



Maintaining Servers and Databases

This chapter explains how to administer and control your local and regional servers' operations through Cisco CNS Network Registrar's Web UI and CLI (the `nrcmd` program).

Controlling Servers

If you are assigned the server-management subrole of the `ccm-admin` role, you can control the Network Registrar servers as follows:

- Start—Load the database and start the server.
- Stop—Stop the server.
- Reload—Stop and restart the server.

Starting and stopping a server is self-explanatory. When you reload the server, Network Registrar performs three steps—stops the server, loads configuration data, and restarts the server. Only after you reload the server does it use your changes to the configuration.

In the Web UI, you can manage the protocol servers in two ways:

- If you are a local or regional cluster administrator, click **Servers** to open the Manage Servers page (see [Figure 6-1](#) for a local cluster example).

Figure 6-1 Manage Servers Page (Local)

Home Administration Servers Clusters Routers DHCP DNS Hosts Address Space												
Manage Servers												
Manage Servers on <i>bgassman-wxp</i>												
Page last refreshed: Mon Nov 21 15:34:31 EST 2005												
Name	IP Address	Type	State	Health	Statistics	View Log	View Startup Log	Start/Stop/Reload			Interfaces	
Local Server Agent	127.0.0.1	CNRAGENT	running		10 [N/A]		[N/A]	[N/A]	[N/A]	[N/A]	[N/A]	[N/A]
Local CCM Server	127.0.0.1	CCM	running		9 [N/A]			[N/A]	[N/A]	[N/A]	[N/A]	[N/A]
Local RIC Server	127.0.0.1	RIC	running		10 [N/A]		[N/A]	[N/A]	[N/A]	[N/A]	[N/A]	[N/A]
Local DHCP Server	127.0.0.1	DHCP	running		10							
Local DNS Server	127.0.0.1	DNS	running		10							
Local TFTP Server	127.0.0.1	TFTP	disabled		0 [N/A]							[N/A]
Local SNMP Server	127.0.0.1	SNMP	running		10 [N/A]		[N/A]			[N/A]		

149375

The local and regional cluster Web UI access to server administration is identical, even though the available functions are different. As a regional administrator, you can check the state and health of the regional CCM server, server agent, and Router Interface Configuration (RIC) server. However, you cannot stop, start, reload, or view statistics, logs, or interfaces for them.

At the local cluster, you can manage the DHCP, DNS, TFTP, and SNMP servers:






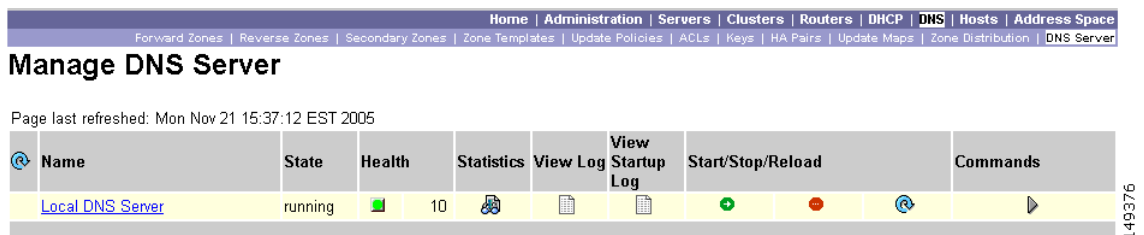




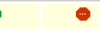

- Click the Statistics icon () to view statistics for the server.
 - Click the Log icon () in the View Log column to view the log messages for the server.
 - Click the Start icon () to start the server.
 - Click the Stop icon () to stop the server.
 - Click the Reload icon () to reload the server.
- If you are a local cluster DNS administrator, click **DNS**, then **DNS Server** to open the Manage DNS Server page (see [Figure 6-2](#)).

Figure 6-2 Manage DNS Server Page (Local)



Page last refreshed: Mon Nov 21 15:37:12 EST 2005

Name	State	Health	Statistics	View Log	View Startup Log	Start/Stop/Reload	Commands
Local DNS Server	running		10 				







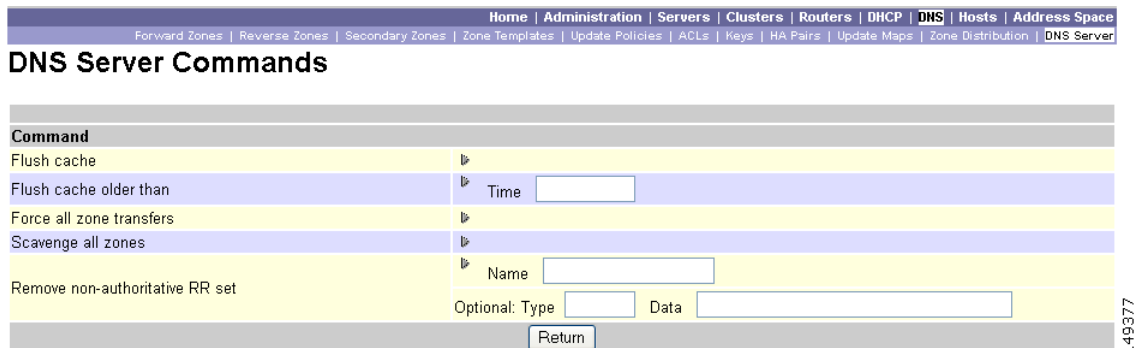



Along with the Statistics () , Log () , Start () , Stop () , and Reload () functions, you can also perform other functions when you click the Run icon () in the Commands column to open the DNS Server Commands page (see [Figure 6-3](#)).



Figure 6-3 DNS Server Commands Page (Local)



DNS Server Commands

Flush cache	
Flush cache older than	Time <input type="text"/>
Force all zone transfers	
Scavenge all zones	
Remove non-authoritative RR set	Name <input type="text"/> Optional: Type <input type="text"/> Data <input type="text"/>

The server command functions are:

- Flushing cache (see the [“Flushing DNS Cache” section on page 16-12](#))—Click the Run icon () . If you want to flush cache older than a certain time, enter the time in the Time field next to Flush cache older than, then click the Run icon. This is the equivalent of `dns flushCache` in the CLI.
- Forcing all zone transfers (see the [“Enabling Zone Transfers” section on page 14-13](#))—Click the Run icon () . This is the equivalent of `dns forceXfer secondary` in the CLI.

- Scavenging all zone transfers (see the “[Scavenging Dynamic Records](#)” section on [page 27-12](#))—Click the Run icon (▶). This is the equivalent of `dns scavenge` in the CLI.
- Removing nonauthoritative resource record sets (see the “[Removing Cached Records](#)” section on [page 15-4](#))—Enter the name of the RR set in the Name field, then click the Run icon (▶). If you optionally want to remove nonauthoritative RR sets based on specific types or data, enter these values in the Type or Data field, respectively. This is the equivalent of `dns removeCachedRR name type data` in the CLI.
- If you are a local cluster DHCP administrator, click **DHCP**, then **DHCP Server** to open the Manage DHCP Server page, which is similar to the Manage DNS Server page (see [Figure 6-2 on page 6-2](#)). Along with the Statistics (📊), Log (📄), Start (➕), Stop (⏹), and Reload (🔄) functions, you can also perform other functions when you click the Run icon (▶) in the Commands column to open the DHCP Server Commands page (see [Figure 6-4](#)).

Figure 6-4 DHCP Server Commands Page (Local)

This page provides the Get Leases with Limitation ID feature, to find clients that are associated through a common limitation identifier (see the “[Administering Option 82 Limitation](#)” section on [page 23-16](#)). Enter at least the IP address of the currently active lease in the IP Address field, then click the Run icon (▶). You can also enter the limitation ID itself in the form `nn:nn:nn` or as a string (“`nnnn`”), in which case the IP address becomes the network in which to search. This is the equivalent of `dhcp limitationList ipaddress limitation-id show` in the CLI.

In the CLI (the regional cluster allows CCM server management only):

- To start the server, use `server type start` (or simply `type start`; for example, `dhcp start`).
- To stop the server, use `server type stop` (or simply `type stop`; for example, `dhcp stop`). If stopping the server, it is advisable to save it first using the `save` command.
- To reload the server, use `server type reload` (or simply `type reload`; for example, `dhcp reload`). Network Registrar stops the server you chose, loads the configuration data, and then restarts the server.
- To set or show attributes for the server, use `[server] type set attribute=value` or `[server] type show`. For example:

```
nrcmd> ccm set ipaddr=192.168.50.10
```



Note

The DNS, DHCP, and SNMP servers are enabled by default to start on a reboot. The TFTP server is not enabled by default to start on a reboot. You can change this using `[server] type enable` or `disable start-on-reboot` in the CLI.

Logging Server Events

When you start Network Registrar, it automatically starts logging Network Registrar system activity. Network Registrar maintains all the logs by default on:

- Windows—*install-path*\logs
- Solaris and Linux—*install-path*/logs (to view these logs, use the **tail -f** command)



Tip

To avoid filling up the Windows Event Viewer and preventing Network Registrar from running, in the Event Log Settings, check the **Overwrite Events as Needed** box. If the events do fill up, save them to a file, then clear them from the Event Log.

Searching the Logs

The Web UI provides a convenient way to search for entries in the activity and startup log files. You can locate specific message text, log message IDs, and message timestamps using a regular expression string entry. When you click the Log icon (📄) in the View Log or View Startup column on the Manage Servers page (or one of the specific server pages), this opens a Log for Server page. In the text field next to the Search icon (🔍) at the top of the page, enter the search string in the regular expression syntax. (For example, entering **name?** searches for zero or one occurrence of the string “name” in the log file.)

Clicking the Search icon opens a Log Search Result page in a separate browser window (see Figure 6-5 for an example). The page shows the log file, line number of the match, and the log number.

Figure 6-5 Log Search Result Page (Local)

Log Search Result for Warning

FileName	Match Line Number	Log Number
name_dhcp_1_log	61	0
10/14/2005 11:25:47 name/dhcp/1 Warning Configuration 0 05336 Existing State didn't contain 'NextAvailableState'		
FileName	Match Line Number	Log Number
name_dhcp_1_log	63	0
10/14/2005 11:25:47 name/dhcp/1 Warning Configuration 0 05337 Existing State didn't contain 'CurrentState'		
FileName	Match Line Number	Log Number
name_dhcp_1_log	64	0
10/14/2005 11:25:47 name/dhcp/1 Warning Configuration 0 05346 Creating new State.		

149379

Click the name of the log message, which opens the Log for Server page with the full message text. Change between Table and Text view by clicking the Log icon (📄). Click **Close** on the Log Search Result page to close the browser window.

Logging Format and Settings

The server log entries include the following categories:

- Activity—Logs the activity of your servers.
- Info—Logs standard operations of the servers, such as starting up and shutting down.

- **Warning**—Logs warnings, such as invalid packets, user miscommunication, or an error in a script while processing a request.
- **Error**—Logs events that prevent the server from operating properly, such as out of memory, unable to acquire resources, or errors in configuration.

In the Web UI, you can affect which events to log. For example, to set the logging for the local cluster DNS and DHCP server:

- **DNS**—Click **DNS**, then **DNS Server** to open the Manage DNS Server page. Click the name of the server to open the Edit DNS Server page. Expand the Logging attributes section to view the log settings. Make changes to these settings as desired, click **Modify Server**, then reload the server.
- **DHCP**—Click **DHCP**, then **DHCP Server** to open the Manage DHCP Server page. Click the name of the server to open the Edit DHCP Server page. Expand the Logging section to view the log settings. Make changes to these settings as desired, click **Modify Server**, then reload the server.

In the CLI, use **dns set log-settings**, **dhcp set log-settings**, and **tftp set log-settings** for the respective servers.



Note

Warnings and errors go to Syslog on Solaris or the Event Viewer on Windows. See the Caution on page 6-4. For a description of the log messages for each server module, see the *install-path/docs/msgid/MessageIdIndex.html* file.

Log Files

Table 6-1 describes the Network Registrar log files in the *install-path/logs* directory.

Table 6-1 Log Files in .../logs Directory

Component	File in /logs Directory	Local/Regional	Logs
Installation	install_cnr_log	Both	Installation process
Upgrade	mcdupgrade_log	Both	Upgrade process
Server agent	agent_server_1_log	Both	Server agent starts and stops
Port check	checkports_log	Both	Network ports
DNS server	name_dns_1_log	Local	DNS activity
DHCP server	name_dhcp_1_log	Local	DHCP activity
TFTP server	file_tftp_1_log file_tftp_1_trace	Local	TFTP activity
SNMP server	cnrsnmp_log	Local	SNMP activity
RIC server	ric_server_log	Both	RIC server activity
CCM database	config_ccm_1_log	Both	CCM configuration, starts, stops
Web UI	cnrwebui_log	Both	Web UI state
Tomcat/Web UI (in cnrwebui subdirectory)	catalina_log.date.txt jsui_log.date.txt localhost_access_log.date.txt	Both	CCM database for Tomcat server and Web UI (because new files are created daily, periodically archive old log files)

Each component can generate a number of log files, each with a preconfigured maximum size of 1 MB. The first log file name has the `_log` suffix. When this file reaches its maximum size, it gets the `.01` version extension appended to its name and a new log file is created without the version extension. Each version extension is incremented by one for each new file created. When the files reach their configured maximum number, the oldest file is deleted and the next oldest assumes its name. The usual maximum number is four for the DNS, DHCP, and TFTP servers.

You can check the configured maximums for the DNS, DHCP, and TFTP servers using `[server] type serverLogs show` in the CLI, which shows the maximum number (`nlogs`) and size (`logsize`) of these protocol server log files. You can adjust these parameters using `[server] type serverLogs set nlogs=value` and `[server] type serverLogs set logsize=value`. You cannot adjust these maximums for any of the other log files.

**Note**

Some user commands can create *User authentication* entries in the Server Agent log because of separate connections to the cluster. Do not interpret these as a system security violation by another user.

Change Logs and Tasks

In the Web UI, you can view the change logs and tasks associated with configurations you make. Click **Administration**, and then **Change Log**, **CCM Tasks**, or **MCD Tasks**. To view the change log and tasks, you must be assigned the database subrole of the `ccm-admin` or `regional-admin` role. The resulting View Change Log page (see [Figure 6-6](#)) shows all the change logs, in reverse chronological order. Click the DBSN number of the change log entry to open a View Change Set page for it.

Figure 6-6 View Change Log Page (Local)

Date	[Month]	[Day]	[hh:mm:ss]	[Year]	Admin	Class Name	Object Name
Start							
End						Server Name	
<input type="button" value="Filter List"/> <input type="button" value="Clear Filter"/> <input type="button" value="older than"/> days							
DBSN	Date	Administrator	Entries				
60	Mon Nov 21 12:58:14 2005	admin	1				
59	Mon Nov 21 12:58:13 2005	admin	1				
58	Mon Nov 21 12:55:16 2005	admin	1				
57	Mon Nov 21 12:45:38 2005	(host-rr)	1				
56	Mon Nov 21 12:45:38 2005	(host-pttr)	1				
55	Mon Nov 21 12:45:38 2005	admin	1				
54	Mon Nov 21 12:45:04 2005	(host-rr)	1				
53	Mon Nov 21 12:45:04 2005	(host-pttr)	1				
52	Mon Nov 21 12:45:03 2005	admin	1				
51	Mon Nov 21 12:39:42 2005	(rrset-host)	1				

You can filter the list, manually trim it, and save it to a file. You can filter the list by:

- Start or end date
- Administrator who initiated the changes
- Configuration object class, or a specific object in that class
- Server (DNS, DHCP, TFTP, CCM, server agent, RIC, or SNMP)

Click **Filter List** or **Cancel Filter** (to cancel the filter that persists through the session). You can initiate a trim of the change log by setting how many days old you want the record to get before trimming it, by setting a value in the “older than” field and clicking the Delete icon (🗑️). To save the change log entries to a comma-separated values (CSV) file, click the Save icon (💾) in the left column.

If a task is associated with a change log, it appears on the View Change Set page. You can click the task name to open the View CCM Task or View MCD Task page for it.

Monitoring and Reporting Server Status

Monitoring the status of a server involves checking its:

- State
- Health
- Statistics
- Log messages
- Address usage
- Related servers (DNS and DHCP)
- Leases (DHCP)

Server States

All Network Registrar protocol servers (DNS, DHCP, SNMP, and TFTP) pass through a state machine consisting of the following states:

- Loaded—First step after the server agent starts the server (transitional).
- Initialized—Server was stopped or fails to configure.
- Unconfigured—Server is not operational because of a configuration failure (transitional).
- Stopped—Server was administratively stopped and is not running (transitional).
- Running—Server is running successfully.

The two essential states are initialized and running, because the server transitions through the states so quickly that the other states are essentially invisible. Normally, when the server agent starts the server, it tells the server to be up. The server process starts, sets its state to loaded, then moves up to running. If you stop the server, it walks down the states to initialized, and if you restart, it moves up to running again. If it fails to configure for some reason, it drops back to initialized, as if you had stopped it.

There is also an exiting state that the server is in very briefly when the process is exiting. The user interface can also consider the server to be disabled, but this rarely occurs and only when there is no server process at all (the server agent was told not to start one).

Displaying Health

You can display aspects of a server’s health, or how well it is running. The following items can decrement the server’s health, so you should monitor their status periodically. For the:

- Server agent (local and regional clusters)
- CCM server (local and regional clusters)

- DNS server (local cluster):
 - Configuration errors
 - Memory
 - Disk space usage
 - Inability to contact its root servers
- DHCP server (local cluster):
 - Configuration errors
 - Memory
 - Disk space usage
 - Packet caching low
 - Options not fitting in the stated packet limit
 - No more leases available
- TFTP server (local cluster):
 - Memory
 - Socket read or write error
 - Exceeding the overload threshold and dropping request packets
- RIC server (regional cluster)

**Tip**

Use the existence of any descending health values as a reminder to check the log files for the server.


In both the local and regional cluster Web UIs, click **Administration**, then **Servers**. Check the Manage Servers page for the state and health of each server (see [Figure 6-1 on page 6-1](#) for a DHCP server example).

In the local cluster CLI, use `[server] type getHealth`. The number 10 indicates the highest level of health, 0 that the server is not running.

**Tip**

On Solaris or Linux, you can run the `cnr_status` command, in the `install-path/usrbin/` directory, to see if your local cluster server is running. See the *Network Registrar Installation Guide*.

Displaying Statistics

To display server statistics, the server must be running. In the local cluster Web UI, go to the Manage Servers page, then click the Statistics icon () in the Statistics column. On the Server Statistics page, click the name of the attribute to get popup help.

The DHCP and DNS statistics are each divided into two groups of statistics. The first group is for total statistics and the second group is for sample statistics. The total statistics are accumulated over time. The sample statistics occur during a configurable sample interval. The names of the two categories vary per server and per user interface, and are identified in [Table 6-2](#).

Table 6-2 Server Statistics Categories

Server	User Interface	Total Statistics (Command)	Sample Statistics (Command)
DHCP	Web UI	Total Statistics	Activity Summary
	CLI	Total Counters since (dhcp getStats)	Sampled counters at (dhcp getStats sample)
DNS	Web UI	Total Statistics	Sample Statistics
	CLI	Total Counters since (dns getStats)	Sampled counters at (dns getStats sample)

To set up the sample counters, you must activate either the *collect-sample-counters* attribute for the server, or a *log-setting* attribute value called *activity-summary*. You can also set a *log-setting* value for the sample interval for each server, which defaults to 5 minutes. The *collect-sample-counters* attribute is set to true by default for the DNS server, but is set to false by default for the DHCP server. To enable the sample counters and set the interval for DHCP, set the following attributes:

```
nrcmd> dhcp enable collect-sample-counters
```

or

```
nrcmd> dhcp set log-settings=activity-summary
```

Then:

```
nrcmd> dhcp set activity-summary-interval
```


Note

You must enable *collect-sample-counters* so that you can query a server's initial interval counter values.

In the CLI, if you use [**server**] *type* **getStats**, the statistics are encoded in curly braces followed by sets of digits, as described in [Table 6-3 on page 6-10](#) for DNS, [Table 6-4 on page 6-13](#) for DHCP, and [Table 6-5 on page 6-14](#) for TFTP. The **server type getStats all** command is more verbose and identifies each statistic on a line by itself. As indicate in [Table 6-3](#), using the additional **sample** keyword shows the sample statistics only.

Reset the counters using **dhcp resetStats**. For example:

```
nrcmd> dhcp resetStats
```

DNS Statistics

The DNS server statistics appear in [Table 6-3](#). The table is organized by category, name and description of the statistic, and the digit position of the statistic in the output of the generic **dns getStats** command, in the format:

```
nrcmd> dns getStats
100 Ok
{1} 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
```

Table 6-3 DNS Statistics

Statistic	Description	Digit
General		
Server Identifier (id)	Implementation ID (release and build information).	{1}
Recursive Service (config-recurs)	Recursion services—(1) available, (2) restricted, (3) unavailable.	2
Process Uptime (config-up-time)	Time (in seconds) elapsed since the last server startup.	3
Time Since Reset (config-reset-time)	Time (in seconds) elapsed since the last server reset (restart).	4
Server Status (config-reset)	Status or action to reinitializes any name server state—If using the (2) reset action, reinitializes any persistent name server state; the following are read-only statuses: (1) other—server in some unknown state, (2) initializing, or (3) running.	5
Authoritative Answers (counter-auth-ans)	Number of queries answered authoritatively.	6
Authoritative No Such Name Answers (counter-auth-no-names)	Number of queries returning authoritative no such name responses.	7
Authoritative No Such Data Answers (counter-auth-no-data-resps)	Number of queries returning authoritative no such name (empty answer) responses.	8
Nonauthoritative Answers (counter-non-auth-datas)	Number of queries answered nonauthoritatively (cached).	9
Nonauthoritative No Such Data Answers (counter-non-auth-no-datas)	Number of queries answered nonauthoritatively with no data.	10
Forwarded Queries (counter-referrals)	Number of queries forwarded to other servers.	11
Error Responses (counter-errors)	Number of responses answered with errors (RCODE values other than 0 or 3).	12
Single Label Name Queries (counter-rel-names)	Number of requests received for names of only one label (relative names).	13
Requests Refused (counter-req-refusals)	Number of refused queries.	14
Unparseable Requests (counter-req-unparses)	Number of unparseable requests.	15
Requests with Other Errors (counter-other-errors)	Number of aborted requests due to other errors.	16
Performance		
updated-rrs	Number of resource records added and deleted, including updates, despite errors.	
update-packets	Number of update packets processed.	

Table 6-3 DNS Statistics (continued)

Statistic	Description	Digit
ixfrs-out	Number of successful outbound incremental zone transfers (IXFRs).	
ixfrs-in	Number of inbound IXFRs, including those resulting in full zone transfers.	
ixfrs-full-resp	Number of outbound full zone transfers (AXFRs) in response to IXFR requests.	
axfrs-out	Number of successful outbound AXFRs, including those counted in ixfrs-full-resp.	
axfrs-in	Number of successful inbound AXFRs.	
queries	Number of queries responded to, excluding updates.	
xfrs-out-at-limit	Number of times that outbound transfers reached the concurrent limit.	
xfrs-in-at-limit	Number of times that inbound transfers reached the concurrent limit.	
notifies-out	Number of outbound notify packets.	
notifies-in	Number of inbound notify packets.	
Query		
auth-answers	Numbered of authoritatively answered queries.	
auth-no-names	Number of queries for which <code>authoritative no such name answers</code> occurred.	
auth-no-data-responses	Number of queries for which <code>authoritative no such name responses</code> occurred.	
nonauth-answers	Number of queries nonauthoritatively answered (from cache).	
nonauth-no-data-responses	Number of queries nonauthoritatively answered, but with no data.	
referrals	Number of requests referred to other servers.	
relative-name-requests	Number of requests received for names that are only one label long.	
refusals	Number of queries refused.	
lame-delegations	Number of queries resulting in lame delegations (see the “Reporting Lame Delegation” section on page 16-11).	
mem-cache-hits	Number of memory cache lookup hits.	
mem-cache-misses	Number of memory cache lookup misses.	
mem-cache-writes	Number of memory cache writes.	
Security		
rcvd-tsig-packets	Number of TSIG RRs processed (see the “Transaction Security” section on page 27-6).	
detected-tsig-bad-time	Number of incoming packets with bad TSIG time stamps.	
detected-tsig-bad-key	Number of incoming packets with invalid or unknown TSIG keys.	
detected-tsig-bad-sig	Number of incoming packets with bad TSIG signatures.	
rcvd-tsig-bad-time	Number of BADTIME errors after sending a TSIG.	
rcvd-tsig-bad-key	Number of BADKEY errors after sending a TSIG.	

Table 6-3 DNS Statistics (continued)

Statistic	Description	Digit
rcvd-tsig-bad-sig	Number of BADSIG errors after sending a TSIG.	
unauth-xfer-reqs	With zone transfer restrictions enabled, the number of ACL authorization failures.	
unauth-update-reqs	Number of updates resulting in ACL authorization failures, or that target zones that do not support updates.	
Error		
update-errors	Number of updates resulting in errors or failures, including negative responses to prerequisite checks, but excluding TSIG responses.	
ixfr-in-errors	Number of inbound IXFR errors, but excluding packet format errors.	
ixfr-out-errors	Number of outbound IXFR errors, but excluding packet format errors.	
axfr-in-errors	Number of inbound AXFR errors, but excluding packet format errors.	
axfr-out-errors	Number of outbound AXFR errors, but excluding packet format errors.	
sent-total-errors	Number of requests answered with errors (RCODE values other than 0, 3, 6, 7, and 8).	
sent-format-errors	Number of unparsable requests received.	
sent-other-errors	Number of requests aborted due to other local server errors.	
sent-refusal-errors	Number of requests resulting in REFUSED responses.	
rcvd-format-errors	Number of responses received with FORMERR status.	
Max Counters		
concurrent-xfrs-in	Maximum number of concurrent threads processing inbound transfers during the last sampling period.	
concurrent-xfrs-out	Maximum number of concurrent threads processing outbound transfers during the last sampling period.	

DHCP Statistics

The DHCP server statistics appear in [Table 6-4](#). The table is organized by category, name and description of the statistic, and the digit position of the statistic in the output of the generic **dhcp getStats** command, in the format:

```
nrcmd> dhcp getStats
100 Ok
{1} 2 3 4 5 6 7 8
```

Table 6-4 DHCP Statistics

Statistic	Description	Digit
General		
start-time-str	Date and time of last server reload, as a text string.	{1}
total-discovers	Number of DISCOVER packets received.	2
total-requests	Number of REQUEST packets received.	3
total-releases	Number of RELEASED packets received.	4
total-offers	Number of OFFER packets sent.	5
total-acks	Number of acknowledgement (ACK) packets sent.	6
total-naks	Number of negative acknowledgement (NAK) packets sent.	7
total-declines	Number of DECLINE packets received.	8
Server		
acks	Number of DHCPACK packets sent in the time interval.	
acks-per-second	Average rate DHCPACK packets are sent to clients.	
declines	Number of DHCPDECLINE packets received.	
discovers	Number of DHCPDISCOVER packets received.	
naks	Number of DHCPNAK packets sent.	
offers	Number of DHCPPOFFER packets sent.	
packets-dropped	Number of incoming packets dropped.	
releases	Number of DHCPRELEASE packets received.	
request-buffers-in-use	Number of request buffers at the time of statistics calculation.	
requests	Number of DHCPREQUEST packets received.	
response-buffers-in-use	Number of response buffers at the time of statistics calculation.	
timeouts	Number of timeouts (leases, offers) during the time interval.	
Failover		
binding-acks-received	Number of failover DHCPBNDACK packets received during the time interval.	
binding-acks-sent	Number of failover DHCPBNDACK packets sent during the time interval.	
binding-naks-received	Number of failover DHCPBNDNAK packets received during the time interval.	
binding-naks-sent	Number of failover DHCPBNDNAK packets sent during the time interval.	
binding-updates-received	Number of failover DHCPBNDUPD packets received during the time interval.	
binding-updates-sent	Number of failover DHCPBNDUPD packets sent during the time interval.	
packets-dropped	Number of failover packets dropped.	

Table 6-4 DHCP Statistics (continued)

Statistic	Description	Digit
packets-received	Number of failover packets received.	
packets-sent	Number of failover packets sent.	
polls-received	Number of failover DHCPOLL packets received.	
polls-sent	Number of failover DHCPOLL packets sent.	
pool-requests-received	Number of failover DHCPPOOLREQ packets received during the time interval.	
pool-requests-sent	Number of failover DHCPPOOLREQ packets sent during the time interval.	
update-done-received	Number of failover DHCPUPDATEDONE packets received during the time interval.	
update-done-sent	Number of failover DHCPUPDATEDONE packets sent during the time interval.	
update-requests-received	Number of failover DHCPUPDATEREQ packets received during the time interval.	
update-requests-sent	Number of failover DHCPUPDATEREQ packets sent during the time interval.	

TFTP Statistics

The TFTP server statistics appear in [Table 6-5](#). The table is organized by category, name and description of the statistic, and the digit position of the statistic in the output of the generic `tftp getStats` command, in the format:

```
nrcmd> tftp getStats
100 Ok
{1} 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
```

Table 6-5 TFTP Statistics


Attribute	Description	Digit
id	Implementation ID (release and build information).	{1}
server-state	State of the server.	2
server-start-time	Start date and time (in seconds).	3
server-reset-time	Reset date and time.	4
server-time-since-start	Running time since last start.	5
server-time-since-reset	Running time since last reset.	6
total-packets-in-pool	Number of packets in the pool.	7
total-packets-in-use	Number of packets the server is using.	8
total-packets-received	Number of packets received since the last start or reload.	9
total-packets-sent	Number of packets sent since the last start or reload.	10
total-packets-drained	Number of packets read and discarded since the last start or reload.	11

Table 6-5 TFTP Statistics (continued)

Attribute	Description	Digit
total-packets-dropped	Number of packets dropped since the last start or reload.	12
total-packets-malformed	Number of packets received that were malformed since the last start or reload.	13
total-read-requests	Number of packets read since the last start or reload.	14
total-read-requests-completed	Number of read packets completed since the last start or reload.	15
total-read-requests-refused	Number of read packets refused since the last start or reload.	16
total-read-requests-ignored	Number of read packets ignored since the last start or reload.	17
total-read-requests-timed-out	Number of read packets that timed out since the last start or reload.	18
total-write-requests	Number of read packets that were write requests since the last start or reload.	19
total-write-requests-completed	Number of write requests completed since the last start or reload.	20
total-write-requests-refused	Number of write requests refused since the last start or reload.	21
total-write-requests-ignored	Number of write requests ignored since the last start or reload.	22
total-write-requests-timed-out	Number of write requests that timed out since the last start or reload.	23
total-docsis-requests	Number of DOCSIS requests received since the last start or reload.	24
total-docsis-requests-completed	Number of DOCSIS requests completed since the last start or reload.	25
total-docsis-requests-refused	Number of DOCSIS requests refused since the last start or reload.	26
total-docsis-requests-ignored	Number of DOCSIS requests ignored since the last start or reload.	27
total-docsis-requests-timed-out	Number of DOCSIS requests that timed out since the last start or reload.	28
read-requests-per-second	Number of read requests per second.	29
write-requests-per-second	Number of write requests per second.	30
docsis-requests-per-second	Number of DOCSIS requests per second.	31

Displaying IP Address Usage


In the Web UI, you can look at the local or regional cluster's address space, or generate a subnet utilization or lease history report at the regional cluster, to determine IP address usage. These functions are available in both Web UIs by clicking **Address Space**, if you have address space privileges at the local or regional cluster.

You can determine the current address space utilization by clicking the View icon () in the Current Usage column for the unified address space, address block, and subnet (see the “[Viewing Address Utilization for Address Blocks, Subnets, and Scopes](#)” section on page 8-11). You can also get the most

current IP address utilization by querying the lease history (see the “[Querying Leases](#)” section on [page 21-21](#)). In the latter case, the regional CCM server references the appropriate DHCP server directly. To ensure this subnet-to-server mapping, you must update the regional address space view so that it is consistent with the relevant local cluster. Do this by pulling the replica address space, or reclaiming the subnet to push to the DHCP server (see the “[Reclaiming Subnets](#)” section on [page 8-9](#)). Also ensure that the particular DHCP server is running.

In the CLI, you can generate an IP address usage report using the **report** command. See the *Network Registrar CLI Reference* for additional options you can set.

Displaying Related Servers

Network Registrar displays the relationship among servers in a DNS zone distribution or a DHCP failover configuration. In the Web UI, you can view a related servers page when you click the Related Servers icon () on various pages.

DNS Zone Distribution Servers

A DNS zone distribution simplifies creating multiple zones that share the same secondary server attributes. In the Web UI, you can view and set the primary and secondary DNS servers in a zone distribution:

- At the local cluster, click **DNS**, then **Zone Distribution**. This opens the List Zone Distributions page. The local cluster allows only one zone distribution, the Default. Click this zone distribution name to open the Edit Zone Distribution page, which shows the authoritative and secondary servers in the zone distribution.
- At the regional cluster, click **DNS**, then **Zone Distributions**. This opens the List/Add Zone Distributions page (see [Figure 14-8 on page 14-19](#)). The regional cluster allows creating more than one zone distribution. Click the zone distribution name to open the Edit Zone Distribution page, which shows the primary, authoritative, and secondary servers in the zone distribution.

In the CLI, create a zone distribution using **zone-dist name create primary-cluster**, then view it using **zone-dist list**. For example:

```
nrcmd> zone-dist distr-1 create Boston-cluster
nrcmd> zone-dist list
```

DHCP Failover Servers

Related servers in a DHCP failover pair relationship can show the following information:

- Type—Main or backup DHCP server.
- Server name—DNS name of the server.
- IP address—Server’s IP address in dotted octet format.
- Requests—Number of outstanding requests, or two dashes if not applicable.
- Communication status—OK or INTERRUPTED.
- Cluster state—Failover state of this DHCP server.
- Partner state—Failover state of its partner server.

In the Web UI, click **DHCP**, then **Failover**. The List DHCP Failover Pairs page shows the main and backup servers in the failover relationship.

In the CLI, use **dhcp getRelatedServers** to display the connection status between the main and partner DHCP servers. If there are no related servers, the output is simply `100 OK`.

Displaying Leases

After you create a scope, you can monitor lease activity and view lease attributes.

In the Web UI:

- At the local cluster, click **DHCP**, then **Scopes**. Click a scope name on the List/Add DHCP Scopes page to open the Edit DHCP Scope page. Halfway down the page, click **List Leases** to open the List DHCP Lease for Scope page.
- At the regional cluster, you can view the lease history. Click **Address Space**, then **Lease History**. Set the query parameters, then click **Query Lease History**. (See the “[Querying Leases](#)” section on page 21-21.)

In the CLI, use **lease list** to view the properties of all the available leases.

Troubleshooting Servers

The following sections describe troubleshooting the DNS, DHCP, and TFTP server.

Immediate Troubleshooting Actions

When facing a problem, it is crucial not to cause further harm while isolating and fixing the initial problem. Here are things to do (or avoid doing) in particular:

- Have 512 MB or more of memory and 2.5 GB or more of a data partition.
- Do not reboot a cable modem termination system (CMTS).
- Enable DHCP failover.
- Do not reload, restart, or disrupt Network Registrar with failover resynchronization in progress.

Troubleshooting Server Failures

The server agent processes (`nwreglocal` and `nwregregion`) normally detect server failures and restart the server. You can usually recover from the failure and the server is not likely to fail again immediately after restarting. On rare occasions, the source of the server failure prevents the server from successfully restarting, and the server fails again as soon as it restarts. In such instances, perform the following steps:

Step 1 If the server takes a significantly long time to restart, stop and restart the server agent. On:

- Windows:

```
net stop nwreglocal or nwregregion
net start nwreglocal or nwregregion
```

- Solaris:

```
/etc/init.d/nwreglocal stop or nwregregion stop
/etc/init.d/nwreglocal stop or nwregregion start
```

- Linux:

```
/etc/rc.d/init.d/nwreglocal stop or nwregregion stop
/etc/rc.d/init.d/nwreglocal stop or nwregregion start
```

- Step 2** Keep a copy of all the log files. Log files are located in the *install-path*/logs directory on Solaris and Linux, and the *install-path*\logs folder on Windows. The log files often contain useful information that can help isolate the cause of a server failure.
- Step 3** Use the TAC tool, as described in the “Using the TAC Tool” section on page 6-20, or save the core or user.dmp file, if one exists, depending on the operating system:
- On Windows—The user.dmp file is located in the system directory, which varies depending on the Windows system. Search for this file and save a renamed copy.
 - On Solaris and Linux—The core file is located in the *install-path*. Save a renamed copy of this file that Network Registrar does not overwrite.
- Step 4** On Windows, use the native event logging application to save the System and Application event logs to files. You can do this from the Event Viewer. These event logs often contain data that helps debug Network Registrar server problems. For a description of the log messages for each server module, see the *install-path*/docs/msgid/MessageIdIndex.html file.
-

Troubleshooting and Optimizing the TFTP Server

You can set certain attributes to troubleshoot and optimize TFTP server performance.

Tracing TFTP Server Activity

The TFTP server has two CLI commands that help create more output to logs and can be useful in troubleshooting, although this usually impacts performance. These commands set up server packet tracing. The **tftp getTraceLevel** command identifies the current trace level, which by default is 0, or no tracing. The **tftp setTraceLevel** command sets the packet tracing to a value between 0 and 4. The trace files are located in the /logs subdirectory of the installation directory. Windows tracing goes to the file_tftp_1_log file; Solaris and Linux tracing goes to the /var/nwreg2/{local | regional}/logs/file_tftp_1_log and file_tftp_1_trace files.

Here are the trace levels, with each higher level being cumulative:

- 0—Disables all server tracing (the default).
- 1—Displays all the log messages in the trace file.
- 2—Displays the client’s IP address and port number for all packets.
- 3—Displays the packet header information.
- 4—Displays the first 32 bytes of the packet.



Note

Setting and getting the trace level only works if the TFTP server is started. Turn on packet tracing only for debugging purposes, and then not for any extended time, for performance reasons.

Optimizing TFTP Message Logging

You can improve TFTP server performance by restricting logging and tracing. By default, the server logs error, warning, and informational messages to `file_tftp_1_log` files. You can set the log levels using a few TFTP server parameters:

- Log level (use the `log-level` attribute)—Master controller of server logging, which defaults to, and is best left at, level 3 (logs all error, warning, and informational messages). As with packet tracing, the higher logging levels are cumulative. If set to 0, no server logging occurs.
- Log settings (use the `log-settings` attribute)—This is the second level of logging control and takes only two values, `default` or `no-success-messages`. The `default` log setting does not alter the default of log level 3 (error, warning, and informational messages). However, you may want to disable writing success informational messages, and thereby improve server performance, by changing the log settings to `no-success-messages`.
- Log file count and size (use the `log-file-count` attribute)—Sets how many log files to maintain and how large to allow them to get in the `/logs` directory. The default is to maintain a maximum of four files of one megabyte each.

**Note**

Reload the TFTP server after changing these values.

Enabling TFTP File Caching

You can improve TFTP server performance significantly by enabling file caching on the server. You must do this explicitly, because it is disabled by default. You must also create and point to a file cache directory, and you can set the maximum size of this directory. Here are the steps:

-
- Step 1** Determine where you want the TFTP cache files to go. This becomes a subdirectory of the TFTP home directory, which by default is `install-path/data/tftp` (on Solaris and Linux, it is `/var/nwreg2/{local | regional}/data/tftp`). If you want a different location, set the `home-directory` attribute.
 - Step 2** Change to the TFTP home directory and create the cache directory, such as `CacheDir`, in the home directory, using the `mkdir CACHEDIR` command. Note that Network Registrar ignores any files in any subdirectories of this cache directory.
 - Step 3** Use the `file-cache-directory` attribute to set up the TFTP server to point to the cache directory. You cannot use relative paths in the directory name, such as `../cachedir`. If the directory does not exist, file caching cannot occur.
 - Step 4** Use the `file-cache-max-memory-size` attribute to set the maximum memory size, in bytes, of the cache. The default is 32 KB. Network Registrar loads all files into cache that cumulatively fit this memory size. If you set the value to 0, Network Registrar does not cache any data, even if you enable file caching.
 - Step 5** Copy all of the files you want cached into the cache directory, and not into any subdirectory. Because all files in this directory are loaded into cache, do not include large files.
 - Step 6** Enable the `file-cache` attribute to enable file caching, then reload the server. Network Registrar logs the name of each cached file, and skips any it cannot load. It reads in all files as binary data and translates them as the TFTP client requests. For example, if a client requests a file as NetASCII, the client receives the cached data in that form.
 - Step 7** Writing to cache is not allowed. If you need to update a cache file, overwrite it in the cache directory, then reload the server.
-

Solaris and Linux Troubleshooting Tools

You can also use the following commands on Solaris and Linux systems to troubleshoot Network Registrar. To:

- See all Network Registrar processes:


```
ps -leaf | grep nwr
```
- Monitor system usage and performance:


```
top
vmstat
```
- View login or bootup errors:
 - On Solaris—`grep /var/adm/messages*`
 - On Linux—`grep /var/log/messages*`
- View the configured interfaces and other network data:


```
ifconfig -a
```

Using the TAC Tool

There may be times when any amount of troubleshooting steps will not resolve your problem and you have to resort to contacting the Cisco Technical Assistance Center (TAC) for help. Network Registrar provides a tool so that you can easily assemble the server or system error information, and package this data for TAC support engineers. This eliminates having to manually assemble this information with TAC assistance. The resulting package from this tool provides the engineers enough data so that they can more quickly and easily diagnose the problem and provide a solution.

The `cnr_tactool` utility is available in the `bin` directory of the Windows, and `usrbin` directory of the UNIX or Linux, installation directories. Execute the `cnr_tactool` utility:

```
> cnr_tactool -N username -P password [-d output-directory]
```

The output directory is optional and normally is the `temp` directory of the installation directories (in the `/var` path on Solaris and Linux). If you do not supply the username and password on the command line, you are prompted for them:

```
> cnr_tactool
username:
password:
[processing messages....]
```

The tool generates a packaged tar file whose name includes the date and version. The tar file contains all the diagnostic files.