



Release Notes for Cisco Network Registrar Release 7.0

December 18, 2007

These release notes are for Cisco Network Registrar Release 7.0. This document describes system requirements, new features in this release, installation notes, caveats, and documentation updates.

Contents

These release notes cover the following topics:

- [Introduction, page 2](#)
- [System Requirements, page 2](#)
- [Software and Standards Compatibility, page 3](#)
- [Interoperability, page 4](#)
- [Installation and Upgrade Notes, page 4](#)
- [Software Features Added in Release 7.0, page 6](#)
- [New Features in the Documentation Set for Network Registrar, page 13](#)
- [Important Notes, page 14](#)
- [Limitations and Restrictions, page 16](#)
- [Related Documentation, page 17](#)
- [Obtaining Documentation and Submitting a Service Request, page 17](#)



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

Introduction

This release of Cisco Network Registrar provides:

- User interface enhancements
- Dynamic DNS for DHCPv6 features
- DHCPv6 leasequery
- DOCSIS 3.0 support
- DHCPv6 extensions
- IPv6 address management
- Enhanced search capabilities
- New documentation features

For more information about these features see the [“Software Features Added in Release 7.0”](#) section on page 6 and the [“New Features in the Documentation Set for Network Registrar”](#) section on page 13.

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 web site.)
- Operating system—Your Network Registrar machine must meet the minimum requirements of the Windows, Solaris, or Linux operating systems that are specified in [Table 1](#). Network Registrar must run on 32-bit operating systems.

Table 1 **Network Registrar Server Requirements**

Component	Windows	Solaris	Linux
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		
* Network Registrar 7.0 does not support 128KB block sizes in the Solaris 10 ZFS file system.			
**Network Registrar 7.0 supports only this specific release of Red Hat Linux.			



Note

The version of Java packaged with Red Hat Linux Enterprise Server 4.0 is not compatible with Network Registrar. Use Java 5.0 (1.5) or later.

Network Registrar no longer supports the following platforms: Red Hat ES 2.1, Red Hat 3.0, and Solaris 8.

- User Interfaces—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.



Note For the CLI, the number of concurrent active user sessions and processes on a cluster can be no more than 14.



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.

Software and Standards Compatibility

Cisco Network Registrar 7.0 is compatible with Cisco Broadband Access Center 4.0. This software release complies with the applicable RFCs, protocols, standards, and Internet drafts as it did in prior releases. With the features introduced in this release, the software conforms to these additional documents:

- Dynamic Host Configuration Protocol (DHCP) Leasequery (RFC-4388).
- A DNS Resource Record (RR) for Encoding Dynamic Host Configuration Protocol (DHCP) Information (DHCID RR) (RFC-4701).
- Resolution of Fully Qualified Domain Name (FQDN) Conflicts among Dynamic Host Configuration Protocol (DHCP) Clients (RFC-4703).
- The Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Client Fully Qualified Domain Name (FQDN) Option (RFC 4704).
- The DHCP Leasequery (RFC 5007).
- New option support added the following RFCs
 - **RFC 4174**—The IPv4 Dynamic Host Configuration Protocol (DHCP) Option for the Internet Storage Name Service
 - **RFC 4280**—Dynamic Host Configuration Protocol (DHCP) Options for Broadcast and Multicast Control Servers
 - **RFC 4388**—Dynamic Host Configuration Protocol (DHCP) Leasequery
 - **RFC 4580**—Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Relay Agent Subscriber-ID Option
 - **RFC 4649**—Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Relay Agent Remote-ID Option
 - **RFC 4776**—Dynamic Host Configuration Protocol (DHCPv4 and DHCPv6) Option for Civic Addresses Configuration Information
 - **RFC 4833**—Timezone Options for DHCP
 - **RFC 4994**—DHCPv6 Relay Agent Echo Request Option

Interoperability

The Network Registrar 7.0 protocol servers (DHCP, DNS, TFTP, and SNMP) interoperate with the protocol servers in versions 6.0 and later with the exception of the DNS HA and DHCPv6 servers. The 7.0 DNS HA server interoperates with the 6.2 DNS HA server.

Cisco strongly recommends, however, that you use Network Registrar 7.0 DNS servers when configuring DNS updates from DHCPv6 lease activity because these updates use the new DHCID RR to identify the client using the name or address. The DHCID RR is new and not supported by earlier Network Registrar releases. DNS updates from DHCPv4 lease activity still use TXT RRs; and, therefore, you can use earlier versions of the Network Registrar DNS server with them.

The 7.0 regional Central Configuration Management server interoperates with prior versions.

Installation and Upgrade Notes

Review the following points before beginning a new installation or an upgrade. For information about installing the Network Registrar SDK, see the [“Installing the SDK” section on page 15](#).

- Network Registrar now implements the FLEXlm licensing mechanism; therefore, you must obtain a FLEXlm license file.

The installation program prompts you for the license file. You can defer submitting a license file during the upgrade, but you must provide one when you invoke the web UI or the CLI. License keys obtained for prior versions of Network Registrar no longer function.

- 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. See the *Installation Guide for Cisco Network Registrar* for more information.
- Windows, Solaris, and Linux installations occur through these means:
 - Windows—Windows-based InstallShield setup program.
 - Solaris—The **pkgadd** command.
 - Linux—The **install_cnr** script that uses RPM Package Manager (RPM).
- On Windows, close all currently running applications, including any antivirus software.
- On Windows, ensure that you uncheck the Dr. Watson Visual Notification check box. If checked, 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 checked by default. Execute C:\WINNT\system32\DRWTSN32.exe, uncheck the **Visual Notification** check box, and then click **OK**. (You can perform this step after installation.)
- To avoid losing the most recent log entries when the Application Event Log is full in the Windows Event Viewer, 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.
- Because Network Registrar maintains lock files in the \Temp directory on Windows and the /tmp directory on Solaris or Linux, do not delete these directories while Network Registrar is running.

- You cannot run the Network Registrar DNS, DHCP, or TFTP servers concurrently with any other DNS, DHCP, and TFTP servers. In many Windows 2000 and 2003 server systems, these services are enabled and running by default. If the Network Registrar installation process detects that a conflict may exist, it displays a warning message. Before installing Network Registrar, take the appropriate action to disable the conflicting servers.

**Note**

Network Registrar includes a list of informational, activity, warning, and error messages that it logs during certain operating conditions. Obtain this list in HTML files for each component as links from a **MessageIDIndex.html** file. By default:

Windows—

C:\Program Files\Network Registrar\{Local | Regional}\Docs\Msgid\MessageIDIndex.html

Solaris and Linux—

/opt/nwreg2/{local | regional}/docs/msgid/MessageIDIndex.html

Upgrade Paths

Network Registrar 7.0 supports upgrades from releases 6.1.x, 6.2.x, and 6.3. When you install the software, the installation program automatically detects an existing version and transparently upgrades the software to the latest release. The program first prompts you to archive existing Network Registrar data. If the program encounters errors during the upgrade, it rolls back the software to the earlier release.

Network Registrar no longer supports the Red Hat ES 2.1, Red Hat 3.0, and Solaris 8 operating systems. See [Table 1 on page 2](#) for currently supported operating systems. Back up your Network Registrar data and upgrade your operating system before installing this latest release.

Complete these tasks before starting the upgrade:

-
- | | |
|---------------|--|
| Step 1 | Ensure that your environment meets the current system requirements (see Table 1 on page 2). |
| Step 2 | Use the currently installed release to complete any configuration changes in progress, so that the existing database is consistent before you perform the upgrade. |
| Step 3 | 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 4 | Back up your database. The installation program tries to detect configuration data from an earlier installation and will upgrade the data. |
-

Software Features Added in Release 7.0

This section describes the most important changes made in Release 7.0.

User Interface Enhancements

The Network Registrar web UI now supports:

- Choice of user modes in the local cluster web UI
- Simplified configuration through the introduction of a Setup interview
- Enhanced search capabilities
- Server status dashboard to monitor system health and view statistics in real time
- Application-wide and per-user preference settings for web page size (items displayed on a page) and web UI mode

User Modes

The local cluster web UI is now available in three user modes:

- Basic mode (the preset choice) provides a means to configure the most often used objects, such as DHCP scopes and DNS zones. Basic mode is new in this release.
- Advanced mode provides access to additional objects such as address blocks, subnets, and IP address ranges. Advanced mode is similar to the web UI available in previous releases, but with some enhancements.
- Expert mode should be used only with the guidance of the Cisco Technical Assistance Center to troubleshoot your configuration.

You can switch between Basic and Advanced mode by clicking **Basic** or **Advanced** at the top left of the page. You can also add Expert mode by setting User Preferences (see the [“Per-User Preferences” section on page 8](#)).

Setup Interview

Beginning with Release 7.0, the web UI on the local cluster provides a setup environment in Basic user mode. The setup is in the form of a series of interview pages, very much like a wizard, based only on the selections you make.

Enhanced Searching

The Network Registrar 7.0 web UI enables server-wide searching for live DHCP and DNS data.

**Note**

Enhanced searching is available only at the local cluster.

You can search for the following live data:

- DHCPv4 lease searches without the user having to know or guess the containing Scope (or VPN).
- DHCPv6 lease searches without the user having to know or guess the containing Prefix (or VPN).
- DNS RR and IP address searches without the user having to know or guess the containing Zone (forward, reverse, or secondary).



Note

The results that appear after a search are static and change only when you click **Search**; that is, if you navigate to an object from a search page and then edit it, the edits will not appear in the search results page when you return to it. Similarly, if other edits result in objects being added or removed from the system (for example, leases), this will not affect the contents of an earlier search. To ensure you are looking at the most current data, click **Search** again.

Server Status Dashboard

The Network Registrar server status dashboard presents a graphical view of the system status, using graphs, charts, and tables, to help in tracking and diagnosis. These dashboard elements are designed to convey system information in an organized and consolidated way, and include:

- Significant protocol server and other metrics
- Alarms and alerts
- Database inventories
- Server health trends

The dashboard is best used in a troubleshooting desk context, where the system displaying the dashboard is dedicated for that purpose and might be distinct from the systems running the protocol servers. The dashboard system should point its browser to the system running the protocol servers.

Application-Wide Preferences

To set application-wide preferences in the web UI:

-
- Step 1** Click **Servers**, then **Manage Servers**.
 - Step 2** Click the **Local CCM Server** link to open the Edit CCM Server page.
 - Step 3** Change the attribute values, such as the *webui-mode* (Basic, Advanced, or Expert). (If need be, change the view to **Show Group View** to see the attributes listed alphabetically.)
 - Step 4** Click **Modify CCM Server**.
 - Step 5** Stop, then restart Network Registrar.
-

Per-User Preferences

To set per-user preferences in the web UI:

-
- Step 1** Click **Home**, then **User Preferences**.
 - Step 2** On the Edit User Preferences for Current User page, change the web page size and mode.
 - Step 3** Click **Modify User Preferences**. The changes take place right away, and are in effect the next time you log in to the web UI.
-

DNS Updates for DHCPv6

Network Registrar now supports updates to DNS in a DHCPv6 environment. This support includes:

- AAAA and PTR mappings for DHCPv6 leases.
- Synthesized fully qualified domain names and the DHCPv6 Client FQDN option. Client names may be synthesized by the server or by an extension. Release 7.0 adds support for a DHCPv6 extension to completely specify the hostname and domain name to allow Broadband Access Center (BAC) and other applications to perform PacketCable provisioning.
- DNS updates for stateful addresses. Delegated prefix leases do not support DNS updates.
- DHCPv4 and DHCPv6 DNS updates over IPv4 only. DNS updates over IPv6 are not currently supported.

DNS updates for DHCPv6 use existing DHCPv4 configuration information; policies can specify DnsUpdateConfig objects, which configure all aspects of the DNS updates. The DHCP support implements this capability as described in RFC-4701, RFC-4703, and RFC-4704. This release thus makes use of the DHCID RR for DHCPv6 DNS updates.



Note

Limiting the DHCID RR to DHCPv6 clients has implications for dual stack clients even if they support RFC 4361. The clients cannot use a single forward fully-qualified domain name because DHCPv4 updates use TXT RRs and DHCPv6 uses DHCID RRs. Conflict resolution rules do not allow the name to be used by both at the same time. This is primarily an issue for client requested names; generated names are typically generated in a way to make them unique.

The DNS server supports the DHCID RR (RFC-4701) in the following ways:

- Properly handling DHCID records in DDNS updates
- Sending and receiving DHCID records in zone transfers
- Resolving queries for DHCID type records
- Exchanging DHCID RRs as part of HA message exchanges
- Adding, deleting, and modifying DHCID RR types using SCP messages

DHCPv6 Leasequery

The Network Registrar Leasequery for DHCPv6 (RFC-5007) available in Release 7.0 is designed to:

- Support the source-verify capability of DHCPv6-aware cable modem termination systems (CMTSs).
- Provide data to additional processes that need real-time information about DHCP lease and client activity (such as Cisco Broadband Access Center).
- Implement a pending RFC for DHCPv6 Leasequery.

Leasequery enables on-demand, programmatic retrieval of data related to the operation of DHCPv6 servers. Leasequery can extract lease information about IPv6 addresses and delegated prefixes.

Available query types are by IPv6 address and by client identifier (DUID).

Data Over Cable Service Interface Specification (DOCSIS) 3.0

Network Registrar now implements the latest DOCSIS 3.0 option definitions based on published documents and pending CableLabs engineering change requests (ECRs).



Note

Full DOCSIS 3.0 support requires use of Cisco Broadband Access Center, or a similar solution, because Network Registrar provides the infrastructure for DOCSIS 3.0 but not the full solution to completely provision cable modems.

CableLabs Options

DOCSIS 3.0 support primarily consists of new options that you configure in the CLI or the web UI. The DHCP server needs these options to decode, display, and return configured values to clients. The DHCP server also provides special handling for a few options because they cannot be configured by administrators but are integral to the operation of DOCSIS 3.0.



Note

The CableLabs DOCSIS 3.0 standard defines several new options for DHCPv4 and DHCPv6. For the full list of required RFCs and Internet-Drafts, refer to the CableLabs *Data-Over-Cable Service Interface Specifications, DOCSIS 3.0, MAC and Upper Layer Protocols Interface Specification*, CM-SP-MULPIv3.0-I01-060804, Annex H (DHCPv6) and Annex I (DHCPv4).

The DOCSIS 3.0 DHCPv6 options are as follows:

- CableLabs Vendor-Specific Information options:
 - CL_OPTION_ORO (Option Request)
 - CL_OPTION_TFTP_SERVERS (TFTP Server Addresses)
 - CL_OPTION_CONFIG_FILE_NAME (Configuration File Name)
 - CL_OPTION_SYSLOG_SERVERS (Syslog Server Addresses)
 - CL_OPTION_TLV5 (TLV5 Encoding, see CM-SP-RFIV2.0, Annex C.1.3.1)
 - CL_OPTION_DEVICE_ID (DOCSIS Device Identifier)
 - CL_OPTION_CCC (Client Configuration) - placeholder for PacketCable/CableHome
 - CL_OPTION_RFC868_SERVERS (RFC 868 Time Server Addresses)

- CL_OPTION_TIME_OFFSET (Time Offset From UTC)
- CL_CM_MAC_ADDR (DOCSIS Relay Agent CM MAC Address)
- CL_OPTION_CMTS_CAP (Relay Agent CMTS Capabilities) and its suboptions (1 = DOCSIS version number)
- The DOCSIS 3.0 DHCPv4 options (CableLabs Vendor-Specific Information Options):
 - CL_V4OPTION_ORO (Option Request Option)
 - CL_V4OPTION_TFTP_SERVERS (TFTP Server Addresses)
 - CL_V4OPTION_CMTS_CAP (Relay Agent CMTS Capabilities) and its suboptions (1 = DOCSIS version number)

DHCPv6 Relay Agent Options

Network Registrar also implements the following options, which are referenced but not required by DOCSIS 3.0:

- DHCPv6 Relay Agent Remote ID Option [RFC-4649]
- DHCPv6 Relay Agent Subscriber-ID Option [RFC-4580]
- DHCPv6 Vendor-Specific Information PacketCable/CableHome for Device Class [RFC-3315]
- DHCPv6 Relay Agent Echo Request Option [RFC-4994]

DHCPv6 Extensions

Network Registrar 7.0 builds on its prior support for DHCPv4 extensions to add support for DHCPv6 request processing. Extensions enable you to alter DHCP server processing through customer-written code (in C/C++ or TCL). An extension can alter the client identity, client class, options received or returned, and more.

Changes implemented in 7.0 are not limited to use with and for DHCPv6:

- Use extension points for DHCPv4, DHCPv6, or both. For backwards compatibility, DHCPv4 only is assumed. These extension points are called at essentially the same places during the server's processing, although in some cases an extension point can be called multiple times for a single client request because a client may request multiple leases or be given multiple leases.
- Set a new environment dictionary data item (this is required) to make sure that an **init-entry** extension point registers whether the extension affects DHCPv6 only or DHCPv4 and DHCPv6.
- Control lease address and delegated prefix generation with the **generate-lease** extension point. If attached, the extension is called at least once for each DHCPv6 lease the server generates. This is a DHCPv6-only extension and can be used to control address assignment and prefix delegation.
- Allow an extension to clean up any context it might have associated with a request using the **environment-destructor** extension point. If attached, the extension is *always* called immediately before the environment dictionary is destroyed, even if another extension or the server drops the request and no other extension point for this extension was called.
- Gain direct access to a received packet and potentially alter that packet before it is decoded, using the **pre-packet-decode** extension.
- Gain direct access to a response packet before it is sent to the client for potential alteration, using the **post-packet-encode** extension. This access allows the extension to change the packet before it is delivered to the client.

- Support the more complex and hierarchical nature of DHCPv6 options. These new methods are also available for DHCPv4 and are more tightly integrated with the option definitions introduced in Network Registrar 6.2.
- Support the more complex nature of the DHCPv6 server's data. This method provides access to the multiple leases and prefixes that may be associated with a single DHCPv6 client.
- Provide new data items to the environment, request, and response dictionaries.

For more information about the use of extension points with both DHCPv4 and DHCPv6, see the *User Guide for Cisco Network Registrar, 7.0*

Client-Class Changes

To simplify configuration and for compatibility between DHCPv4 and DHCPv6 the following changes occurred in this release of Network Registrar:

- The **one-shot** action flag is deprecated and removed from DHCPv4. Instead, use **inhibit-all-renews**. To implement this change, create an embedded policy, if none exists in the client-class or client-entry, and enable **inhibit-all-renews**.



Caution

DCHPv6 supports **inhibit-all-renews**, but Cisco strongly recommends that you use care if you enable this flag. With this flag enabled, memory is quickly consumed.

- The **use-release-grace-period** action is also deprecated and removed from DHCPv4. Additionally, this release simplifies release grace support by deprecating:
 - The server **allow-release-grace-period** attribute
 - The server **use-release-grace-period** attribute
 - The scope **use-release-grace-period** attribute
 - The client-class and client-entry **use-release-grace-period** attribute.

To use release-grace-periods, just configure the **release-grace-period** attribute (viz 3) on the appropriate policy.

IPv6 Address Management in the Web UI

The web UI now:

- Displays prefixes, links, and scopes in lists filtered by VPN. Prefix list pages may be sorted by name or address. The address space for IPv6 also includes new parent prefixes.
- Supports link-template and prefix-template. You can create these templates and use them to facilitate creating prefixes and links.
- Provides improved error reporting for expression validation and evaluation.

IPv6 Address Management in the CLI

This release of Network Registrar:

- Introduces new CLI commands.
 - **link**, replaces **dhcp-link**, which is still valid.
 - **link-policy**, replaces **dhcp-link-policy**, which is still valid.
 - **prefix**, replaces **dhcp-prefix**, which is still valid.
 - **link-template**, enables you to create, modify, or show the link-template.
 - **prefix-template**, enables you to create, modify, or show the prefix-template.
- Modifies CLI commands.
 - **dhcp**, adds new reporting options:


```
dhcp getScopeCount [FailoverPair name | vpn name | ALL]
```

```
dhcp getPrefixCount [vpn name | ALL]
```
 - **dns**, adds new reporting options:


```
dns getZoneCount [forward | reverse | primary | secondary | published |
unpublished | ALL]
```

```
dns getRRCount [zone name | forward | reverse | primary | secondary | published |
unpublished | ALL]
```



Note

The new and modified commands are fully documented in the Network Registrar CLI Reference Guide, available in HTML format. To access this information, follow the steps provided in the [“New Features in the Documentation Set for Network Registrar”](#) section on page 13.

New Features in the Documentation Set for Network Registrar

Two new significant changes to the documentation are introduced in this release:

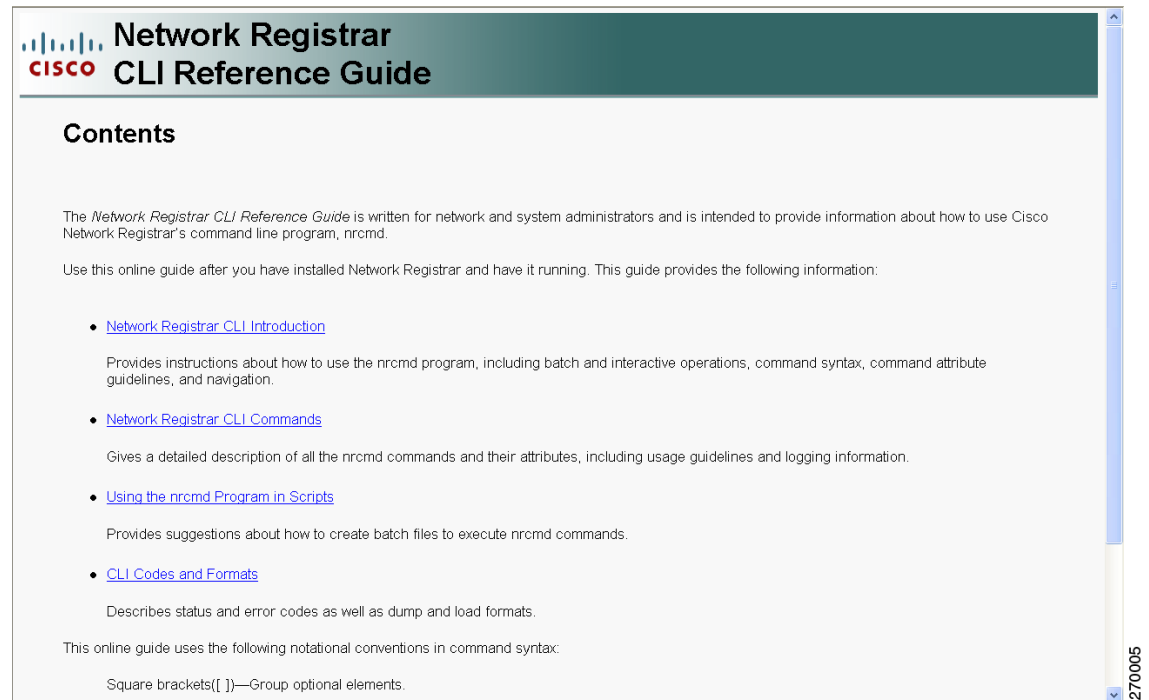
- New delivery mechanism for the Network Registrar CLI Reference Guide.
- Complete revision of the web UI help system.

New Delivery Mechanism for the CLI Reference Guide

The *Cisco Network Registrar CLI Reference Guide* is now delivered as an HTML document that you can view in your web browser when you install the software. To use the reference guide:

- Step 1** Open the directory or filesystem where you installed the software.
- Step 2** On Windows, go to `\Network Registrar\Local\docs`. The path is similar on Solaris and Linux.
- Step 3** Click `CLIContents.html`. Your web browser displays the Contents page for the document (see [Figure 1](#)).

Figure 1 Contents Page for Network Registrar CLI Reference Guide



- Step 4** Click the links to open sections of the reference guide.

Revision of the Web UI Help System

Now when you click **Help** in the web UI, a separate browser window displays the complete *User Guide for Cisco Network Registrar* in the appropriate context; that is, the guide opens to the relevant topic based on the web UI page you are on. The window shows a Contents pane and a text pane with navigation functions. The Contents pane also has Index and Favorites tabs so that you can access the book index and set the current topic as a favorite for future access. The help system also includes a search and print function as well as a glossary function to access the Cisco Internetworking Terms and Acronyms page over the web.

Important Notes

This section contains important information related to this software release that was unavailable when the user documentation was completed; and it contains information in response to recent customer queries. This section describes:

- Modifying the configuration file (cnr.conf)
- Installing the SDK
- CLI prompt change

Modifying the Configuration File (cnr.conf)

The cnr.conf file contains important configuration information. In rare cases, you might want to modify the file; for example, to exclude certain data from daily backups due to capacity issues. To do this, you need to add the appropriate settings manually.



Caution

In most situations, Cisco recommends that you use the default settings in this file. If you must change these settings, do so only in consultation with the Cisco Technical Assistance Center (TAC) or the Network Registrar development team.

The following settings are supported:

- **cnr.backup-dest**—Specify the destination to place backed-up databases. Defaults to cnr.datadir if not specified.
- **cnr.backup-dbs**—Provide a comma-separated list of the databases you want to back up. For a local cluster the default is **ccm,dhcp,dns,mcd,cnrsnmp**. For a regional cluster it is **ccm,leasehist,subnetutil,replica**.



Note

The raima (mcd) database is always included in a back-up.

- **cnr.backup-files**—Provide a comma-separated list of files and the complete path to the files that you want copied as part of the backup. Files are copied to cnr.backup-dest. The default action is to copy *install/conf/mcdschema.txt*.

- **cnr.dbrecover-backup**—Specify whether or not to run **db recover** and **db verify** on a backed-up Sleepy Cat database. The default value is **true**. This setting is used for daily backups only, and manual backups ignore this setting. Disabling the automatic operation means that you must run the operation manually, preferably on a separate machine, or at a time when the CNR servers are relatively idle.
- **cnr.daily-backup**—Specify whether to run the daily backup. The default is **true**.

Installing the SDK

This section documents how to install the Network Registrar SDK on Linux, Solaris, and Windows platforms.

Installing on Linux or Solaris

1. Extract the contents of the distribution tar file.
 - a. Create the SDK directory:


```
% mkdir /cnr-sdk
```
 - b. Change to the directory you just created and extract the tar file contents:


```
% cd /cnr-sdk
% tar xvf <sdk tar file location>/cnrsdk.tar
```
2. Export your LD_LIBRARY_PATH and CLASSPATH environment variable.


```
% export LD_LIBRARY_PATH=/cnr-sdk/lib
% export CLASSPATH=/cnr-sdk/classes/cnrsdk.jar:.
```

Installing on Windows

1. Extract the contents of the distribution tar file.
 - a. Create the SDK directory:


```
> md c:\cnr-sdk
```
 - b. Change to the directory you just created and extract the zip file contents:


```
>c:
>cd \cnr-sdk
>tar xvf <sdk tar file location>\cnrsdk.tar
```

You may optionally use winzip to extract cnrsdk.tar to the c:\cnr-sdk directory.
2. Set your PATH and CLASSPATH variables:


```
>set PATH=%PATH%;c:\cnr-sdk\lib
>set CLASSPATH=c:\cnr-sdk\classes\cnrsdk.jar;.
```

Testing Your Installation

On Linux or Solaris, the following test program verifies that you have set your PATH or LD_LIBRARY_PATH correctly:

```
%java -jar /cnr-sdk/classes/cnr-sdk.jar
```

On Windows, the following test program verifies that you have set your CLASSPATH correctly:

```
>java -jar c:\cnr-sdk\classes\cnr-sdk.jar
```

CLI Prompt Change

When you use the **session set current-vpn=name** command to set the VPN used for subsequent operations from the global (default) VPN to the specified VPN, the **nrcmd** prompt changes. In Network Registrar 7.0, the *-vpn-name* is appended to the **nrcmd** prompt when the current VPN is not the default (global vpn); For example:

```
nrcmd -vpn-example1>
```

Limitations and Restrictions

This section describes limitations and restrictions you might encounter using Network Registrar 7.0.

- In situations where a DHCPv6 server supports clients with multiple leases, be aware that the demand on server memory increases. DHCPv4 supports only one lease per client, while DHCPv6 supports multiple leases. Therefore, a DHCPv6 server cannot support as many leases (clients) as can the same server running DHCPv4. For example, one DHCPv6 client might require 2,500 bytes of space compared to 1,000 bytes per DHCPv4 client. This comparison means that a machine that would support one million DHCPv4 clients will only support 400,000 DHCPv6 clients. Cisco recommends that you allow three times the memory for DHCPv6 clients as you would for DHCPv4. As a result, you must:
 - Be aware of how many prefixes per link are configured. If the configuration has two prefixes on a link, then with default configuration parameters, you have to cut in half the number of clients.
 - Use care if you enable inhibit-all-renews. When enabled, each client would use at least two leases, and perhaps three, depending on the grace and affinity times per prefix.
 - Be aware that the max-client-leases value is now pre-set to 50. A known issue exists, and if clients renew rapidly, you quickly reach the limit of 50 leases per client, consuming much more memory.
- An issue is known to exist when Network Registrar 7.0 attempts to push a subnet to cable interface on a Cisco 10000 series uBR running Cisco IOS 12.2(8.22.34). Network Registrar can push subnets to Ethernet and GigaEthernet interfaces on the Cisco 10000 series, but it cannot push subnets to cable interfaces. Push subnets to bundled cable interfaces, instead.

Defects

You can find the complete list of resolved and known bugs in the `cnr_7_0-buglist.html` file included with the release. Refer to this list especially for information about fixes to customer-reported issues.

Related Documentation

See also the following documents for important information about installing, configuring, and managing Network Registrar:

- For Network Registrar installation procedures, see the *Installation Guide for Cisco Network Registrar*.
- To become familiar with Network Registrar features, see the *Quick Start Guide for Cisco Network Registrar*.
- For configuration and management procedures, see the *User Guide for Cisco Network Registrar*.
- For details about commands available through the command line interface (CLI), see the “[New Delivery Mechanism for the CLI Reference Guide](#)” section on page 13 for information about the new delivery mechanism and the location of the reference material.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

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

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

This document is to be used in conjunction with the documents listed in the “[Related Documentation](#)” section.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.

