Managing Caching DNS Server

In Cisco Prime Network Registrar, the authoritative and caching services are separated, and are handled by two separate servers. This chapter explains how to set the Caching DNS server parameters. Before you proceed with the tasks in this chapter, see Introduction to the Domain Name System, which explains the basics of DNS.

Setting DNS Caching Server Properties

You can set properties for the Caching DNS server. These include:

- **General server properties**—See Setting General Caching DNS Server Properties, on page 2
- **Log settings**—See Specifying Log Settings, on page 2
- **Packet logging**—See Enabling Packet Logging, on page 3
- **Activity summary settings**—See Specifying Activity Summary Settings, on page 4
- **Top names settings**—See Specifying Top Names Settings, on page 18
- **Security events settings**—See Logging Security Events, on page 19
- **TLS settings**—See Specifying TLS Settings, on page 23
- **HTTPS settings**—See Specifying HTTPS Settings, on page 26
- **Caching settings**—See Setting Prefetch Timing, on page 28
- **Cache TTLs**—See Setting Cache TTLs, on page 28
- **Smart caching**—See Smart Cache settings, on page 29
- **Root name servers**—See Defining Root Nameservers, on page 31
- **UDP ports**—See Dynamic Allocation of UDP Ports, on page 31
- **Maximum memory cache sizes**—See Setting Maximum Memory Cache Sizes, on page 31

- **Resolver settings**—See Specifying Resolver Settings, on page 32
- **Network settings**—See Specifying Network Settings, on page 34
- **Client subnet**—See Enabling Client Subnet, on page 34
- **Advanced settings**—See Specifying Advanced Settings, on page 36
- **Flush cache**—See Flushing Caching DNS Cache, on page 36
- **Prevent DNS cache poisoning**—See Detecting and Preventing DNS Cache Poisoning, on page 37
- **Handle unresponsive nameservers**—See Handling Unresponsive Nameservers, on page 38

Setting General Caching DNS Server Properties

You can view general Caching DNS server properties, such as log settings, basic cache settings, SNMP traps, and root nameservers.

The following subsections describe some of the most common property settings. They are listed in Setting DNS Caching Server Properties, on page 1.

Local Web UI

Step 1 To access the server properties, from the **Deploy** menu, choose **CDNS Server** under the **DNS** submenu to open the Manage DNS Caching Server page.

Step 2 The local CDNS Server page is automatically selected when you choose the **CDNS Server** tab, either from the Deploy menu or by clicking the **CDNS Server** tab in the left pane. The page displays all the Caching DNS server attributes.

Step 3 Click **Save** to save the Caching DNS server attribute modifications.

CLI Commands

Use **cdns show** to display the Caching DNS server properties (see the **cdns** command in the CLIGuide.html file in the /docs directory for syntax and attribute descriptions).

Specifying Log Settings

The *log-settings* attribute determines which detailed events the Caching DNS server logs. Logging these additional details can help analyze a problem. However, leaving detailed logging enabled for a long period, can fill the log files and cause the loss of important information.

The possible options are:

- **activity-summary**—Causes logging of a server statistics summary at a regular interval.
- **config**—Controls logging pertaining to server configuration and server de-initialization.
- **query**—Causes logging of all DNS queries to the server.
- **scp**—Controls logging pertaining to SCP message processing.
- **server-detailed-ops**—Controls detailed logging of server operations.
- **server-ops**—Controls high level logging of server operations.

- **name-servers**—Enables logging when name servers for exceptions and forwarders become unresponsive or again become responsive.

The *immediate-response-stats* attribute (available in Advanced mode) enables collecting response times statistics when queries are answered immediately. If this feature is disabled, the related statistics *(immediate-response-count*, *immediate-response-average*, and *immediate-response-median*) will show zero.

Enabling Packet Logging

Cisco Prime Network Registrar supports packet logging for Caching DNS server to help analyze and debug the Caching DNS server activity. The packet logging settings determine the type of packet logging (summary or detail), the type of packets logged, and to which log file the messages are logged. By default, the Caching DNS server does not log any packet log messages.

Use the following server level attributes to enable packet logging for the Caching DNS server:

Table 1: Caching DNS Server Packet Logging Attributes

Attribute	Description
Packet Logging (*packet-logging*)	Determines the type of packet logging that is logged to the CDNS logs. The type of packets logged can be controlled with the *packet-log-settings* attribute. • **disabled**—This settings disables packet logging. • **summary**—This setting enables one line summary packet logging. • **detail**—This setting enables detailed packet tracing. **Note** This setting may significantly increase the amount of information that is logged and should only be used on a temporary basis for debugging purposes. Note that while packet logging can be helpful for debugging and troubleshooting, it does have an impact on DNS server performance. Therefore, Cisco does not recommend leaving packet logging enabled in production environments.
Packet Logging File (*packet-logging-file*)	Determines the destination log of packet log messages when packet logging is enabled. • **cdns**—Packet logging messages are logged to the standard CDNS log file (cdns_log*). • **packet**—Packet logging messages are logged to a separate CDNS packet log file (cdns_query_log*).

Attribute	Description
Packet Log Settings (*packet-log-settings*)	Determines the type of packets to log when packet logging is enabled. Packet logging can be enabled by configuring the *packet-logging* attribute. • **query-in**—This setting enables logging of incoming query packets. These are packets coming in from DNS clients. • **query-out**—This setting enables logging of outgoing query packets. These are queries going to upstream DNS servers. • **response-in**—This setting enables logging of incoming query response packets. These are responses coming from upstream DNS servers. • **response-out**—This setting enables logging of outgoing query response packets. These are responses going to DNS clients.

Local Advanced Web UI

Step 1 On the Manage DNS Caching Server page, under the **Packet Logging** section, select the value for **packet-logging** from the drop-down list. The value can be **summary** or **detail**.

Step 2 For the *packet-log-settings* attribute, check the desired check boxes.

Step 3 Click **Save** to save the changes.

CLI Commands

Use **cdns set packet-logging=summary** to enable one line summary packet logging.

Use **cdns set packet-logging=detail** to enable detailed packet tracing.

Use **cdns set packet-log-settings**=*value* to set the type of packets to log when packet logging is enabled.

Note Reloading of Caching DNS server is not required for the *packet-logging* and *packet-log-settings* attributes to take effect immediately (similar to log settings). However, the *packet-logging-file* attribute requires a Caching DNS server reload.

Specifying Activity Summary Settings

Note To specify the activity summary settings, you have to check *activity-summary* under Log Settings.

You can specify the interval at which to log activity summary information using the Statistics Interval (*activity-summary-interval*) attribute. It has a default value of 60 seconds.

The Caching DNS server logs sample and/or total statistics based on the option you check for the Statistics Type (*activity-summary-type*) attribute. The default value is "sample".

The option checked for the Statistics Settings (*activity-summary-settings*) attribute determines the category of statistics that is logged as part of activity summary. The possible settings are:

- **cache**—Logs statistics on the RR cache.

  For the list of activity summary statistics that are displayed in the logs for the **cache** setting, see Cache Statistics, on page 6.

- **firewall**— Logs statistics on DNS firewall usage.

  For the list of activity summary statistics that are displayed in the logs for the **firewall** setting, see Firewall Statistics, on page 7.

- **memory**—Logs statistics on memory usage.

  For the list of activity summary statistics that are displayed in the logs for the **memory** setting, see Memory Statistics, on page 9.

- **query**—Logs statistics related to incoming queries.

  For the list of activity summary statistics that are displayed in the logs for the **query** setting, see Query Statistics, on page 9.

- **query-type**—Logs statistics on the RR types that are being queried.

  For the list of activity summary statistics that are displayed in the logs for the **query-type** setting, see Query by Type Statistics, on page 11.

- **rate-limiting**—Logs the number of rate limiting events.

  For the list of activity summary statistics that are displayed in the logs for the **rate-limiting** setting, see Rate Limiting Statistics, on page 12.

- **resol-queue**—Logs statistics on the resolution queue.

  For the list of activity summary statistics that are displayed in the logs for the **resol-queue** setting, see Resolution Queue Statistics, on page 13.

- **responses**—Logs statistics about query responses.

  For the list of activity summary statistics that are displayed in the logs for the **responses** setting, see Responses Statistics, on page 14.

- **security**—Logs statistics related to security events.

  For the list of activity summary statistics that are displayed in the logs for the **security** setting, see Security Statistics, on page 15.

- **system**—Logs statistics on system usage.

  For the list of activity summary statistics that are displayed in the logs for the **system** setting, see System Statistics, on page 16.

- **top-names**—Logs the top names queried and hit count.

  For the list of activity summary statistics that are displayed in the logs for the **top-names** setting, see Top Names Statistics, on page 17.

- **upstream**—Logs the number of upstream queries.

For the list of activity summary statistics that are displayed in the logs for the **upstream** setting, see Upstream Statistics, on page 17.

Activity Summary Statistics

Following sections describe the list of activity summary statistics that are displayed in the logs under each of the *activity-summary-settings* category.

Cache Statistics

The **cache** activity-summary-settings logs statistics on the RR cache.

Sample log message:

```
10/19/2023 10:36:08 cdns tid: 0 Activity Stats 0 22173 [Cache] Sample since Thu Oct 19
10:35:08 2023: hits=number, misses=number, prefetches=number, message-overflow=number,
rrset-overflow=number, remote-ns-overflow=number, key-overflow=number, smart-cache=number
```

Table 2: Cache Statistics

Activity Summary Name	Statistic[1]	Description
hits	cache-hits	Total number of queries that were answered from cache.
misses	cache-misses	Total number of queries that were not found in the cache.
prefetches	cache-prefetches	Number of prefetches performed.
rrset-overflow	mem-cache-exceeded	Number of times the RRSet cache has gone over the configured limit. This indicates that the configured limit may be undersized for its environment.
message-overflow	mem-query-cache-exceeded	Number of times the message cache has gone over the configured limit. This indicates that the configured limit may be undersized for its environment.
remote-ns-overflow	remote-ns-cache-exceeded	Number of times the remote name server cache has gone over the configured limit. This indicates that the configured limit may be undersized for its environment.
key-overflow	key-cache-exceeded	Number of times the key cache has gone over the configured limit. This indicates that the configured limit may be undersized for its environment.
smart-cache	smart-cache	Total number of times the CDNS Server employed a smart-cache response, when *smart-cache* is enabled.

[1] The statistics listed in this column are the server statistics displayed in the web UI and CLI. The REST API calls will have the statistic name camel-cased without dashes (that is, queries-total is queriesTotal

in the REST API). Note that the activity summary and statistics are keyed off the same server data, but the activity-summary names are shortened to conserve space in the log message. For the complete list of Caching DNS server statistics, see the *"CDNS Statistics" section of the "Server Statistics" appendix in Cisco Prime Network Registrar 11.2 Administration Guide*.

Firewall Statistics

The **firewall** activity-summary-settings logs statistics on DNS Firewall usage.

Sample log message:

```
10/19/2023 10:36:08 cdns tid: 0 Activity Stats 0 22322 [Firewall] Sample since Thu Oct 19
10:35:08 2023: redirected=number, dropped=number, refused=number, redirect-nxdomain=number,
 rpz=number
```

Table 3: Firewall Statistics

Activity Summary Name	Statistic[2]	Description
dropped	firewall-dropped	Number of times DNS Firewall dropped a query.
redirected	firewall-redirected	Number of times DNS Firewall redirected a query.
refused	firewall-refused	Number of times DNS Firewall refused a query.
redirect-nxdomain	firewall-redirect-nxdomain	Number of times DNS Firewall redirected a query with an NXDOMAIN answer.
rpz	firewall-rpz	Number of times DNS Firewall RPZ rules matched an incoming query.

[2] The statistics listed in this column are the server statistics displayed in the web UI and CLI. The REST API calls will have the statistic name camel-cased without dashes (that is, queries-total is queriesTotal in the REST API). Note that the activity summary and statistics are keyed off the same server data, but the activity-summary names are shortened to conserve space in the log message. For the complete list of Caching DNS server statistics, see the *"CDNS Statistics" section of the "Server Statistics" appendix in Cisco Prime Network Registrar 11.2 Administration Guide*.

When you create firewall object with RPZ action, the below shown are the additional statistics for the firewall rpz:

```
10/19/2023 10:36:08 cdns tid: 0 Activity Stats 0 22481 [Firewall RPZ] Sample since Thu Oct
 19 10:35:08 2023: rpz-nxdomain=number, rpz-nodata=number, rpz-passthru=number,
rpz-drop=number, rpz-tcp=number, rpz-local=number, rpz-cname=number, rpz-disabled=number,
rpz-no-override=number, rpz-invalid=number
```

```
10/19/2023 10:36:08 cdns tid: 0 Activity Stats 0 22483 [Firewall RPZ-2] Sample since Thu
Oct 19 10:35:08 2023: rpz-notifys=number, rpz-notifys-invalid=number, rpz-axfrs=number,
rpz-ixfrs=number, rpz-rrs-added=number, rpz-rrs-removed=number, rpz-rrset-count=number
```

Table 4: Firewall Statistics with RPZ enabled

Activity Summary Name	Statistic[3]	Description
rpz-nxdomain	rpz-nxdomain	Number of queries where rpz required an nxdomain response.

Activity Summary Name	Statistic[3]	Description
rpz-nodata	rpz-nodata	Number of queries were rpz required a nodata response.
rpz-passthru	rpz-passthru	Number of queries where rpz required a passthru.
rpz-drop	rpz-drop	Number of queries where rpz required a drop action.
rpz-tcp	rpz-tcp	Number of queries where rpz required a tcp query.
rpz-local	rpz-local	Number of queries were rpz required a local response.
rpz-cname	rpz-cname	Number of queries where rpz required a cname response.
rpz-disabled	rpz-disabled	Number of queries where rpz did not override.
rpz-no-override	rpz-no-override	Number of queries where rpz did not require override.
rpz-invalid	rpz-invalid	Number of queries where rpz was invalid.
rpz-notifys	rpz-notifys	Number of valid notifys received.
rpz-notifys-invalid	rpz-notifys-invalid	Number of invalid notifys received.
rpz-axfrs	rpz-axfrs	Number of full zone transfers performed.
rpz-ixfrs	rpz-ixfrs	Number of incremental zone transfers performed.
rpz-rrs-added	rpz-rrs-added	Number of resource records added.
rpz-rrs-removed	rpz-rrs-removed	Number of resource records removed.
rpz-rrset-count	rpz-rrset-count	Total number of rpz resource records.

[3] The statistics listed in this column are the server statistics displayed in the web UI and CLI. The REST API calls will have the statistic name camel-cased without dashes (that is, queries-total is queriesTotal in the REST API). Note that the activity summary and statistics are keyed off the same server data, but the activity-summary names are shortened to conserve space in the log message. For the complete list of Caching DNS server statistics, see the *"CDNS Statistics" section of the "Server Statistics" appendix in Cisco Prime Network Registrar 11.2 Administration Guide*.

Memory Statistics

The **memory** activity-summary-settings logs statistics on memory usage.

Sample log message:

```
10/19/2023 10:36:08 cdns tid: 0 Activity Stats 0 22303 [Memory] Current:
mem-cache-process=number, mem-cache-rrset=number, mem-cache-message=number,
mem-mod-iterator=number, mem-mod-validator=number
```

Table 5: Memory Statistics

Activity Summary Name	Statistic[4]	Description
mem-cache-process	mem-process	An estimate of the memory in bytes of the CDNS process.
mem-cache-rrset	mem-cache	Memory in bytes allocated to the RRset cache. Note that the allocated memory will be maintained across server reloads, unless the *rrset-cache-size* configuration has changed.
mem-cache-message	mem-query-cache	Memory in bytes allocated to the message cache. Note that the allocated memory will be maintained across server reloads, unless the *msg-cache-size* configuration has changed.
mem-mod-iterator	mem-iterator	Memory in bytes used by the CDNS iterator module.
mem-mod-validator	mem-validator	Memory in bytes used by the CDNS validator module.

[4] The statistics listed in this column are the server statistics displayed in the web UI and CLI. The REST API calls will have the statistic name camel-cased without dashes (that is, queries-total is queriesTotal in the REST API). Note that the activity summary and statistics are keyed off the same server data, but the activity-summary names are shortened to conserve space in the log message. For the complete list of Caching DNS server statistics, see the *"CDNS Statistics" section of the "Server Statistics" appendix in Cisco Prime Network Registrar 11.2 Administration Guide*.

Query Statistics

The **query** activity-summary-settings logs statistics related to incoming queries.

Sample log message:

```
10/19/2023 10:36:08 cdns tid: 0 Activity Stats 0 22171 [Query] Sample since Thu Oct 19
10:35:08 2023: total=number, queries-per-second=number, acl-failures=number, udp=number,
tcp=number, ipv4=number, ipv6=number, tls=number, tls-errors-in=number, tls-errors-out=number,
 https=number, https-errors-in=number, edns=number, dnssec=number, dns64-aaaa=number,
dns64-ptr=number, dns64-ns=number, unwanted-class=number, https-query-buffer=number,
https-response-buffer=number
```

Table 6: Query Statistics

Activity Summary Name	Statistic[5]	Description
total	queries-total	Total number of queries received by the CDNS Server.

Activity Summary Name	Statistic[5]	Description
queries-per-second	queries-per-second	Number of queries received per second.
acl-failures	queries-failing-acl	Number of queries being dropped or refused due to ACL failures.
tcp	queries-over-tcp	Total number of queries received over TCP by the CDNS Server. This statistic is also incremented when queries are received over HTTPS.
udp	N/A	Total number of queries received over UDP by the CDNS Server.
ipv4	N/A	Total number of IPv4 queries received by the CDNS Server.
ipv6	queries-over-ipv6	Total number of IPv6 queries received by the CDNS Server.
tls	queries-over-tls	Total number of queries received over TLS by the CDNS Server. This statistic is also incremented when queries are received over HTTPS.
tls-errors-in	tls-errors-in	Total number of TLS related errors on inbound DNS query attempts.
tls-errors-out	tls-errors-out	Total number of TLS related errors on outbound DNS query attempts.
https	queries-over-https	Total number of queries received over HTTPS by the CDNS Server.
https-errors-in	queries-over-https- failed	Total number of queries failed with HTTPS errors.
edns	queries-with-edns	Number of queries with EDNS OPT RR present.
dnssec	queries-with-edns-do	Number of queries with EDNS OPT RR with DO (DNSSEC OK) bit set.
dns64-aaaa	dns64-a2aaaa-conversions	Number of times dns64 has converted a type A RR to a type AAAA RR.
dns64-ptr	dns64-ptr-conversions	Number of times dns64 has converted an IPv4 PTR RR to an IPv6 PTR RR.
dns64-ns	N/A	Number of times dns64 converted a type A RR to a type AAAA RR for a name server.
unwanted-class	queries-unwanted-class	Total number of queries with unwanted classes.
https-query-buffer	https-query-buffer	Number of HTTPS queries in memory buffer.
https-response-buffer	https-response-buffer	Number of HTTPS responses in memory buffer.

[5] The statistics listed in this column are the server statistics displayed in the web UI and CLI. The REST API calls will have the statistic name camel-cased without dashes (that is, queries-total is queriesTotal in the REST API). Note that the activity summary and statistics are keyed off the same server data, but the activity-summary names are shortened to conserve space in the log message. For the complete list of Caching DNS server statistics, see the *"CDNS Statistics" section of the "Server Statistics" appendix in Cisco Prime Network Registrar 11.2 Administration Guide*.

Query by Type Statistics

The **query-type** activity-summary-settings logs statistics on the RR types that are being queried.

Sample log message:

```
10/19/2023 10:36:08 cdns tid: 0 Activity Stats 0 22172 [Query-by-Type] Sample since Thu Oct
 19 10:35:08 2023: A=number, AAAA=number, ANY=number, CNAME=number, PTR=number, MX=number,
 NS=number, SOA=number, DS=number, DNSKEY=number, RRSIG=number, NSEC=number, NSEC3=number,
 HTTPS=number, SVCB=number, TXT=number, SRV=number, NAPTR=number, Other=number
```

Table 7: Query by Type Statistics

Activity Summary Name	Statistic[6]	Description
A	queries-type-A	Number of A queries received.
AAAA	queries-type-AAAA	Number of AAAA queries received.
ANY	queries-type-ANY	Number of ANY queries received.
CNAME	queries-type-CNAME	Number of CNAME queries received.
PTR	queries-type-PTR	Number of PTR queries received.
NS	queries-type-NS	Number of NS queries received.
SOA	queries-type-SOA	Number of SOA queries received.
MX	queries-type-MX	Number of MX queries received.
DS	queries-type-DS	Number of DS queries received.
DNSKEY	queries-type-DNSKEY	Number of DNSKEY queries received.
RRSIG	queries-type-RRSIG	Number of RRSIG queries received.
NSEC	queries-type-NSEC	Number of NSEC queries received.
NSEC3	queries-type-NSEC3	Number of NSEC3 queries received.
HTTPS	queries-type-HTTPS	Number of HTTPS (TYPE 65) queries received.
SVCB	queries-type-SVCB	Number of SVCB (TYPE 64) queries received.
NAPTR	queries-type-NAPTR	Number of NAPTR RR queries received.
SRV	queries-type-SRV	Number of SRV RR queries received.

Activity Summary Name	Statistic[6]	Description
TXT	queries-type-TXT	Number of TXT RR queries received.
Other	queries-type-other	All other queries received.

[6] The statistics listed in this column are the server statistics displayed in the web UI and CLI. The REST API calls will have the statistic name camel-cased without dashes (that is, queries-total is queriesTotal in the REST API). Note that the activity summary and statistics are keyed off the same server data, but the activity-summary names are shortened to conserve space in the log message. For the complete list of Caching DNS server statistics, see the *"CDNS Statistics" section of the "Server Statistics" appendix in Cisco Prime Network Registrar 11.2 Administration Guide*.

Rate Limiting Statistics

The **rate-limiting** activity-summary-settings logs the number of rate limiting events.

Sample log message:

```
10/19/2023 10:36:08 cdns tid: 0 Activity Stats 0 22388 [Ratelimit] Sample since Thu Oct 19
 10:35:08 2023: client-ratelimited=number, domain-ratelimited=number

10/19/2023 10:36:08 cdns tid: 0 Activity Stats 0 22390 [Ratelimit-Client] from 10:35:04 to
 10:36:04; interval=number, num-ratelimited=number, total-counted=number, not-counted=number

10/19/2023 10:36:08 cdns tid: 0 Activity Stats 0 22390 [Ratelimit-Domain] from 10:35:04 to
 10:36:04; interval=number, num-ratelimited=number, total-counted=number, not-counted=number
```

Table 8: Rate Limiting Statistics

Activity Summary Name	Logging Sub Category	Statistic[7]	Description
client-ratelimited	Ratelimit	client-rate-limit	Number of times a client was rate limited.
domain-ratelimited	Ratelimit	domain-rate-limit	Number of times a domain was rate limited.
interval	Ratelimit-Domain	N/A	Length of data collection period.
num-ratelimited	Ratelimit-Domain	N/A	Total number of domains that were rate limited.
total-counted	Ratelimit-Domain	N/A	Total number of times a domain was rate limited.
not-counted	Ratelimit-Domain	N/A	Number of times the domain rate limiting table overflowed.
interval	Ratelimit-Client	N/A	Length of data collection period.
num-ratelimited	Ratelimit-Client	N/A	Total number of clients that were rate limited.

Activity Summary Name	Logging Sub Category	Statistic[7]	Description
total-counted	Ratelimit-Client	N/A	Total number of times a client was rate limited.
not-counted	Ratelimit-Client	N/A	Number of times the client rate limiting table overflowed.

[7] The statistics listed in this column are the server statistics displayed in the web UI and CLI. The REST API calls will have the statistic name camel-cased without dashes (that is, queries-total is queriesTotal in the REST API). Note that the activity summary and statistics are keyed off the same server data, but the activity-summary names are shortened to conserve space in the log message. For the complete list of Caching DNS server statistics, see the *"CDNS Statistics" section of the "Server Statistics" appendix in Cisco Prime Network Registrar 11.2 Administration Guide*.

Resolution Queue Statistics

The **resol-queue** activity-summary-settings logs statistics on the resolution queue.

Sample log message:

```
10/19/2023 10:36:08 cdns tid: 0 Activity Stats 0 22174 [Resolution-Queue] Sample since Thu
 Oct 19 10:35:08 2023: num-entries=number, user-queries=number, system-queries=number,
average-num-entries=number, max-num-entries=number, entries-overwritten=number,
exceeded-limit=number, replies-sent=number, exceeded-max-target-count=number
```

Table 9: Resolution Queue Statistics

Activity Summary Name	Statistic[8]	Description
num-entries	requestlist-total	Total number of queued requests waiting for recursive replies.
user-queries	requestlist-total-user	Total number of queued user requests waiting for recursive replies.
system-queries	requestlist-total-system	Total number of queued system requests waiting for recursive replies.
average-num-entries	requestlist-total-average	Average number of requests on the request list.
max-num-entries	requestlist-total-max	Maximum number of requests on the request list.
entries-overwritten	requestlist-total-overwritten	Number of requests on the request list that were overwritten by newer entries.
exceeded-limit	requestlist-total-exceeded	Number of requests dropped because the request list was full.
replies-sent	recursive-replies-total	Total number of query replies that were not found in the cache and required external resolution.
exceeded-max-target-count	exceeded-max-target-count	Number of queries that exceeded the maximum number of name servers glue lookups allowed.

[8] The statistics listed in this column are the server statistics displayed in the web UI and CLI. The REST API calls will have the statistic name camel-cased without dashes (that is, queries-total is queriesTotal in the REST API). Note that the activity summary and statistics are keyed off the same server data, but the activity-summary names are shortened to conserve space in the log message. For the complete list of Caching DNS server statistics, see the *"CDNS Statistics" section of the "Server Statistics" appendix in Cisco Prime Network Registrar 11.2 Administration Guide*.

Responses Statistics

The **responses** activity-summary-settings logs statistics about query responses.

Sample log message:

```
10/19/2023 10:36:08 cdns tid: 0 Activity Stats 0 22175 [Responses] Sample since Thu Oct 19
 10:35:08 2023: total=number, no-error=number, no-data=number, formerr=number,
servfail=number, nxdomain=number, notimp=number, refused=number, notauth=number,
other-errors=number, secure=number, unsecure=number, rrset-unsecure=number, unwanted=number

10/19/2023 10:36:08 cdns tid: 0 Activity Stats 0 22318 [Response-Times] Sample since Thu
Oct 19 10:35:08 2023: current-median=number, average=number

10/19/2023 10:36:08 cdns tid: 0 Activity Stats 0 22423 [Response-Immediate] Sample since
Thu Oct 19 10:35:08 2023: immediate-median=number, immediate-average=number
```

Table 10: Responses Statistics

Activity Summary Name	Statistic[9]	Description
total	answers-total	Number of responses sent to clients.
no-error	answers-with-NOERROR	Number of answers from cache or recursion that result in rcode of NOERROR being returned to client.
nxdomain	answers-with- NXDOMAIN	Number of answers from cache or recursion that result in rcode of NXDOMAIN being returned to client.
no-data	answers-with-NODATA	Number of answers that result in pseudo rcode of NODATA being returned to client.
other-errors	answers-with-other-errors	Number of answers that result in pseudo rcode of NODATA being returned to client.
secure	answers-secure	Number of answers that correctly validated.
unsecure	answers-unsecure	Number of answers that did not correctly validate.
rrset-unsecure	answers-rrset-unsecure	Number of RRSets marked as bogus by the validator.
unwanted	answers-unwanted	Number of replies that were unwanted or unsolicited. High values could indicate spoofing threat.

Activity Summary Name	Statistic[9]	Description
refused	answers-with-REFUSED	Number of answers from cache or recursion that result in rcode of REFUSED being returned to client.
servfail	answers-with-SERVFAIL	Number of answers from cache or recursion that result in rcode of SERVFAIL being returned to client.
formerr	answers-with-FORMERR	Number of answers from cache or recursion that result in rcode of FORMERR being returned to client.
notauth	answers-with-NOTAUTH	Number of answers from cache or recursion that result in rcode of NOTAUTH being returned to client.
notimp	answers-with-NOTIMP	Number of answers from cache or recursion that result in rcode of NOTIMP being returned to client.
current-median	recursive-time-median	The median time, in milliseconds, to complete a recursive query when not found in the cache.
average	recursive-time-average	The average time, in milliseconds, to complete a recursive query when not found in the cache.
immediate-median	immediate-response-median	The median time, in microseconds, to respond to a query when no recursion is needed.
immediate-average	immediate-response-average	The average time, in microseconds, to respond to a query when no recursion is needed.

[9] The statistics listed in this column are the server statistics displayed in the web UI and CLI. The REST API calls will have the statistic name camel-cased without dashes (that is, queries-total is queriesTotal in the REST API). Note that the activity summary and statistics are keyed off the same server data, but the activity-summary names are shortened to conserve space in the log message. For the complete list of Caching DNS server statistics, see the *"CDNS Statistics" section of the "Server Statistics" appendix in Cisco Prime Network Registrar 11.2 Administration Guide*.

Security Statistics

The **security** activity-summary-settings logs statistics related to security events.

The security activity summary statistics are logged under the **Security-Events-Categories** sub category.

Sample log message:

```
10/19/2023 10:36:08 cdns tid: 0 Activity Stats 0 22439 [Security-Events-Categories] Sample
 since Thu Oct 19 10:35:08 2023: total=number, requests=number, alarm=number,
amplification=number, dos=number, firewall=number, malware=number, phishing=number,
poisoning=number, snooping=number, tunneling=number
```

Table 11: Security Statistics

Activity Summary Name	Statistic[10]	Description
total	security-events	Total number of security events detected and captured within a configurable interval that are used to trigger DNS Security Event Resource Limit alarms.
requests	queries-total	Total number of queries received by the CDNS Server.
alarm	security-events-alarm	Total number of security events detected and captured within a configurable interval that are used to trigger DNS Security Event Resource Limit alarms.
amplification	security-events-amplification-attack	Total number of security events due to amplification attack detected and captured.
dos	security-events-dos	Total number of security events due to a potential DoS attack detected and captured.
firewall	security-events-firewall	Total number of security events due to firewall restrictions.
malware	security-events-malware	Total number of security events due to malware detected and captured.
phishing	security-events-phishing	Total number of security events due to DNS phishing detected and captured.
poisoning	security-events-poisoning	Total number of security events due to DNS cache poisoning detected and captured.
snooping	security-events-snooping	Total number of security events due to DNS cache snooping detected and captured.
tunneling	security-events-dns-tunneling	Total number of security events due to DNS tunneling detected and captured.

[10] The statistics listed in this column are the server statistics displayed in the web UI and CLI. The REST API calls will have the statistic name camel-cased without dashes (that is, queries-total is queriesTotal in the REST API). Note that the activity summary and statistics are keyed off the same server data, but the activity-summary names are shortened to conserve space in the log message. For the complete list of Caching DNS server statistics, see the "CDNS Statistics" section of the "Server Statistics" appendix in *Cisco Prime Network Registrar 11.2 Administration Guide*.

System Statistics

The **system** activity-summary-settings logs statistics on system usage.

Sample log message:

```
10/19/2023 10:36:08 cdns tid: 0 Activity Stats 0 22375 [System] Current: conntrack-max=number,
 conntrack-count=number, conntrack-usage=number
```

Table 12: System Statistics

Activity Summary Name	Description
conntrack-max	Maximum number of connection tracking entries allowed.
conntrack-count	Number of connection tracking entries currently in use.
conntrack-usage	Percentage of connection tracking entries in use.

Top Names Statistics

The **top-names** activity-summary-settings logs the top names queried and hit count.

Sample log message:

```
10/19/2023 10:36:08 cdns tid: 0 Activity Stats 0 22371 [Top-Names] from 10:35:03 to 10:36:03;
 interval=number, total-counted=number
```

Table 13: Top Names Statistics

Activity Summary Name	Statistic[11]	Description
interval	N/A	Length of data collection period. It corresponds to the CDNS *top-names-max-age* setting, which controls how long it has to collect the top names for each log entry. It then lists a configurable number of top names (default 10) and the number of queries for those names.
total-counted	total-counted	Total number of queries counted in this collection period.

[11] The statistics listed in this column are the server statistics displayed in the web UI and CLI. The REST API calls will have the statistic name camel-cased without dashes (that is, queries-total is queriesTotal in the REST API). Note that the activity summary and statistics are keyed off the same server data, but the activity-summary names are shortened to conserve space in the log message. For the complete list of Caching DNS server statistics, see the *"CDNS Statistics" section of the "Server Statistics" appendix in Cisco Prime Network Registrar 11.2 Administration Guide*.

Upstream Statistics

The **upstream** activity-summary-settings logs the number of upstream queries.

Sample log message:

```
10/19/2023 10:36:08 cdns tid: 0 Activity Stats 0 22442 [Upstream] Sample since Thu Oct 19
10:35:08 2023: upstream-queries-total=number, upstream-queries-udp=number,
upstream-queries-tcp=number, upstream-queries-tls=number
```

Table 14: Upstream Statistics and

Activity Summary Name	Statistic[12]	Description
upstream-queries-total	N/A	Total number of upstream queries sent.
upstream-queries-udp	upstream-queries-udp	The number of upstream queries sent using UDP.
upstream-queries-tcp	upstream-queries-tcp	The number of upstream queries sent using TCP.
upstream-queries-tls	upstream-queries-tls	The number of upstream queries sent using TLS.

[12] The statistics listed in this column are the server statistics displayed in the web UI and CLI. The REST API calls will have the statistic name camel-cased without dashes (that is, queries-total is queriesTotal in the REST API). Note that the activity summary and statistics are keyed off the same server data, but the activity-summary names are shortened to conserve space in the log message. For the complete list of Caching DNS server statistics, see the *"CDNS Statistics" section of the "Server Statistics" appendix in Cisco Prime Network Registrar 11.2 Administration Guide*.

Specifying Top Names Settings

The *top-names* attribute specifies if top names data should be collected. When enabled, a snapshot of the cache hits for the top names that are queried is collected for each interval set by the *top-names-max-age* value. The list of top names that is reported with activity summary statistics is the most current snapshot.

You can specify the maximum age (based on last access time) of a queried name allowed in the list of top names by using the *top-names-max-age* attribute.

Note The *top-names-max-age* attribute has a default value of 60 seconds.

You can specify the maximum number of entries in the list of top names queried by using the *top-names-max-count* attribute. This limit is applied to the lists of top names that are logged as part of the activity summary or returned as part of the top names statistics. The default value is 10.

Local Web UI

To enable Top Names, on the Edit Local CDNS Server tab, under the **Top Names Settings** section, enable the *top-names* attribute by selecting the **enabled** option, and then click **Save** to save the changes.

Top Names Statistics

The Top Names tab displays the relevant information with respect to top N domains and other important statistics attributes.

Local Web UI

Step 1 From the **Operate** menu, choose **Manage Servers** under the **Servers** submenu to open the Manage Servers page.

Step 2 Click **CDNS** in the Manage Servers pane to open the Edit Local CDNS Server page.

Step 3 Click the **Top Names** tab available in the Local CDNS Server page.

CLI Commands

Use **cdns getStats top-names** to view the Top Names statistics.

Logging Security Events

Since DNS is fundamental to the operation of many endpoints, DNS traffic is often allowed to flow in and out of customer's networks. Also, the DNS traffic is not typically well monitored due to the volume of traffic. This makes DNS a prime target for various DNS attacks. DNS Tunneling/Exfiltration allows information to be carried as payload on top of the DNS protocol. This data can be sensitive corporate data that is being exfiltrated, contacting command and control hosts (botnets), bypassing captive portals for WiFi service, and so on.

Cisco Prime Network Registrar Caching DNS already has support for Response Policy Zones (RPZs) which allows the user to either subscribe to a third-party RPZ service and/or craft their own RPZs. This allows to block domains associated with malicious activity. For more information, see Setting Up RPZ Primary Zones on the Authoritative DNS Server. Similarly, Cisco Prime Network Registrar Caching DNS allows the user to use Cisco Umbrella as a trusted source for query resolution. Cisco Umbrella also blocks/redirects known threats and may also be able to check for new threats or unusual patterns based on the queries it is processing. Along with these, there are also other smaller functions to detect anomalies such as looking for usual DNS requests and the 2008 Kaminsky style protections. Cisco Prime Network Registrar 11.2 provides insight into various security triggers in the form of security events.

Security Events Settings

You can specify whether or not to log security events for the Caching DNS server using the *security-event-logging* attribute on the Manage Servers page. You can also control which security event triggers to log under the **Security Events** section. When the Caching DNS server detects a security event and the related security event log setting is enabled, a log message will be written to the cdns_security_log file.

If *security-event-logging* is disabled, the security events are still monitored for activity summary.

Table 15: Security Events Attributes in the Caching DNS Server

Attribute	Description
Security Event Logging (*security-event-logging*)	Enables DNS security event logging based on settings configured in *security-event-log-settings*. Security event log messages are written to the cdns_security_log file. Note that *security-event-logging* and *security-event-log-settings* configuration changes take effect immediately without requiring a CDNS server reload.

Attribute	Description
Security Event Log Settings (*security-event-log-settings*)	Specifies the DNS security events that should be logged. When the CDNS server detects a security event and the related security event log setting is enabled, a log message will be written to the cdns_security_log file. In order for this setting to take effect, the *log-settings* attribute must include the security setting. Note that *security-event-logging* and *security-event-log-settings* configuration changes take effect immediately without requiring a CDNS server reload. • cisco-umbrella—A security event log message will be generated when Cisco Umbrella forwarders respond with redirected addresses. Note that Cisco Umbrella forwarders must be configured in order for this security event to be caught. Note that a Cisco Umbrella subscription may be required. • configuration—A security event log message will be generated based on DNS server configuration settings (that is, ACL failures). • dnssec—A security event log message will be generated if the CDNS server fails to validate DNSSEC data. DNSSEC validation failures may indicate a cache poisoning attempt. • packet-inspection—A security event log message will be generated based on DNS server detecting issues in the request packet. These issues may be detected by basic packet inspection (that is, *packet-inspection* setting) or during packet processing. Excessive malformed packets may indicate a DoS attack. • rate-limit—A security event log message will be generated if the CDNS server reaches configured IP and/or domain rate limits. Excessive DNS traffic requiring rate limiting may indicate an amplification attack. The default settings are configuration, dnssec, packet-inspection, rate-limit, and cisco-umbrella

Attribute	Description
Security Event Alarm Settings (*security-event-alarm-settings*)	Specifies the DNS security event triggers that will be counted towards resource limit alarming. This allows the user to still be able to get statistics and log messages for all security events, but limits the events that will trigger alarms. Note that *security-event-alarm-settings* configuration changes take effect immediately without requiring a CDNS server reload. • cisco-umbrella—A security event log message will be generated when Cisco Umbrella forwarders respond with redirected addresses. Note that Cisco Umbrella forwarders must be configured in order for this security event to be caught. Note that a Cisco Umbrella subscription may be required. • configuration—A security event log message will be generated based on DNS server configuration settings (that is, ACL failures). • dnssec—A security event log message will be generated if the CDNS server fails to validate DNSSEC data. DNSSEC validation failures may indicate a cache poisoning attempt. • packet-inspection—A security event log message will be generated based on DNS server detecting issues in the request packet. These issues may be detected by basic packet inspection (that is, *packet-inspection* setting) or during packet processing. Excessive malformed packets may indicate a DoS attack. • rate-limit—A security event log message will be generated if the CDNS server reaches configured IP and/or domain rate limits. Excessive DNS traffic requiring rate limiting may indicate an amplification attack.
Maximum Query Name Size (*security-event-max-qname-size*)	Specifies the maximum size of a query name (QNAME) allowed. If a longer hostname is detected, the server will trigger a packet inspection DNS security event for the DNS tunneling category and the query will be refused. A setting of 0 (default) disables query name length checking.

Local Advanced Web UI

Step 1 From the **Operate** menu, choose **Manage Servers** under the **Servers** submenu to open the Manage Servers page.

Step 2 Click **CDNS** in the Manage Servers pane to open the Edit Local CDNS Server page.

Step 3 Under the **Security Events** section, select **enabled** from the *security-event-logging* drop-down list to enable Caching DNS security event logging.

Step 4 For the *security-event-log-settings* attribute, check the desired check boxes.

Step 5 Click **Save** to save the changes.

CLI Commands

Use **cdns enable security-event-logging** to enable DNS security event logging.

Procedure

	Command or Action	Purpose
Step 1	Use **cdns set security-event-log-settings**=*value* to specify the DNS security events that should be logged.	

Security Events Statistics

On the Manage DNS Caching Server page, click the **Statistics** tab to view the Server Statistics page. The Security Events statistics appear under the **Security Events** section of both the Total Statistics and Sample Statistics categories.

Table 16: Security Events Statistics Attributes

Attribute	Description
security-events	Total number of security events detected and captured.
security-events-alarm	Total number of security events detected and captured within a configurable interval that are used to trigger DNS Security Event Resource Limit alarms.
security-events-amplification-attack	Total number of security events due to amplification attack detected and captured.
security-events-dns-tunneling	Total number of security events due to DNS tunneling detected and captured.
security-events-dos	Total number of security events due to a potential DoS attack detected and captured.
security-events-firewall	Total number of security events due to DNS firewall detected and captured.
security-events-malware	Total number of security events due to malware detected and captured.
security-events-phishing	Total number of security events due to DNS phishing detected and captured.
security-events-poisoning	Total number of security events due to DNS poisoning detected and captured.
security-events-snooping	Total number of security events due to caching or data snooping detected and captured.

Security Logs

The Caching DNS security events are saved in the cdns_security_log file. The Security Logs tab displays the the contents of this log file.

Local Web UI

Step 1 From the **Operate** menu, choose **Manage Servers** under the **Servers** submenu to open the Manage Servers page.

Step 2 Click **CDNS** in the Manage Servers pane to open the Edit Local CDNS Server page.

Step 3 Click the **Security Logs** tab.

Security Events Resource Monitoring

On the Edit Local CCM Server page, you can configure the warning and critical levels for Caching DNS security events.

Local and Regional Advanced Web UI

Step 1 From the **Operate** menu, choose **Manage Servers** under the **Servers** submenu to open the Manage Servers page. Click **CCM** in the Manage Servers pane to open the Edit Local CCM Server page.

Step 2 Under the **DNS Security Events** section, enter the required values in the following fields:

- **cdns-security-events-critical-level**—Specifies the critical level for the number of DNS security events in the Caching DNS server. If the server's number of security events exceeds this value, a critical notification is triggered.
- **cdns-security-events-warning-level**—Specifies the warning level for the number of DNS security events in the Caching DNS server. If the server's number of security events exceeds this value, a warning notification is triggered.

Step 3 Click **Save**.

CLI Commands

Use **resource set cdns-security-events-critical-level**=*value* to set the critical level for the number of DNS security events in the Caching DNS server.

Use **resource set cdns-security-events-warning-level**=*value* to set the warning level for the number of DNS security events in the Caching DNS server.

Specifying TLS Settings

DNS queries without encryption are vulnerable to spoofing and other attacks that threaten privacy. To address these issues, Cisco Prime Network Registrar supports DNS over TLS (DoT) as specified by RFC 7858 for both Authoritative DNS server and Caching DNS server.

DNS over TLS is a security protocol for encrypting and wrapping DNS queries and answers via the Transport Layer Security (TLS) protocol. It improves privacy and security between clients and resolvers. It uses TCP as the basic connection protocol and layers over TLS encryption and authentication.

TLS Keys

TLS key pair consists of a private key and a public key. These two keys are related to one another by means of a cryptographic algorithm. The private key is "private" to the server which receives the incoming TLS connection and must be kept secret. The server introduces itself to the client by handing over its certificate. The certificate is a signed ("certified") container that includes the server's public key.

In Cisco Prime Network Registrar, the DNS server listens on configurable port 853 for TLS. On port 853, only TCP TLS connections are accepted and other connections are dropped. The DNS server has configurable parameters to enable or disable TLS, and to add TLS private and public key files, and TLS certificate bundle for upstream.

Caching DNS exceptions and forwarders have configuration parameters to enable or disable TLS for upstream.

Note

- Cisco Prime Network Registrar does not support a command for generating self-signed certificates. However, they can be generated using readily available command line tool like openssl. For example:

  ```
  # openssl req -new -x509 -days 365 -nodes -out public.pem -keyout private.pem
  ```

- TLS is not supported in hybrid mode and in zone transfers.
- TLS keys are not supported with password phrase.

Adding the certificate of ADNS server

For upstream queries, with the public.pem and private.pem of the forwarder/exception servers create a certificate object in the Caching DNS server and update the same in *tls-upstream-cert-bundle*.

Table 17: TLS Attributes in the Caching DNS Server

Attribute	Description
TLS (*tls*)	Before enabling TLS, certificate object of type cdns must be created using public and private key files and *tls-certificate* attribute be set. Enabling or disabling TLS service requires a Cisco Prime Network Registrar service restart for the change to take effect.
TLS Port (*tls-port*)	The port number on which to provide TCP TLS service. The Caching DNS server will not serve non-TLS queries on this port.
TLS Certificate (*tls-certificate*)	Specifies the name of the managed certificate to be used for DNS over TLS (DoT) or DNS over HTTPS (DoH).
TLS Certificate Bundle File (*tls-upstream-cert-bundle*)	Defines the file name which contains the certificate bundle (that is, cdns_tls_upstream_cert_bundle.crt). These certificates are used for TLS connections made to outside peers. These certificates are used to authenticate connections made to upstream DNS servers. The file must be in the CDNS data directory under the **tls** subdirectory (that is, <cnr.datadir>/cdns/tls). When TLS is enabled, the CDNS server will generate this file during server configuration and add entries for all managed certificates. The CDNS will also append system certificates to this file. See the tls-system-cert-bundle setting for more details on system certificates.

Attribute	Description
TLS System Certificate Bundle File (*tls-system-cert-bundle*)	Specifies the file path to the system certificate bundle (that is, /etc/pki/tls/certs/ca-bundle.crt). When TLS is enabled, CDNS will read this certificate bundle during configuration and append it to the tls-upstream-cert-bundle file. This will allow CDNS to use system certificates when communicating with upstream DNS servers. In order to disable the use of the system certificate bundle, set this setting to disabled.

You can also enable TLS at the forwarder (see Using Forwarders), exception (see Using Exceptions), and at the firewall (see Enabling TLS for RPZ) level.

Local Advanced Web UI

To enable TLS support for the Caching DNS server, do the following:

Before you begin

Before enabling TLS, you must create certificate object of type cdns using the public and private key. Under the **TLS Settings** section on the Manage DNS Caching Server page, set tls-certificate attribute to the created certificate object.

Step 1 From the **Operate** menu, choose **Manage Servers** under the **Servers** submenu to open the Manage Servers page.

Step 2 Click **CDNS** in the Manage Servers pane to open the Edit Local CDNS Server page.

Step 3 Under the **TLS Settings** section, enable the *TLS* attribute by selecting the **enabled** option.

Step 4 Click **Save** to save the changes.

Note You must restart the Cisco Prime Network Registrar service whenever TLS settings are modified.

CLI Commands

Use **cdns enable tls** to enable TLS support for the Caching DNS server. Then, use **systemctl restart nwreglocal.service** to restart the Cisco Prime Network Registrar service.

Use **cdns set** *attribute=value* to set the TLS attributes in the Caching DNS server.

Note You must restart the Cisco Prime Network Registrar service whenever TLS settings are modified.

TLS Statistics

On the Manage DNS Caching Server page, click the **Statistics** tab to view the Server Statistics page. The *queries-over-tls* attribute appears under the **Query Details** section of both the Total Statistics and Sample Statistics categories. The *tls-errors-in* and *tls-errors-out* attributes appear under the **Server Statistics** section of both the Total Statistics and Sample Statistics categories.

Table 18: TLS Statistics Attributes

Attribute	Description
queries-over-tls	Total number of queries received over TLS by the CDNS Server. This statistic is also incremented when queries are received over HTTPS.
tls-errors-in	Total number of TLS related errors on inbound DNS query attempts. An error may occur whether a query was succcessfully received or not.
tls-errors-out	Total number of TLS related errors on outbound DNS query attempts. An error may occur whether a query was successfully transmitted or not.

Specifying HTTPS Settings

DNS over HTTPS (DoH) is a protocol for sending DNS queries and getting DNS responses over HTTPS. Each DNS query-response pair is mapped into an HTTP exchange. The goal of this method is to increase user privacy and security by preventing eavesdropping and manipulation of DNS data by man-in-the-middle attacks. To achieve this, it uses the HTTPS protocol to encrypt the data between DoH client and DoH-based DNS resolver. Typically, DoH involves a client accessing a caching server known to support DoH.

Starting Cisco Prime Network Registrar 11.1, the Caching DNS server supports DoH. Caching DNS supports DoH only for incoming queries. The Caching DNS server listens on configurable port 443 for HTTPS. If network interfaces are not configured, then the server listens on HTTPS port, TLS port, and DNS port (TCP and UDP) on all network interfaces. If network interfaces are configured manually, then the server listens on HTTPS port, TLS port, and DNS port (TCP and UDP) on those configured network interfaces. In Cisco Prime Network Registrar, the DoH configuration is available in web UI, CLI, and REST API.

Note

- Cisco Prime Network Registrar does not support a command for generating self-signed certificates. However, they can be generated using readily available command line tool like openssl.
- DoH configuration is not supported in Authoritative DNS and for upstream queries.

Table 19: HTTPS Attributes in the Caching DNS Server

Attribute	Description
HTTPS	Enables or disables HTTPS support for Caching DNS. DoH is supported only for incoming queries. DoH supports GET and POST methods as specified in RFC 8484. Before enabling HTTPS, the private and public key files must be placed in the CDNS data directory under cdns/tls and the *service-key* and *service-pem* attributes be set. If using managed CDNS certificates, the certificate settings will be automatically set. Otherwise, the public certificate file must be placed in the CDNS data directory under cdns/tls and the *service-pem* attribute be set.

Attribute	Description
HTTPS Port (*https-port*)	The port number on which to provide HTTPS service. The Caching DNS server will not serve non-HTTPS queries on this port.

Local Advanced Web UI

To enable DoH support in the Caching DNS server, do the following:

Step 1 From the **Operate** menu, choose **Manage Servers** under the **Servers** submenu to open the Manage Servers page.

Step 2 Click **CDNS** in the Manage Servers pane to open the Edit Local CDNS Server page.

Step 3 Under the **HTTPS Settings** section, enable the *HTTPS* attribute by selecting the **enabled** option. In the *https-port* field, enter the port number on which to provide HTTPS service. The value can be any integer in the range of 1 to 65535. The default value is 443. Note that the Caching DNS server will not serve non-HTTPS queries on this port.

Step 4 Click **Save** to save the changes.

CLI Command

Use **cdns enable https** to enable DoH support in the Caching DNS server.

HTTPS Statistics

On the Manage DNS Caching Server page, click the **Statistics** tab to view the Server Statistics page. The *queries-over-https* attribute appears under the **Query Details** section of both the Total Statistics and Sample Statistics categories. The *queries-over-https-failed*, *https-query-buffer*, and *https-response-buffer* attributes appear under the **Server Statistics** section of both the Total Statistics and Sample Statistics categories.

Table 20: HTTPS Statistics Attributes

Attribute	Description
queries-over-https	Total number of queries received over HTTPS by the CDNS server.
queries-over-https-failed	Total number of queries failed with HTTPS errors.
https-query-buffer	Number of HTTPS queries in memory buffer.
https-response-buffer	Number of HTTPS responses in memory buffer.

HTTP Error Codes

Following HTTP error codes are supported in DoH:

- HTTP_STATUS_OK (200): DoH is able to process the query and return an answer. This could be a negative answer or an error like SERVFAIL or FORMERR.
- HTTP_STATUS_BAD_REQUEST (400): No valid query received.

- HTTP_STATUS_NOT_FOUND (404): The request is directed to a path other than the configured endpoint in http-endpoint (default /dns-query).
- HTTP_STATUS_PAYLOAD_TOO_LARGE (413): The payload received in the POST request is too large. Payloads cannot be larger than the content-length communicated in the request header. The payload length is limited to 512 bytes if harden-large-queries is enabled.
- HTTP_STATUS_URI_TOO_LONG (414): The base64url encoded DNS query in the GET request is too large. The DNS query length is limited to 512 bytes if harden-large-queries is enabled.
- HTTP_STATUS_UNSUPPORTED_MEDIA_TYPE (415): The media type of the request is not supported. DoH currently only supports the "application/dns-message" media type. Requests without content-type will be treated as application/dns-message.
- HTTP_STATUS_NOT_IMPLEMENTED (501): The method used in the request is not GET or POST.

Setting Prefetch Timing

Use the *Prefetch* attribute under the **Smart Cache** section to set whether message cache elements should be prefetched before they expire to keep the cache up to date. Turning it **on** gives about 10 percent more traffic and load on the machine, but can increase the query performance for popular DNS names.

When *Prefetch* is enabled, records are assigned a prefetch time that is within 10 percent of the expiration time. As the server processes client queries and looks up the records, it checks the prefetch time. Once the record is within 10 percent of its expiration, the server will issue a query for the record to keep it from expiring.

Setting Cache TTLs

Time to Live (TTL) is the amount of time that a DNS server is allowed to cache data learned from other nameservers. Each record added to the cache arrives with some TTL value. When the TTL period expires, the server must discard the cached data and get new data from the authoritative nameservers the next time it sends a query. TTL attributes, *cache-min-ttl* and *cache-max-ttl* defines the minimum and maximum time Cisco Prime Network Registrar retains the cached information. These parameters limit the lifetime of records in the cache whose TTL values are very large or very small.

Local Web UI

Step 1 From the **Operate** menu, choose **Manage Servers** under the **Servers** submenu to open the Manage Servers page. Click **CDNS** on the Manage Servers pane.

Step 2 On the Edit Local CDNS Server tab, under the **Caching** section, you can find:

- The Maximum Cache TTL (*cache-max-ttl*) attribute, set it to the desired value (the default value is 24 hours)
- The Min Cache TTL (*cache-min-ttl*) attribute, set it to the desired value (the preset value is 0)

Step 3 Click **Save** to save the changes.

CLI Commands

Use **cdns set cache-max-ttl**=*value* to set the maximum Cache TTL value.

Use **cdns set cache-min-ttl** =*value* to set the minimum Cache TTL value.

Smart Cache settings

Whenever Authoritative DNS servers face an outage or are offline for other reasons, this could cause issues with being able to reach Internet services that are likely not impacted. Smart caching allows the Caching DNS server to continue to serve the expired data (last known answer) when it cannot reach the authoritative name servers. The Caching DNS server will still continue to contact the authoritative name servers and when the name servers are once again functional, the Caching DNS server will update its cached data.

Note Enabling Smart Cache (*smart-cache*) automatically enables prefetch.

Smart Cache Configuration Settings

The *smart-cache* attribute is enabled by default at the Caching DNS server level.

When the Caching DNS server receives a query for data that has expired and if the *smart-cache* attribute is enabled, it will continue to respond with its expired cached data and increment the *smart-cache* counter under the **Query Details** section in the Statistics tab.

Note Smart Cache is available in Advanced mode and requires a Caching DNS server reload to take effect.

Table 21: Smart Cache Attributes

Attribute	Description
Smart Cache (*smart-cache*)	Specifies if the Caching DNS server should use Smart Caching. With *smart-cache* attribute enabled, the Caching DNS server continues to use its last best known answer when cached responses have expired and it cannot reach the authoritative name servers. The RRs in smart cache responses will have a 0 TTL. Smart Caching is useful to mitigate network outages and possible DDoS attacks that make the authoritative name servers unavailable. The *smart-cache* attribute is enabled by default
Smart Cache Expiration (*smart-cache-expiration*)	When *smart-cache* is enabled, specifies a time limit for responding with expired RRs. The default is 0, which allows the server to respond with expired answers as long as they remain in the cache.

Attribute	Description
Smart Cache Expiration Reset (*smart-cache-expiration-reset*)	When *smart-cache* is enabled and *smart-cache-expiration* is greater than 0, will reset the expiration time on active queries. This allows active queries to return expired answers, while allowing others to return SERVFAIL responses for a short period. Once the queries become active, will return expired answers. Default is disabled.
Smart Cache Expired Reply TTL (*smart-cache-expired-reply-ttl*)	When *smart-cache* is enabled, specifies the TTL value to use when replying with expired data.
Prefetch (*prefetch*)	Sets whether message cache elements should be prefetched before they expire to keep the cache up to date. Turning it on gives about 10 percent more traffic and load on the machine, but popular items do not expire from the cache. When *Prefetch* is enabled, records are assigned a prefetch time that is within 10 percent of the expiration time. As the server processes client queries and looks up the records, it checks the prefetch time. Once the record is within 10 percent of its expiration, the server will issue a query for the record in order to keep it from expiring.

Note From Cisco Prime Network Registrar 10.1, the *Prefetch* attribute is available under the **Smart Cache** section and it is an Advanced mode feature.

Local Advanced Web UI

Step 1 From the **Operate** menu, choose **Manage Servers** under the **Servers** submenu to open the Manage Servers page.

Step 2 Click **CDNS** in the Manage Servers pane to open the Edit Local CDNS Server page.

Step 3 On the Edit Local CDNS Server page, under the **Smart Cache** section, do the following steps with the *smart-cache* attribute enabled by default:

- The Smart Cache Expiration (*smart-cache-expiration*) attribute to specify a time limit for responding with expired RRs (the default value is 0)
- The Smart Cache Expiration Reset (*smart-cache-expiration-reset*) attribute to reset the expiration time on active queries with *smart-cache-expiration* attribute value greater than 0

CLI Commands

Use **cdns set smart-cache-expiration=***value* to specify a time limit for responding with expired RRs, when *smart-cache* is enabled. For example:

```
nrcmd> cdns set smart-cache-expiration=5m
```

Use **cdns enable smart-cache-expiration-reset** to reset the expiration time on active queries, when *smart-cache* is enabled and *smart-cache-expiration* is greater than 0.

Defining Root Nameservers

Root nameservers know the addresses of the authoritative nameservers for all the top-level domains. When you first start a newly installed Cisco Prime Network Registrar Caching DNS server, it uses a set of preconfigured root servers, called root hints, as authorities to ask for the current root nameservers.

When Cisco Prime Network Registrar gets a response to a root server query, it caches it and refers to the root hint list. When the cache expires, the server repeats the process. The TTL on the official root server records is preconfigured and you can specify a different cache TTL value (see Setting Cache TTLs, on page 28).

As the configured servers are only hints, they do not need to be a complete set. You should periodically (every month to six months) look up the root servers to see if the information needs to be altered or augmented.

Local Web UI

On the Edit Local CDNS Server tab, under the **Root Name Servers** section, enter the domain name and IP address of each additional root nameserver, clicking **Add Root Namerserver** after each one, then click **Save**.

CLI Commands

Use **cdns addRootHint** *name addr* [*addr* ...] to add the name of a root server and the root name server address(es).

Dynamic Allocation of UDP Ports

The Caching DNS server uses a large number of UDP port numbers, by default up to 50000 port numbers. These numbers are divided among the processing threads. The large number of port numbers reduce the risk of cache poisoning via Birthday Attacks. The Caching DNS server uses the default pool of UDP ports (2048) and the maximum allowable size of the default pool of UDP ports is 4096.

Currently, Cisco Prime Network Registrar uses the port range from 1024 to 65535. Based on the number of outstanding resolution queries, the Caching DNS server adjusts the pool size by adding or removing ports. The Caching DNS server allocates and releases the UDP ports dynamically when the server is running. If you reload the server, all the UDP ports are released and randomly picked again.

Setting Maximum Memory Cache Sizes

The maximum memory cache size property specifies how much memory space you want to reserve for the DNS in-memory cache. The larger the memory cache, the less frequently the Caching DNS server will need to re-resolve unexpired records.

Local Advanced Web UI

On the Edit Local CDNS Server tab, under the **Caching** section, set the desired value for the RRSet Cache Size (*rrset-cache-size*) attribute, then click **Save**. The default size is 1 GB.

To set the size of the message cache, use the Message Cache Size (*msg-cache-size*) attribute. The message cache stores query responses. The default size is 1 GB.

CLI Commands

- Use **cdns set rrset-cache-size** to set RRSet Cache Size.
- Use **cdns set msg-cache-size** to set Message Cache Size.

Specifying Resolver Settings

Glue record(s) is/are A record(s) for name server(s) that cannot be found through normal DNS processing because they are inside the zone they define. When the *harden-glue* attribute is enabled, the Caching DNS server will ignore glue records that are not within the zone that is queried. The *harden-glue* attribute is on by default.

Domain randomization allows a DNS server to send upstream queries for resolution with a randomly generated query name. A valid name server responds with the query name unchanged and therefore this technique can be used to ensure that the response was valid.

On certain occasions, an attacker issues a request and floods the server with fake responses in an attempt to poison the DNS server's cache with rogue data. Randomizing the case gives the server another level of protection against this type of attacks.

Cisco Prime Network Registrar supports randomizing upstream queries, but there are some name servers that do not maintain the randomized case. Therefore, if you enable case randomization, you may block out valid name servers. The *randomize-query-case-exclusion* attribute allows you to create an exclusion list, so that you can continue to use case randomization, but exclude name servers that do not maintain the case but still respond with a valid answer.

Cisco Prime Network Registrar supports Query name minimisation feature (RFC-9156). This feature lets the server minimize the query name it sends to upstream servers. This limits the amount of query name information that is sent to servers that do not need it.

Note The Query name minimisation feature should not be used if connected to CPNR DNS servers prior to CPNR 11.0 or other DNS servers that do not report NOERROR for empty non-terminals.

Table 22: Resolver Settings Attributes

Attribute	Description
harden-glue	Specified if glue should only be trusted if it is within the servers authority.
randomize-query-case	Enables the use of 0x20-encoded random bits in the query to foil spoof attempts. This perturbs the lowercase and uppercase of query names sent to authority servers and checks if the reply still has the correct casing.
randomize-query-case-exclusion	Allows to create an exclusion list for randomization of upstream queries. This attribute will be used when *randomize-query-case* is enabled.
query-name-minimisation	Enables query name minimisation. This limits the amount of query name information that is sent to servers that do not need it.

Configuring Case Randomization Exclusions

The *randomize-query-case-exclusion* attribute is available under the **Resolver Settings** section on the Manage DNS Caching Server page. The *randomize-query-case* is not enabled by default. To use randomize query case exclusion, the *randomize-query-case* attribute must be enabled at the Caching DNS server level.

Both *randomize-query-case* and *randomize-query-case-exclusion* attributes are available in the web UI in Advanced mode.

Local Advanced Web UI

Step 1 From the **Operate** menu, choose **Manage Servers** under the **Servers** submenu to open the Manage Servers page.

Step 2 Click **CDNS** in the Manage Servers pane to open the Edit Local CDNS Server page.

Step 3 Under the **Resolver Settings** section:

a) Enable the *randomize-query-case* attribute by selecting the **enabled** option.

b) In the *randomize-query-case-exclusion* field, enter the list of domains (comma separated) that you want to exclude from case randomization.

Step 4 Click **Save** to save the changes.

Note You must reload the Caching DNS server for the changes to take effect.

CLI Commands

Use **cdns enable randomize-query-case** to enable the case randomization.

Use the **cdns set** and **cdns unset** commands to set or unset *randomize-query-case-exclusion*. For example:

```
nrcmd> cdns set randomize-query-case-exclusion="cisco.com"
nrcmd> cdns set randomize-query-case-exclusion="cisco.com, example.com"
nrcmd> cdns unset randomize-query-case-exclusion
```

Configuring Query Name Minimisation

The query name minimisation settings is available under the **Resolver Settings** section on the Manage DNS Caching Server page. The *query-name-minimisation* attribute is available in the Web UI in Advanced mode and is not enabled by default.

Local Advanced Web UI

Step 1 From the **Operate** menu, choose **Manage Servers** under the **Servers** submenu to open the Manage Servers page.

Step 2 Click **CDNS** in the Manage Servers pane to open the Edit Local CDNS Server page.

Step 3 Under the **Resolver Settings** section:

a) Enable the *query-name-minimisation* attribute by selecting the **enabled** option.

Step 4 Click **Save** to save the changes.

Note You must reload the Caching DNS server for the changes to take effect.

CLI Commands

Use **cdns enable query-name-minimisation** to enable the query-name-minimisation.

Specifying Network Settings

The *listen-ip-version* attribute lets you to choose the IP packets to accept and issue. You can check IPv4, IPv6, or both. The *listen-protocol* attribute lets you to choose the packet protocol to answer and issue. You can check UDP, TCP, or both.

Note The default *listen-ip-version* is both IPv4 and IPv6. You can change this to IPv4 if the server you are running does not support IPv6 or does not have IPv6 connections to upstream name servers. Otherwise, you will likely experience query timeouts.

Table 23: Network Settings Attributes

Attribute	Description
Listening Port (*port*)	Specifies the UDP and TCP port number that the DNS caching server uses to listen for queries.
Incoming TCP (*incoming-num-tcp*)	Sets the number of incoming TCP buffers to allocate per thread. If set to 0, or if the DNS caching server is not listening for TCP queries, no TCP queries from clients are accepted. If multiple interfaces are configured, this number is applied to each interface for each thread. If tls or http is enabled for the Caching DNS Server, this number is also applied to these services per interface and for each thread.
listen-ip-version	Controls which ip packets to accept and issue, IPv4, IPv6, or both.
listen-protocol	Controls which packet protocol to answer and issue, UDP, TCP, or both.

Enabling Client Subnet

The EDNS0 Client Subnet (Client Subnet) feature allows an authoritative DNS server to provide the most appropriate response to its end user client. This is especially useful when the DNS Recursive Resolver (caching DNS server) closest to the Authoritative DNS Server is topologically far from the end user client. The Client Subnet feature allows the caching DNS server closest to the client may attach part of the client's IP address to its upstream queries to signal authoritative servers where in the network the client resides and how to select the best response.

The appropriate response to the end user client is given by using the ECS (EDNS Client Subnet) option for the EDNS0 feature of the DNS protocol as mentioned in the RFC 7871.

In Cisco Prime Network Registrar, the EDNS0 Client Subnet (ECS) option is not enabled by default. To use ECS, the *ecs-enable* attribute must be enabled at the Caching DNS server level.

Once the ECS option is enabled, the ECS data will be created based on the below shown criteria:

- If the CDNS client does not supply an ECS option in its query, if *ecs-always-forward* is on, the ECS option data is created from the client's IP address. If *ecs-always-forward* is off, only queries allowed by *ecs-destination* are forwarded with ECS option.
- If the DNS client does supply an ECS option in its query, use the client's ECS data.

When an answer contains the ECS option, the response and the option are placed in the ECS cache. If the authority indicated no support, the response is stored in the regular cache. Currently, the ECS cache is only flushed on reload.

The *ecs-destination* attribute includes both IPv4 and IPv6 addresses and prefixes as well as domains.

Table 24: EDNS Client Subnet Attributes

Attribute	Description
Enable EDNS Client Subnet (*ecs-enable*)	Enables the EDNS0 Client Subnet feature.
Destinations for ECS (*ecs-destination*)	Specifies to which IP addresses, subnets, prefixes, or DNS zones EDNS0 Client Subnet information will be sent. Default is all addresses.
Always Apply ECS (*ecs-always-forward*)	If on, specifies that all incoming queries with an EDNS0 Client Subnet option should be resolved using the ECS feature, even if the authoritative name server is not specified in the "Destination for ECS" attribute.

Local Advanced Web UI

To enable Client Subnet, do the following:

Step 1 From the **Operate** menu, choose **Manage Servers** under the **Servers** submenu to open the Manage Servers page.

Step 2 Click **CDNS** in the Manage Servers pane to open the Edit Local CDNS Server page.

Step 3 Under the **Enable Client Subnet** section, enable the *ecs-enable* attribute by selecting the **enabled** option.

Step 4 Click **Save** to save the changes.

CLI Command

Use **cdns enable ecs-enable** to enable Client Subnet.

Specifying Advanced Settings

The *minimal-responses* attribute controls whether the DNS Caching server omits or includes records from the authority and data sections of query responses when these records are not required. Enabling this attribute may improve query performance such as when the DNS server is configured as a caching server.

The *remote-ns-host-ttl* attribute sets TTL for entries in the remote name server cache. The remote name server cache contains roundtrip timing (RTT), lameness and EDNS support information. Once an entry expires, it is removed from the remote name server cache and the next time the server is contacted a new entry will be added.

Note that RTT is used to decide which name server to query. If a timeout occurs, the RTT value of that server is doubled. If a server starts to become unresponsive, a probing scheme is applied in which a few queries are selected to probe the IP address. If that fails, the name server is blocked for 15 minutes (*remote-ns-host-ttl*) and re-probed with one query after that. Therefore, it may be necessary to decrease the *remote-ns-host-ttl* to allow probing more frequently. The remote name server cache is not flushed after a CDNS server reload, but can be flushed using the **cdns execute flush-ns-cache** command.

The *remote-ns-cache-numhosts* attribute lets you to set the number of hosts for which information is cached.

Enabling Round-Robin

A query might return multiple A or AAAA records for a name lookup. To compensate for most DNS clients starting with, and limiting their use to, the first record in the list, *round-robin* is enabled to share the load. This ensures that successive clients resolving the same name will connect to different addresses on a revolving basis. The DNS server then rearranges the order of the records each time it is queried. It is a method of load sharing, rather than load balancing, which is based on the actual load on the server.

Local Advanced Web UI

On the Edit Local CDNS Server tab, under the **Advanced Settings** section, find the *round-robin* attribute.

CLI Commands

Use **cdns get round-robin** to see if round-robin is enabled (it is by default). If not, use **cdns enable round-robin**.

Flushing Caching DNS Cache

Cisco Prime Network Registrar cache flushing function lets you remove all or a portion of cached data in the memory cache of the server.

Local Web UI

Step 1 From the **Deploy** menu, choose **CDNS Server** under the **DNS** submenu to open the Manage DNS Caching Server page.

Step 2 On the Manage DNS Caching Server page, click the **Commands** button to open the CDNS Command dialog box. There will be two types of cache flushing commands.

- **Flush the CDNS cache**—Allows you to either flush all cache entries for a particular zone or the entire cache if no zone is provided. To remove all data for a specific zone, enter the zone name in the Zone field. To clear the whole cache, leave the Zone field empty.
- **Flush Resource Record**—Allows you to flush an RR name or an RRSet when the type field is specified.

- Remove common RR types (A, AAAA, NS, SOA, CNAME, DNAME, MX, PTR, SRV, NAPTR, and TXT) from a specific domain—Enter the required RR name as the FQDN for the Flush Resource Record command and leave the RR type field empty.
- Remove a specified RR type for a domain—Specify the domain in the FQDN field, and the RR type in the RR type field.

Note When no type is specified, the server flushes types A, AAAA, NS, SOA, CNAME, DNAME, MX, PTR, SRV, TXT, and NAPTR.

CLI Commands

- Use the following command to remove all cached entries at or below a given domain. If no domain is given, it flushes all RRs in the cache.

  ```
  nrcmd> cdns flushCache domain
  ```

- Use the following command to flush RRs from the cache associated with the given RR name. When type is provided, it flushes all entries with the given name and type. If no type is provided, it flushes types A, AAAA, NS, SOA, CNAME, DNAME, MX, PTR, SRV, TXT, and NAPTR.

  ```
  nrcmd> cdns flushName name type
  ```

Detecting and Preventing DNS Cache Poisoning

Cisco Prime Network Registrar enhances the Caching DNS server performance to address the CDNS related issues such as DNS cache poisoning attacks (CSCsq01298), as addressed in a Cisco Product Security Incident Response Team (PSIRT) document number PSIRT-107064 with Advisory ID cisco-sa-20080708-dns, available at:

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080708-dns

DNS Cache Poisoning Attacks

A cache poisoning attack can change an existing entry in the DNS cache as well as insert a new invalid record into the DNS cache. This attack causes a hostname to point to the wrong IP address. For example, let us say that www.example.com is mapped to the IP address 192.168.0.1, and this mapping is present in the cache of a DNS server. An attacker can poison the DNS cache and map www.example.com to 10.0.0.1. If this happens, if you try to visit www.example.com, you will end up contacting the wrong web server.

A DNS server that uses a single static port for receiving responses to forwarded queries are susceptible to malicious clients sending forged responses.

The DNS transaction ID and source port number used to validate DNS responses are not sufficiently randomized and can easily be predicted, which allows an attacker to create forged responses to DNS queries. The DNS server will consider such responses as valid.

Handling DNS Cache Poisoning Attacks

To reduce the susceptibility to the DNS cache poisoning attack, the DNS server randomizes the UDP source ports used for forwarded queries. Also, a resolver implementation must match responses to the following attributes of the query:

- Remote address
- Local address
- Query port
- Query ID
- Question name (not case-sensitive)
- Question class and type, before applying DNS trustworthiness rules (see [RFC2181], section 5.4.1)

Note The response source IP address must match the query's destination IP address and the response destination IP address must match the query's source IP address. A mismatch must be considered as format error, and the response is invalid.

Resolver implementations must:

- Use an unpredictable source port for outgoing queries from a range (either 53, or > 1024) of available ports that is as large as possible and practicable.
- Use multiple different source ports simultaneously in case of multiple outstanding queries.
- Use an unpredictable query ID for outgoing queries, utilizing the full range available (0 to 65535). By default, CDNS uses up to 48000 port numbers.

The Caching DNS server attribute *randomize-query-case*, when enabled, specifies that when sending a recursive query, the query name is pseudo-randomly camel-cased and the response is checked to see if this camel-casing is unchanged. If *randomize-query-case* is enabled and the casing has changed, then the response is discarded. The *randomize-query-case* is disabled by default, disabling this feature.

Local Basic or Advanced Web UI

The Caching DNS server statistics appears on the Statistics tab of the Manage DNS Caching Server page. The Statistics displays the *answers-unwanted* values. You can refresh the DNS Caching Server Statistics by clicking the **Refresh Server Statistics** icon at the top of the statistics table.

Handling Unresponsive Nameservers

When trying to resolve query requests, Caching DNS servers may encounter unresponsive nameservers. A nameserver may be unresponsive to queries or respond late. This affects the performance of the local DNS server and remote nameservers.

Using Cisco Prime Network Registrar, you can resolve these problems by barring unresponsive nameservers. You can configure a global ACL of unresponsive nameservers that are to be barred, using the *acl-do-not-query* attribute.

When Cisco Prime Network Registrar receives a list of remote nameservers to transmit a DNS query request to, it checks for the nameservers listed in the *acl-do-not-query* list and removes them from this list. Conversely, all incoming DNS requests from clients or other nameservers are also filtered against *acl-blocklist*.

Use the *acl-query* attribute to specify which clients are allowed to query the server. By default, any client is allowed to query the server. A client that is not in this list will receive a reply with status REFUSED. Clients on the *acl-blocklist* do not get any response whatsoever.

Local Advanced Web UI

On the Edit Local CDNS Server tab, expand the **Query Access Control** section to view the various attributes and their values. For the Do Not Query (*acl-do-not-query*) attribute, enter the value (for example, 10.77.240.73). Then, click **Save**.

Tuning Network Buffers

It may be necessary to adjust network buffers for busy servers. Cisco Prime Network Registrar Caching DNS server makes the following Expert mode parameters available to run the receive and send buffers for the server without effecting other processes on the system.

- **so-rcvbuf**—Sets the SO_RCVBUF socket option to get more buffer space for incoming queries, so that short spikes on busy servers do not drop packets. The operating system caps it at a maximum. Default is 0 (uses the system value).
- **so-sndbuf**—If not 0, the SO_SNDBUF socket option is used to adjust the buffer space on the UDP port used for outgoing queries. For very busy servers, this handles spikes in answer traffic. Default is 0 (uses the system value).

Note The system administrator is responsible for setting the correct tuning parameters as they are deployment specific.

Local Expert Web UI

On the Edit Local CDNS Server tab, expand the **Network Settings** section to view the **so-rcvbuf** and **so-sndbuf** attributes.

Running DNS Caching Server Commands

Access the DNS Caching server commands using the Commands button. Clicking the **Commands** button opens the CDNS Commands dialog box in the local web UI. Each command has its own Run icon (click it, then close the dialog box):

- **Flush the CDNS cache**— This command allows you to flush either all RRs or RRs for a particular zone from the in-memory cache. See Flushing Caching DNS Cache, on page 36.
- **Flush Resource Record**— This command that lets you specify an RR name and optionally a type to remove from the in-memory cache.

Note To remove all the entries from the in-memory cache, you need to reload the Caching DNS server.

Note If you find a server error, investigate the server log file for a configuration error, correct the error, return to this page, and refresh the page.

Configuring Caching DNS Server Network Interfaces

You can configure the network interfaces for the Caching DNS server from the Manage Servers page in the local web UI. When no interfaces are explicitly configured, the server will use all the available interfaces for inbound (client) and outbound (upstream) queries. If interfaces are configured, the server will only use those interfaces for all query traffic, inbound and outbound.

Local Advanced Web UI

Step 1 From the **Operate** menu, choose **Manage Servers** under the **Servers** submenu to open the Manage Servers page.

Step 2 Click **CDNS** in the Manage Servers pane to open the Edit Local CDNS Server page.

Step 3 Click the **Network Interfaces** tab to view the available network interfaces that you can configure for the server. By default, the server uses all of them.

Step 4 To configure an interface, click the **Configure** icon in the Configure column for the interface. This adds the interface to the Configured Interfaces table, where you can edit or delete it.

Step 5 Click the name of the configured interface to edit the configured interfaces, where you can change the address, direction and port of the interface.

Step 6 Click **Modify Interface** when you are done editing, then click **Go to Server Interfaces** to return to the Network Interfaces page.

Configuring CDNS Server in Regional

You can set properties for the CDNS server in regional. The CDNS Server Config page has been designed for CDNS pod to fetch the CDNS server related configuration.

For more information on setting the DNS Caching Server properties, refer to Setting DNS Caching Server Properties, on page 1.

Regional Advanced Web UI

From the Design menu, choose **CDNS Server Config** under Cache DNS to access the Caching DNS server attributes.

CLI Commands

Use the following commands to set, get, and unset the CDNS Config related attributes.

```
cdns-config <name> set <attribute>=<value> [<attribute>=<value>...]
cdns-config <name> unset <attribute>
cdns-config <name> get <attribute>
```

For example:

```
nrcmd-R> cdns-config Default set packet-log-settings=+query-out,response-in
```

```
nrcmd-R> cdns-config Default get packet-log-settings=query-in,query-out,
response-in,response-out

nrcmd-R> cdns-config Default unset packet-log-settings
```