



Network Registrar Components

Cisco CNS Network Registrar provides the tools to configure and control the servers necessary to manage your IP address space. This chapter provides an overview of the related management and network concepts and protocols.

Management Components

Network Registrar contains two management components:

- Regional component, consisting of:
 - Web-based user interface (Web UI)
 - Command line interface (CLI)
 - Central Configuration Management (CCM) server to provide to local cluster, address space, and router management
- Local component, consisting of:
 - Web UI
 - CLI
 - CCM server
 - Domain Name System (DNS) server
 - Dynamic Host Configuration Protocol (DHCP) server
 - Trivial File Transport Protocol (TFTP) server
 - Simple Network Management Protocol (SNMP) server
 - Router Interface Configuration (RIC) server
 - Management of local address space, zones, scopes, DHCPv6 prefixes and links, and users

The remainder of this chapter describes the TFTP and SNMP protocols. The CCM server, Web UIs, and CLI are described in [Chapter 2, “Network Registrar User Interfaces.”](#) The DNS, DHCP, and RIC server are described in their respective sections of this manual.

Trivial File Transfer

The Trivial File Transfer Protocol (TFTP) is a way of transferring files across the network using the User Datagram Protocol (UDP), a connectionless TCP/IP transport layer protocol. Network Registrar maintains a TFTP server so that systems can provide device provisioning files to cable modems that comply with the Data Over Cable Service Interface Specification (DOCSIS) standard. The TFTP server buffers the DOCSIS file in its local memory as it sends the file to the modem. After an TFTP transfer, the server flushes the file from local memory. TFTP also supports non-DOCSIS configuration files.

Here are some of the features of the Network Registrar TFTP server:

- Complies with RFCs 1350 and 1123.
- Includes a high performance multithreaded architecture.
- Caches data for performance enhancements.
- Is configurable and controllable in the Web UI and using the **tftp** command in the CLI.
- Includes flexible path and file access controls.
- Includes audit logging of TFTP connections and file transfers.
- Has a default root directory in the Network Registrar *install-path/data/tftp*.

Simple Network Management

The Network Registrar Simple Network Management Protocol (SNMP) notification support allows you to be warned of error conditions and possible problems with the DNS and DHCP servers, and to monitor threshold conditions that may indicate failure or impending failure conditions.

Network Registrar implements SNMP Trap Protocol Data Units (PDUs) according to the SNMPv1 standard. Each trap PDU contains:

- Generic-notification code, if enterprise-specific.
- Specific-notification field that contains a code indicating the event or threshold crossing that has occurred.
- Variable-bindings field that contains additional information about certain events.

Refer to the Management Information Base (MIB) for the details. You can find the MIB in the locations based on the operating system in the following subsections. The MIB requires these files to compile:

- SNMPv2-SMI.my
- SNMPv2-CONF.my
- SNMPv2-TC.my
- CISCO-TC.my
- CISCO-SMI.my

These individual MIBs are available at this public website:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

You will find the CISCO-NETWORK-REGISTRAR-MIB.my file at these locations in the default Network Registrar installation:

- Windows—*install-path/misc*
- Solaris and Linux—*install-path/misc*

How Notification Works

Network Registrar SNMP notification support allows a standard SNMP management station to receive notification messages from the two servers. These messages contain the details of the event that triggered the SNMP trap.

Network Registrar generates notifications in response to predetermined events that are detected and signaled by the application code. In addition to the knowledge that a particular event occurred, each event can also carry with it a particular set of parameters or current values. For example, the *free-address-low-threshold* event may occur in the FDDI-Devices scope with a value of 10 percent free. Other scopes and values are also possible for such an event and each type of event can have different parameters associated with it. The scope level threshold settings override those set globally.

Table 1-1 describes the events that can generate notifications.

Table 1-1 Notification Events

Event	Result
Address conflict with another DHCP server detected	Notification when an address conflict with another DHCP server is detected.
Configuration mismatch	Notification when a configuration mismatch between DHCP failover partners occurs.
DNS queue becomes full	Notification when the DHCP server's DNS queue fills and the DHCP server stops processing requests. This is a rare internal condition.
Duplicate IP address detected	Notification whenever a duplicate IP address is detected.
Change in free address count	The <i>free-address-low</i> trap when the number of free IP addresses becomes less than or equal to the low threshold; or a <i>free-address-high</i> trap when the number of free IP addresses exceeds the high threshold after having previously triggered the <i>free-address-low</i> trap.
Other server not responding	Notification when another server (DHCP, DNS, or LDAP) stops responding to the DHCP server.
Other server responding	Notification when another server (DHCP, DNS, or LDAP) responds after having been unresponsive.
Server start	Notification whenever the DHCP or DNS server is started or reinitialized.
Server stop	Notification whenever the DHCP or DNS server is stopped.

Handling Notification Events

When Network Registrar generates a notification, a single copy of the notification is transmitted as an SNMP Trap PDU to each recipient. The list of recipients and other notification configuration data are shared by all events (and scopes) and are read when the server is initialized.

You configure notifications for each protocol server by setting the server's SNMP attributes in the Web UI or the *traps-enabled* attribute for the server in the CLI. For example, the SNMP attributes for the DHCP server are available in the local cluster Web UI by clicking **Servers**, then the DHCP server on the Manage Servers page. The SNMP attributes are halfway down the Edit DHCP Server page (see Figure 1-1).

Figure 1-1 SNMP Attributes on the Edit DHCP Server Page (Local)

Attribute	Value	Data Type	Default	Unset?
Enabled Traps (traps-enabled)	<input type="checkbox"/> all <input type="checkbox"/> server-start <input type="checkbox"/> server-stop <input type="checkbox"/> free-address-low <input type="checkbox"/> free-address-high <input type="checkbox"/> dns-queue-size <input type="checkbox"/> other-server-down <input type="checkbox"/> other-server-up <input type="checkbox"/> duplicate-address <input type="checkbox"/> address-conflict <input type="checkbox"/> failover-config-error	flags		<input type="checkbox"/>
default-free-address-config	<input type="text"/>	name reference		<input type="checkbox"/>

149346

You can also set the default free-address trap configuration for the DHCP server (which affects all scopes not explicitly configured) by setting the *default-free-address-config* attribute.

In the local cluster CLI, use **dhcp set traps-enabled=value** to set the value of the traps. You can also set the *default-free-address-config* attribute in the same way. For example:

```
nrcmd> dhcp set traps-enabled=server-start,server-stop,free-address-low,free-address-high
```

You can also set the scope (or scope template) configuration specifically by setting the *free-address-config* attribute. The DNS server also includes a *traps-enabled* setting.

To use SNMP notifications on your system, you must specify trap recipients. These recipients indicate where Network Registrar notifications are directed. By default, all notifications are enabled, but no trap recipients are defined. Until you define the recipients, no notifications are sent. To define trap recipients:

- In the Web UI, click **Servers**, then the name of the SNMP server to open the Edit SNMP Server page. On that page, click **List Trap Recipients** to open the List/Add Trap Recipients page. On that page, enter the name and IP address of the trap recipient, then click **Add Trap Recipient**.
- In the CLI, use **trap-recipient**, in the following syntax:

```
nrcmd> trap-recipient name create ip-addr=ip-addr
```

The DHCP server has a special configuration for traps so that it can send notifications, especially about free addresses, to the SNMP server. In the Web UI, the trap configuration is available if you click **DHCP**, then **Traps** to open the List Trap Configurations page. On this page, click **Add Trap Configuration** to open the Add Trap Configuration page (see [Figure 1-2](#)).

Figure 1-2 Add Trap Configuration Page (Local)

Attribute	Value	Data Type	Default
name*	<input type="text"/>	string	
mode	[scope] <input type="button" value="v"/>	32-bit enum	scope
enable	<input type="radio"/> on <input type="radio"/> off	boolean	on
low-threshold	<input type="text"/>	percentage	20%
high-threshold	<input type="text"/>	percentage	25%

149347

On this page, enter the name, mode, and percentages for the low threshold and high threshold. The mode determines how scopes aggregate their free address levels: by scope, network, or selection tags. The low and high thresholds of free addresses are set to 20% and 25%, respectively. The modes are:

- Scope mode—Causes the scopes to track their own free address levels independently.
- Network mode—Causes all scopes set with this trap configuration (through the *free-address-configuration* attribute) to aggregate their free-address levels if they share a *primary-subnet* setting.
- Selection-tags mode—Causes scopes to aggregate their free-address levels if they share a primary subnet and their *selection-tag-list* matches.

The configuration is enabled by default (*enable=on*). After making these settings, click **Add Trap Configuration**.

In the CLI, use **addr-trap name create** followed by the attribute=value pairs for the settings; for example:

```
nrcmd> addr-trap ex-trap-conf create mode=scope low-threshold=25% high-threshold=30%
```

