CHAPTER 1

Overview

This guide describes how to install Cisco Network Registrar (CNR) Release 7.2 on Windows, Solaris, and Linux operating systems, and how to install the CNR Virtual Appliance. You can also see the following documents for important information about configuring and managing CNR:

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

About Cisco Network Registrar

CNR 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 the following 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 CNR 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.

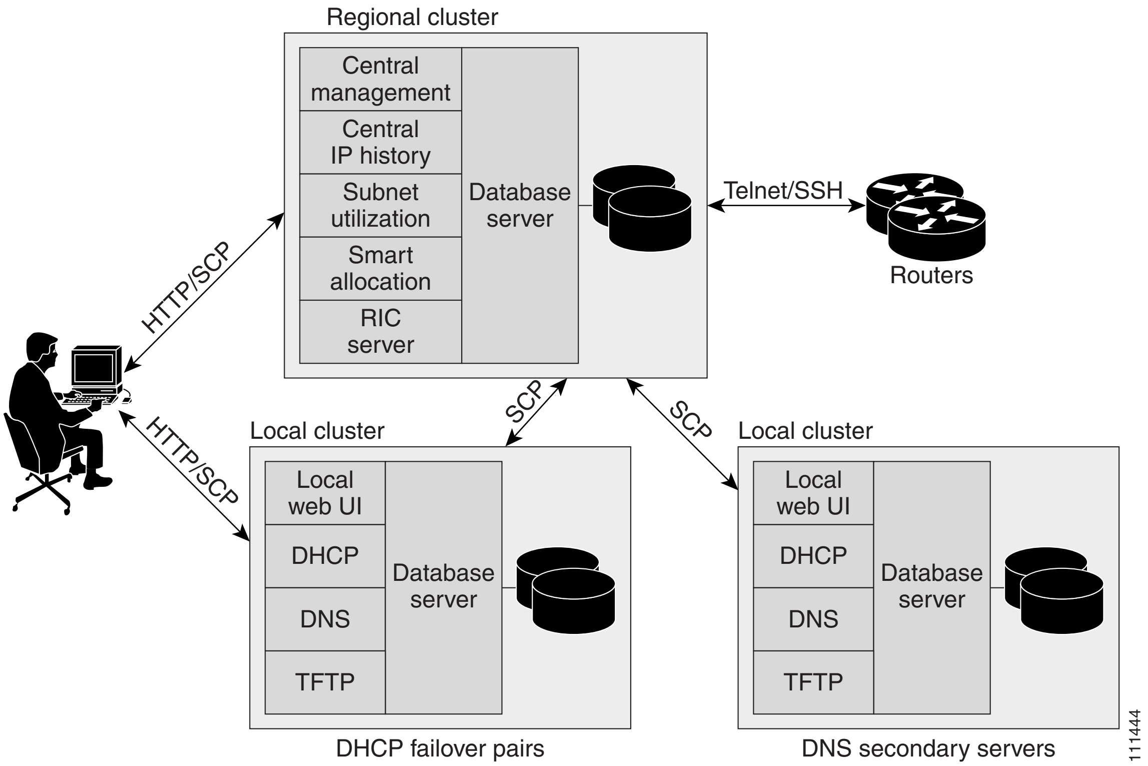
You can install CNR in either local or regional mode:

- 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 the following 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 Cisco Network Registrar User Interfaces and the Server Cluster



System Requirements

Review the system requirements before installing the CNR 7.2 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 Oracle on its website.)
- Operating system—We recommend that your CNR machine run on the Windows, Solaris, or Linux operating systems as described in Table 1-1 on page 1-3. CNR must run on 32-bit or 64-bit operating systems.

Note CNR applications are 32-bit applications and the system should support 32-bit applications (Java JRE/JDK, OpenLDAP library (for RH)).

- User Interface—CNR currently includes two user interfaces: a web UI and a CLI:
  - The web UI runs on Microsoft Internet Explorer 7.1 and 8.0, Mozilla Firefox 3.0 and 3.5, and requires JRE 5.0 [1.5.0_06].
  - 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 the aggregated data at the regional server appears consistently.

Table 1-1 CNR Server Minimum Requirements

	Operating System		
Component	**Solaris**[1]	**Linux**	**Windows**
OS version[2]	Solaris 10[3]	• Red Hat Enterprise Linux ES 5.0[4]	Windows Server 2008 R2[4]
Disk space[5]	2 x 73/146 SAS[6] drives	With basic DHCP and optimal hardware configuration: • SATA[7] drives with 7500 RPM drive > 500 leases/second • SAS drives with 15K RPM drive > 1000 leases/second Recommended hard drive—146 GB	
Memory[8]	16 GB	Small networks—4 GB, Average networks—8 GB, or Large networks—16 GB	

[1] Solaris support is restricted to Solaris Sparc.

[2] CNR must run on 32-bit or 64-bit operating systems.

[3] CNR 7.2 supports 128-KB block sizes in the Solaris 10 ZFS.

[4] CNR 7.2 supports running in a VMWARE (ESX Server 3.5) and LDOM environment for Red Hat Enterprise Linux ES 5.0, and Windows Server 2008 R2. CNR 7.2 supports running in Cisco Unified Computing System (CUCS) and Sun Sparc Enterprise T5220.

[5] Higher I/O bandwidth usually results in higher average leases per second.

[6] Serial Attached SCSI.

[7] Serial Advanced Technology Attachment (Serial ATA).

[8] Faster CPU and more memory typically result in higher peak leases per second.

Note If you are upgrading from an earlier version of CNR to CNR 7.2, on the Solaris platform, make sure you upgrade the Solaris version as mentioned in "Installation and Upgrade Procedure" section on page 2-3.

Installation Modes

The modes of installation that exist for the local and regional clusters are new installations and upgrades from a previous version. 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

CNR uses the FLEXlm licensing tool. Your license file defines the features of CNR to which you have access. When you install the software, you are prompted to provide the name of the license file and its location. You can give any name to the license file. You must specify this file name while you install CNR.

A CNR license file gives you the right to manage a specified number of IP addresses. A single 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 license that covers 97,000 total nodes.

To learn about obtaining the license files for CNR, see "Obtaining Network Registrar License Files" section on page 2-2.

Backup Software and Virus Scanning Guidelines

If you have automatic backup or virus scanning software enabled on your system, exclude the CNR 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 CNR processes. If you are installing on the default locations, exclude the following directories and their subdirectories:

Note In this documentation set, when *install-path* is used, it refers to all or part of the installation paths that were specified when installing CNR.
As an example using the Solaris and Linux default local cluster paths of /opt/nwreg2/local and /var/nwreg2/local, the *install-path* may represent these paths or just the /opt/nwreg2 or /var/nwreg2 portion.

- Windows—

  install-path\data (for example, C:\NetworkRegistrar\Local\data and C:\Network Registrar\Regional\data)
  install-path\logs (for example, C:\NetworkRegistrar\Local\logs and C:\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 CNR 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, we recommend 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 sub directories contain data that you may want only the Administrators system group to access:

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

Modifying the ACLs is strictly optional, and CNR will function normally without making any changes to them. See 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 CNR. The server maintains all the logs by default in the following directories:

- Windows—Local cluster: C:\NetworkRegistrar\Local\logs;
  Regional cluster: C:\NetworkRegistrar\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 and check 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 if you uninstall CNR 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 CNR folder and the directory itself. To keep this 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 CNR DNS, DHCP, or TFTP servers concurrently with any other DNS, DHCP, and TFTP servers. If the CNR installation process detects that a conflict exists, it displays a warning message.

On Windows systems, use one of the following methods to change the configuration from the Service Control Manager:

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

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