Managing Caching DNS Server

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.

Configuring CDNS Server Network Interfaces

You can configure the network interfaces for the CDNS server from the Manage Servers page in the local web UI.

Local Advanced Web UI

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

Step 2 Select **Local CDNS Server** from the Manage Servers pane.

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.

Setting DNS Caching Server Properties

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

- **General server properties—**See Setting General CDNS Server Properties, on page 2
- **Log Settings—**See Specifying Log Settings, on page 3
- **Activity Summary Settings—**See Specifying Activity Summary Settings, on page 3
- **Caching Settings —**See Setting Prefetch Timing, on page 4
- **Cache TTLs—**See Setting Cache TTLs, on page 4
- **Root name servers—**See Defining Root Nameservers, on page 5
- **UDP Ports—**See Dynamic Allocation of UDP Ports, on page 5
- **Maximum memory cache sizes—**See Setting Maximum Memory Cache Sizes, on page 6
- **Resolver Settings—**See Specifying Resolver Settings, on page 6
- **Network Settings—**See Specifying Network Settings, on page 6
- **Advanced Settings—**See Specifying Advanced Settings, on page 6
- **Flush cache—**See Flushing CDNS Cache, on page 7
- **Prevent DNS cache poisoning—**See Detecting and Preventing DNS Cache Poisoning, on page 8
- **Handle unresponsive nameservers—**See Handling Unresponsive Nameservers, on page 9

Setting General CDNS Server Properties

You can view CDNS general 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 2.

Local Basic or Advanced Web UI

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

Step 2 Select **Local CDNS Server** from the CDNS Server pane, to open the Edit Local CDNS Server page. The page displays all the CDNS server attributes.

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

CLI Commands

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

Specifying Log Settings

This setting determines which detailed events the Caching DNS server logs, as set using a bit mask. Logging these additional details can help analyze a problem. Leaving detailed logging enabled for a long period, however, can fill the log files and cause the loss of important information.

The possible options are:

- **config—**Controls logging pertaining to server configuration and server de-initialization (unconfiguration).
- **server-ops—**Controls high level logging of server operations.
- **server-detailed-ops—**Controls detailed logging of server operations.
- **scp—**Controls logging pertaining to SCP message processing.
- **activity-summary—**This causes a summary message to appear at an interval specified by activity-summary-interval. The summary provides detailed statistics about the servers operation.
- **query—**Causes logging of all DNS queries to the server.

Specifying Activity Summary Settings

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

You can specify the interval at which to log activity-summary information using the Statistics Interval (*activity-summary-interval*) attribute.

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

Note The *Activity-summary- interval* attribute has a default value of 60 seconds. The default *Activity-summary -type* is sample.

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

- query—Logs statistics related to incoming queries.
- query-type—Logs statistics on the RR types that are being queried.
- cache—Logs statistics on the RR cache.
- resol-queue—Logs statistics on the resolution queue.
- responses—Logs statistics about query responses.

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

Setting Prefetch Timing

Use the *Prefetch* attribute 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 in order to keep it from expiring.

Setting Cache TTLs

TTL is the amount of time that any nameserver 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 the maximum time Cisco Prime IP Express retains the cached information. These parameters limit the lifetime of records in the cache whose TTL values are very large.

Local Basic or Advanced Web UI

Step 1 On the Edit Local CDNS Server tab, 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 2 Click **Save** to save the changes.

CLI Commands

Use:

- **CDNS set cache-max-ttl** to set the Maximum Cache TTL.
- **CDNS set cache-min-ttl** to set the Minimum Cache TTL.

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 IP Express 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 IP Express 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 time to live (TTL) on the official root server records is preconfigured and you can specify a different cache TTL value, (see Setting Cache TTLs, on page 4).

Because 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 Basic or Advanced Web UI

On the Edit Local CDNS Server tab, under the Root Name Servers category, 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**.

Dynamic Allocation of UDP Ports

The Caching DNS server uses a large number of UDP port numbers, by default approximately 60000 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 IP Express 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.

Cisco Prime IP Express uses *outgoing-range-avoid* attribute that allows you to define ports or ranges of ports that will be excluded from use by the DNS server when sending queries.

Note You need to ensure that UDP ports needed by other applications are in the port exclusion list. Otherwise, these applications may not be able bind to their port(s) if the DNS server is using the port.

Local Basic or Advanced Web UI

On the Edit Local CDNS Server tab, expand Additional Attributes to view various attributes and their values. For the query-source-port-exclusion-list attribute value, enter a range of ports that need to be excluded. Then click Modify Server.

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, in the Caching category, set it to the desired value for the RRSet Cache Size (*rrset-cache-size*), then click Save. The default size is 200MB.

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 200MB.

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 *harden-glue* 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.

Specifying Network Settings

The *listen-ip-version* attribute lets you to choose the ip packets to accept and issue. You can check IPv4, IPv6, both, or none. The *listen-protocol* attribute lets you to choose the packet protocol to answer and issue, UDP, TCP, both, or none.

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 lets you to set the time to live for entries in the host entries in the remote name server cache. They contains roundtrip timing and EDNS support information.

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 records for a nameserver. To compensate for most DNS clients starting with, and limiting their use to, the first record in the list, you can enable round-robin to share the load. This method

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 Manage DNS Caching Server page, under the Advanced Settings section, find the Enable round-robin (*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 CDNS Cache

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

Local Basic or Advanced 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** link 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.
- The 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

To:

- Remove all cached entries at or below a given domain, use **cdns flushCache** *domain*. If no domain is given, it flushes all RRs in the cache.

- Flush RRs from the cache associated with the given RR name, use **cdns flushName** *name type*. When type is provided, it flushes all entries with the given name and type. If no type if provided, it flushes types A, AAAA, NS, SOA, CNAME, DNAME, MX, PTR, SRV, TXT, and NAPTR.

Detecting and Preventing DNS Cache Poisoning

Cisco Prime IP Express enhances the CDNS 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 about 60000 port numbers.

The **Expert** mode Caching DNS server setting *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 DNS server statistics appears on the Statistics tab of the Manage DNS Caching Server Statistics page. The Statistics displays the answers-unwanted values. You can refresh the DNS Caching Server Statistics.

Handling Unresponsive Nameservers

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

Using Cisco Prime IP Express, 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 IP Express receives a list of remote nameservers to transmit a DNS query request to, it checks for the name-servers 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 the *acl-blacklist*.

Note Using the *acl-do-not-query* does not affect the configuration of communication with certain servers such as forwarders.

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-blacklist* do not get any response whatsoever.

Local Advanced Web UI

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

Running DNS Caching Server Commands

Access the commands by 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 CDNS Cache, on page 7

- **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 CDNS 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.