: /opt/nwreg2/regional/debug_install.sh

If the `## Executing checkinstall script` part of the Solaris **pkgadd** fails, ensure that the /tmp directory has sufficient permissions to allow a nonprivileged installation user ID to write to it.

If you still need help determining the cause or resolution of the failure, forward the output of this script to Cisco Systems for further analysis. To contact Cisco for assistance, see the following Cisco website:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

Uninstalling Network Registrar

Follow the appropriate procedure to uninstall Network Registrar. The procedure differs based on which operating system you are using. (You must have administrator or superuser privileges to uninstall Network Registrar, just as you must to install it.)

To back up your database before uninstalling Network Registrar, see the *Cisco Network Registrar User's Guide* for the procedure.

Note Uninstallation stops the Network Registrar server agents first. If you find that the server processes are not shutting down, see the "Starting and Stopping Servers" section on page 2-8.

Uninstalling on Windows

Follow this procedure to uninstall Network Registrar on Windows:

Step 1 Choose the Add/Remove Program function from the Windows control panel, or the Uninstall Network Registrar choice from the Windows Start menu Network Registrar shortcut folder. The uninstallation program removes the server and user interface components but does not delete user data files.

Step 2 Optionally, delete all Network Registrar data by deleting the Network Registrar folder.

Note Temporarily stop any service that is related to software that integrates with Performance Monitoring that might interfere with removing shared libraries in the Network Registrar folder.

Step 3 Reboot after the uninstallation completes to finish the uninstall process.

Uninstalling on Solaris

Follow this procedure to uninstall Network Registrar on Solaris:

Step 1 From the root account, use the **pkgrm** program to remove the **nwreg2** package:

```
pkgrm nwreg2
```

The uninstallation procedure removes the server and user interface components; but does not delete user data, such as the log and data files.

Step 2 Optionally, delete the database and log files that are associated with Network Registrar, as mentioned in the instructions at the end of the **pkgrm** process.

Uninstalling on Linux

Follow this procedure to uninstall Network Registrar on Linux:

Step 1 Run the **uninstall_cnr** program from the *install-path*/usrbin directory:

```
./uninstall_cnr
Stopping Server Agent...
Deleting startup files...
Removing Network Registrar...
cannot remove /opt/nwreg2/usrbin - directory not empty
cannot remove /opt/nwreg2/conf - directory not empty
package optnwreg2 not found in file index
Note that any files that have been changed (including your database) have _not_ been
uninstalled. You should delete these files by hand when you are done with them, before you
reinstall the package.
```

The `cannot remove` warnings mean that, although the uninstall program removes the server and user interface components, it cannot delete directories that are not empty. Certain configuration and data files that are created during installation remain deliberately after uninstallation.

Step 2 Optionally, delete the database and log files that are associated with Network Registrar, as mentioned in the instructions at the end of the **uninstall_cnr** script execution.

APPENDIX A

Performing a Silent Installation

This appendix describes how to perform a silent installation, upgrade, or uninstallation of the Network Registrar product. A silent installation or upgrade allows for unattended product installations based on the configuration values that are provided at the time that a silent installation response file was created.

Caution You must use a "clean install" mode silent-response file for fresh installations, and an "upgrade" mode silent-response file for product upgrades. The configuration values specified in the silent-response files are specific to a particular installation or upgrade environment, and cannot be mixed and matched. Unpredictable results occur if you attempt to use a silent-response file that does not exactly match the installation or upgrade system configuration.

Follow these procedures to generate a silent installation response file:

Step 1 For each silent installation or upgrade, use these commands to create a separate response file:

- Windows:

  setup.exe -r

  Complete the installation or upgrade steps as you normally would. This command installs or upgrades Network Registrar according to the parameters that you specified. It also generates the setup.iss response file based on these parameters. Look for this file in the Windows installation directory, such as C:\WINDOWS. Each time you use the command, the file is overwritten.

  Cisco recommends that you rename or relocate this file before running the silent-process in Step 2. Rename the file to something distinguishable, such as local-nr-https-install, and relocate it to a temporary folder.

- Solaris:

  pkgask -d *install-path* **-r** *response-file* **nwreg2**

  Complete the installation or upgrade steps as you normally would. This action does not actually install or upgrade Network Registrar, but simply generates a response file by the specified name that includes the installation or upgrade parameters that you want to replicate for additional installations or upgrades. Cisco recommends that you name the file something distinguishable, such as local-nr-upgrade or regional-nr-https-install.

- Linux:

  Create a text response file with these variable declarations (modify the values to suit the desired configuration for your system):

```
BACKUPDIR=/opt/nwreg2.sav
CCM_PORT=1234
CNR_CCM_MODE=local | regional
CNR_EXISTS=n
DATADIR=/opt/nwreg2/local | regional/data
INSTALL_DEBUG=n
JAVADIR=/usr/java/jdk1.5.0_06
JSSEDIR=n
KEYSTORE_FILE=keystore
KEYSTORE_PASSWORD=changeit
LOGDIR=/opt/nwreg2/local | regional/logs
PERFORM_BACKUP=n
ROOTDIR=/opt/nwreg2/local | regional
SKIP_VALIDATION=n
START_SERVERS=y
TEMPDIR=/opt/nwreg2/local | regional/temp
USE_HTTP=y
USE_HTTPS=n
WEBUI_PORT=8080 | 8090
WEBUI_SEC_PORT=8443 | 8444
```

Step 2 Use these commands to invoke the silent installation or upgrade for each instance:

- Windows:

  setup.exe -s -f1*path+response-file*

  Note that the silent installation fails if you do not specify the **–f1** argument with a fully qualified path to the response file, unless the response file is located in the i386 directory and setup.exe is run from that directory.

- Solaris:

  pkgadd -a *pkgdir***/nwreg2/install/cnradmin -d** *pkgdir* **-r** *response-file* **nwreg2**

- Linux:

  install_cnr -r *response-file*

Step 3 If you want to uninstall the product, invoke the silent uninstallation:

- Windows:

  uninst.exe -y -f"*install-dir***\DeIsL1.isu" -c"***install-dir***\unregistrar.dll"**

- Solaris:

  pkgrm -a *pkgdir***/nwreg2/install/cnradmin -n nwreg2**

- Linux (this command is noninteractive except during an error):

  uninstall_cnr

APPENDIX B

Lab Evaluation Installations

This appendix describes how to install, upgrade, and uninstall Network Registrar regional and local clusters on a single machine to support smaller test configurations for evaluation purposes.

Caution Installing the regional and local clusters on a single machine is intended only for lab evaluations, and should not be chosen for production environments. The aggregated regional cluster databases are expected to be too large to be reasonably located with a local server that is also running DNS or DHCP services. Running out of free disk space causes these servers to fail.

Installing Network Registrar in a Lab

Follow this procedure to install Network Registrar on a single machine for evaluation purposes:

Step 1 Before you run the installation program, check that the machine has enough disk space to accommodate two separate installations of Network Registrar.

Step 2 Install or upgrade the local cluster on the machine, according to the procedures in Chapter 2, "Installing and Upgrading Network Registrar." Specify the Local cluster installation. In Windows, do not reboot.

Step 3 Install or upgrade the regional cluster on the same machine, according to the same procedures. Specify the Regional cluster installation. In Windows, this time reboot.

Testing the Lab Installation

Follow this procedure to test the installation:

Step 1 Start and log in to the web UI for the local cluster, using the URL appropriate to the port number. By default, the local port numbers are **8080** for HTTP connections and **8443** for HTTPS (secure) connections. In Windows, from the Start menu, choose **Network Registrar 7.0 local Web UI**.

Step 2 Add DNS zones and DHCP scopes, templates, client-classes, or virtual private networks (VPNs) as a test to pull data to the regional cluster.

Step 3 Start and log in to the web UI for the regional cluster, using the URL appropriate to the port number. By default, the regional port numbers are **8090** for HTTP connections and **8453** for HTTPS (secure) connections. In Windows, from the Start menu, choose **Network Registrar 7.0 regional Web UI**.

Step 4 Test the regional cluster for single sign-on connectivity to the local cluster. Try to pull DNS zone distributions, DHCP scopes, templates, client-classes, or VPNs from the local cluster to the regional replica database.

Uninstalling in a Lab Environment

If you need to uninstall Network Registrar, follow the procedure in the "Starting and Stopping Servers" section on page 2-8.

No option exists to uninstall only the regional or local cluster in a dual-mode installation environment.

INDEX

J

K

L

M

N

O

P

R

S

T

U

V

W