Advanced Caching DNS Server

This chapter explains how to set the Caching DNS parameters for the advanced features of the server. Before you proceed with the tasks in this chapter, see Introduction to the Domain Name System, which explains the basics of DNS.

- Using Forwarders, on page 1
- Using Exceptions, on page 3
- Managing DNS64, on page 5
- Managing DNSSEC, on page 6
- Managing Caching Rate Limiting, on page 7
- Managing DNS Views, on page 10
- Setting up Caching DNS and Authoritative DNS Servers on the Same Operating System, on page 11
- Managing DNS Firewall, on page 11
- Configuring Caching DNS to Use Umbrella, on page 11

Using Forwarders

You can specify a domain for which forwarding should occur. The forwarder definition is a list of IP addresses with an optional port number or a list of names of servers, or both. Typically forwarders are other DNS Caching servers that have access to Internet or external DNS resources.

Note We highly recommend using IP address rather than hostnames.

When forwarders are used, the Caching DNS server forwards user queries matching the forwarding domain to another Caching DNS server to perform the resolution. This can be useful in situations where the local Caching DNS server does not have Internet access (that is, inside a firewall). In these situations, it is typical for exceptions to be configured for local zones and then a root (.) forwarder to be created for all external queries. Forwarder name corresponds to the domains you would like to have forwarded. For example, to forward example.com queries, your forwarder will be named example.com.

Note You can specify IPv4 and/or IPv6 addresses and for the changes to take effect, you must reload the Caching DNS server.

Tip To force the Caching DNS server to forward all queries to one or more DNS forwarders, use the DNS root (.) as the forwarder name.

Note Caching DNS by default does not allow access to AS112 and RFC 1918 reverse zones. These are the reverse zones for IP address ranges that are reserved for local use only. To access these zones, define an exception or forwarder for the reverse zones that are defined locally.

In Cisco Prime Network Registrar, you can enable TLS at the individual forwarder object level. To do this, enable the *tls* attribute by selecting the **enabled** option. If you enable this, you should configure a *tls-cert-bundle* to load the CA certificates, otherwise, the connections cannot be authenticated. To add public key to the Certificate Authority bundle, copy the public.pem of forwarder server to the Caching DNS server, and update the same in *tls-upstream-cert-bundle* using the following commands:

```
scp -r public.pem @client-ip:/etc/pki/ca-trust/source/anchors/

# update-ca-trust
```

The *tls-auth-name* indicates the auth name for the forwarder server. If TLS is enabled, the Caching DNS server checks the TLS authentication certificates with that name sent by the forwarder server.

Starting with Cisco Prime Network Registrar 11.1, you can enable/disable forwarder as a Cisco Umbrella CDNS forwarder using the *cisco-umbrella* attribute. This allows Caching DNS to capture and log security events detected by upstream Cisco Umbrella servers.

Local and Regional Web UI

To define a forwarder:

Step 1 From the **Design** menu, choose **Forwarders** under the **Cache DNS** submenu. This opens the List/Add Forwarders page.

Step 2 Click the **Add Forwarders** icon on the **Forwarders** pane to open the Add Forwarder dialog box.

Step 3 Enter the name of the zone to be forwarded as the name and click **Add Forwarder**.

Note To use a forwarder for all external queries, create a forwarder with the name ".".

Step 4 In the Edit Forwarders page, enter the hostname, and click **Add Host** or enter the IP address for the forwarder, and then click **Add Address**.

Step 5 Click **Save**.

CLI Commands

- To specify the address (or space-separated addresses) of nameservers to use as forwarders, use **cdns addForwarder** *domain* [**tls**=**on** | **off**] [**tls-auth-name**=*name*] *addr*.

  If the **tls** flag is on, the server connects to the name server using TLS. If **tls-auth-name** is provided, the server verifies this name in the TLS certificate provided by the name server.

You can also use **cdns-forwarder** *name* **create** *attribute=value* to create the Caching DNS forwarder objects.

- To list the current forwarders, use **cdns listForwarders** or **cdns-forwarder list**.
- To modify the forwarder objects, use **cdns-forwarder** *name* **set** *attribute=value*.
- To remove a forwarder or list of forwarders, use **cdns removeForwarder** *domain* [*addr ...*] or **cdns-forwarder** *name* **delete**.

Note For any TLS related changes in the forwarders to take effect, you should restart the Caching DNS server.

Using Exceptions

If you do not want the Caching DNS server to use the standard resolution method to query the nameserver for certain domains, use exceptions. This bypasses the root nameservers and targets a specific server (or list of servers) to handle name resolution. Typically exceptions are used to access local DNS authoritative resources (that is, a company's internal zones).

Let us say that example.com has two subsidiaries: Red and Blue. Each has its own domain under the .com domain. When users at Red want to access resources at Blue, their Caching DNS server follows delegations starting at the root nameservers.

These queries cause unnecessary traffic, and in some cases fail because internal resources are often barred from external queries or sites that use unreachable private networks without unique addresses.

Exceptions solve this problem. The Red administrator can list all the other example.com domains that users might want to reach and at least one corresponding nameserver. When a Red user wants to reach a Blue server, the Red server queries the Blue server instead following delegations from the root servers down.

To enable resolution exceptions, simply create an exception for the domain listing the IP address(es) and/or hostname(s) of the authoritative nameserver(s).

Note Exceptions can contain both IPv4 and/or IPv6 addresses, and require a Caching DNS server reload to take effect.

Warning If the Authoritative DNS server is using a non-standard DNS port (a port other than 53) and if the exception zone has subzones, then the user must configure separate exceptions for each subzone that refers to the non-standard port. Otherwise, the Caching DNS server defaults to using port 53 for the subzones, leading to resolution failures.

In Cisco Prime Network Registrar, you can enable TLS at the individual exception object level. To do this, enable the *tls* attribute by selecting the **enabled** option. If you enable this, you should configure a *tls-cert-bundle* to load the CA certificates, otherwise, the connections cannot be authenticated. To add public key to the Certificate Authority bundle, copy the public.pem of exception server to the Caching DNS server, and update the same in *tls-upstream-cert-bundle* using the following commands:

```
scp -r public.pem @client-ip:/etc/pki/ca-trust/source/anchors/

# update-ca-trust
```

The *tls-auth-name* attribute indicates the auth name for the exception server. If TLS is enabled, the Caching DNS server checks the TLS authentication certificates with that name sent by the exception server.

Local and Regional Web UI

Step 1 From the **Design** menu, choose **Exceptions** under the **Cache DNS** submenu. This opens the List/Add Exceptions page.

Step 2 Click the **Add Exceptions** icon in the **Exceptions** pane to open the Add Exception dialog box.

Step 3 In the Name field, enter the domain or zone for which an exception is wanted and click **Add Exception**.

Step 4 In the Edit Exceptions page, enter the hostname in the DNS Name field and click **Add Host**. To address, enter the IP address in the IP Address field and click **Add Address**.

Step 5 If the *prime* attribute is on, Caching DNS server queries the zone for the currently published name servers and use those. This is similar to how the server treats root hints.

Step 6 Click **Save**.

To delete an exception list, select the exception in the Exceptions pane and click the **Delete** icon. To add or remove name servers to an exception, click the name of the exception in the List/Add Exceptions page to open the Edit Exceptions page.

CLI Commands

Use the exception commands only if you do not want your Caching DNS server to use the standard name resolution for querying root name servers for names outside the domain. Cisco Prime Network Registrar sends non-recursive queries to these servers.

- To add the resolution exception domains and IP addresses of servers, separated by spaces, use **cdns addException** *domain* [**prime=on** | **off**] [**tls=on** | **off**] [**tls-auth-name**=*name*] [**views=on** | **off**] [*addr ...*]. The addresses can be IPv4 or IPv6 with an optional port number (that is, *addr*[*@port*]) or the name of a server (it must be possible to resolve the server name before it is used). Use this command only if you do not want your Caching DNS server to use the standard name resolution for a zone.

  If the **tls** flag is on, the server connects to the name server using TLS. If **tls-auth-name** is provided, the server verifies this name in the TLS certificate provided by the name server.

  You can also use **cdns-exception** *name* **create** *attribute=value* to create the Caching DNS exception objects.

- To list the domains that are configured to have exceptional resolution of their names, use **cdns listExceptions** or **cdns-exception list**.

- To remove an entry for exceptional resolution of addresses within a domain, use **cdns removeException** *domain* [*addr ...*] or **cdns-exception** *name* **delete**. You can remove an individual server by specifying it, or the exception itself by just specifying its name.

- To modify the exception objects, use **cdns-exception** *name* **set** *attribute=value*.

Note For any TLS related changes in the exceptions to take effect, you should restart the Caching DNS server.

Managing DNS64

DNS64 with NAT64 provides access to the IPv4 Internet and servers for hosts that have only IPv6 addresses. DNS64 synthesizes AAAA records from A records, when an IPv6 client queries for AAAA records, but none are found. It also handles reverse queries for the NAT64 prefix(es).

In Cisco Prime Network Registrar, you can define multiple prefixes for synthesizing AAAA record.

Note

- When you enable DNS64 on multiple Caching DNS servers, you must ensure that the same version of Cisco Prime Network Registrar is installed on all the Caching DNS servers.
- If DNS firewall redirect is also enabled, the Caching DNS redirect takes precedence over DNS64 functionality.
- If DNS64 is enabled, enabling DNSSEC is not recommended. DNS64 causes responses to be simulated which may cause DNSSEC validation to fail.
- For DNS64 to be useful, there must be a corresponding NAT64 service on the network.

Local Advanced and Regional Advanced Web UI

To add, edit, or view the DNS64 configuration items:

Step 1 From the **Design** menu, choose **DNS64** under the **Cache DNS** submenu to open the List/Add DNS64 page.

Step 2 Click the **Add DNS64** icon in the DNS64 pane to open the Add DNS64 dialog box.

Step 3 Enter the name for the DNS64 configuration item in the Name field.

Step 4 Click **Add Dns64** to add the configuration item. The Edit DNS64 page appears with the list of attributes that can be edited.

Step 5 Edit the values of the attributes, as required. The value defined for *Priority* decides the search order for the client's DNS64 configuration.

Step 6 Click **Save** to save your settings for the selected DNS64 configuration item.

To delete a DNS64 configuration item, select the DNS64 entry on the DNS64 pane, click the **Delete DNS64** icon, and then confirm the deletion.

CLI Commands

To create DNS64 in the Caching DNS server, use the **cdns64** *name* **create** [**acl-match-clients**=*ACL* **prefix**=*IPv6 prefix*] command (see the **cdns64** command in the CLIGuide.html file in the /docs directory for syntax and attribute descriptions or use **help cdns64** in the CLI). For Example:

```
nrcmd> cdns64 dns64 create
```

```
nrcmd> cdns64 dns64 set acl-match-clients=baaa::56ff:febd:3d6
```

When connected to a regional cluster, you can use the following pull, push, and reclaim commands. For push and reclaim, a list of clusters or "all" may be specified.

- **cdns64** <*name* | **all** > **pull** < **ensure** | **replace** | **exact** > *cluster-name* [**-report-only** | **-report**]
- **cdns64** <*name* | **all** > **push** < **ensure** | **replace** | **exact** > *cluster-list* [**-report-only** | **-report**]
- **cdns64** *name* **reclaim** *cluster-list* [**-report-only** | **-report**]

Managing DNSSEC

DNS Security Extensions (DNSSEC) enables the server to determine the security status of all Resource Records that are retrieved. You can manage DNSSEC in the Advanced and Expert modes. The *dnssec* attribute enables validation of DNS information. The *domain-insecure* attribute defines domain names to be insecure, DNSSEC chain of trust is ignored towards the domain names. So, a trust anchor above the domain name can not make the domain secure with a DS record, such a DS record is then ignored. DNSSEC requires a root trust anchor to establish trust for the DNS root servers. The initial DNSSEC root trust anchor, root.anchor, is stored in the .../data/cdns directory and is the default value of the *auto-trust-anchor-file* attribute. Additional trust anchors may be added by adding them to the .../data/cdns directory and to the *auto-trust-anchor-file* if the zone supports automated updates according to RFC 5011 or the *trust-anchor-file* attribute if not. The **cdnssec** command controls and configures DNSSEC processing in the Cisco Prime Network Registrar Caching DNS server.

To set the size of the aggressive negative cache in bytes, use the *neg-cache-size* attribute on the Manage DNS Caching Server page.

The *key-cache-size* attribute sets the size of the key cache in bytes. The *prefetch-key* attribute sets whether the Caching DNS server should fetch the DNSKEYs earlier in the validation process, when a DS record is encountered.

Note If DNS64 is enabled, enabling DNSSEC is not recommended. DNS64 causes responses to be simulated which may cause DNSSEC validation to fail.

Local Advanced Web UI

Step 1 From the **Design** menu, choose **Caching DNSSEC** under the **Security** submenu to open the Manage Caching DNSSEC page.

Step 2 Enable DNSSEC validation by selecting the **enabled** option for the Enable DNSSEC validation (*dnssec*) attribute.

Step 3 The page displays all the Caching DNSSEC attributes. Modify the attributes as per your requirements.

Step 4 Click **Save** to save your settings.

CLI Commands

- To create DNSSEC in the Caching DNS server, use **cdnssec create** *attribute=value*. To enable DNSSEC, use **cdnssec enable dnssec** (see the **cdnssec** command in the CLIGuide.html file in the /docs directory for syntax and attribute descriptions or use **help cdnssec** in the CLI).
- Use **cdns set neg-cache-size** to set Negative Cache Size.

Managing Caching Rate Limiting

Rate limiting helps the DNS server from being overwhelmed by a small number of clients. It also protects against upstream query attacks against Authoritative DNS servers. The rate limiting feature helps to mitigate some of the DDoS attacks and prevents the server from being overwhelmed by a small number of clients. This feature allows you to limit the malevolent traffic.

You can manage rate limiting in Advanced mode in the local web UI. Rate limiting is divided into two separate categories, Client Rate Limiting and Domain Rate Limiting, which are managed separately.

Client Rate Limiting

Client Rate Limiting imposes limits on the QPS per client and when the limit is reached, new queries are dropped. When a client is rate limited, it is possible to still allow some queries through.

The *client-rate-limiting* attribute on the Rate Limiting Settings tab enables IP based client rate limiting. It is not enabled by default. The *client-rate-limit-qps* attribute specifies the maximum QPS for an incoming client IP before starting the rate limiting. Default value is 1000. The *client-rate-limiting-factor* specifies that one out of this many number of queries will be allowed through when a client IP is being rate limited. For information about all the Client Rate Limiting attributes, see Table 1: Client Rate Limiting Attributes below.

The Client Rate Limiting tab on the Manage Caching Rate Limiting page displays information about the current clients being rate limited and the limits they are hitting. The table on the page shows:

- **Client**—Rate limited client IP addresses.
- **Number of times rate limited**—Total number of times a client was rate limited.

Table 1: Client Rate Limiting Attributes

Attribute	Description
Client Rate Limiting (*client-rate-limiting*)	Enables IP based client rate limiting.
Client Rate Limiting QPS (*client-rate-limiting-qps*)	Specifies the rate limit for incoming DNS clients.
Client Rate Limiting Factor (*client-rate-limiting-factor*)	When *client-rate-limiting* is enabled and a client is being rate limited, specifies that one out of this number of queries from that client will be allowed to complete.

Attribute	Description
Client Report Max (*client-report-max-count*)	Specifies the maximum number of entries in the list of rate limited clients. This limit is applied to the lists of clients that are logged, returned as part of activity summary or included in statistics.

Domain Rate Limiting

Domain Rate Limiting imposes limits on the QPS the server may send to authoritative name server for a DNS zone. When a domain is rate limited, it is possible to still allow some queries through.

The *domain-rate-limiting* attribute on the Rate Limiting Settings tab enables domain based (name server zones) rate limiting. It is not enabled by default. The *domain-rate-limit-qps* specifies the maximum QPS for a domain/zone before starting the rate limiting. The default value is 1000. The *domain-rate-limiting-factor* specifies that one out of this many number of queries to the specified zone will be allowed through, when the zone is being rate limited. For information about all the Domain Rate Limiting attributes, see Table 2: Domain Rate Limiting Attributes below.

The Domain Rate Limiting tab on the Manage Caching Rate Limiting page displays information about the current domains being rate limited and the limits they are hitting. The table on the page shows:

- **Domain**—Rate limited domains.
- **Rate Limit Max QPS**—Maximum number of entries in the list of rate limited domains.
- **Number of times rate limited**—Total number of times a domain was rate limited.

Table 2: Domain Rate Limiting Attributes

Attribute	Description
Domain Rate Limiting (*domain-rate-limiting*)	Enables rate limiting for name server zones.
Domain Rate Limiting QPS (*domain-rate-limiting-qps*)	Specifies the rate limit for name server zones.
Domain Rate Limiting Factor (*domain-rate-limiting-factor*)	When *domain-rate-limiting* is enabled and a zone is being rate limited, specifies that one out of this number of queries to the specified zone will be allowed to complete.
Per Domain Limit	Specifies a list of domains that use a rate limit other than *domain-rate-limiting-qps*. The list entries have the following attributes: • domain—The name of the zone delegation point to which this entry applies. • applies-to—Specifies if this entry applies to only the zone designated by 'domain', only zones specified by subdomains of 'domain', or both. • rate-limit—The rate limit that applies to zones covered by this entry.

Attribute	Description
Domain Report Max (*domain-report-max-count*)	Specifies the maximum number of entries in the list of rate limited domains. This limit is applied to the lists of domains that are logged, returned as part of activity summary or included in statistics.

Managing Rate Limiting

You can manage both Client Rate Limiting and Domain Rate Limiting from the Manage Caching Rate Limiting page in the local web UI. This page contains the following three tabs:

- **Rate Limiting Settings**—Displays all the Rate Limiting attributes under their respective categories.
- **Domain Rate Limiting**—Displays a list of domains that are rate limited. This tab also contains information such as Rate Limit Max QPS and number of times a domain was rate limited.
- **Client Rate Limiting**—Displays a list of clients that are rate limited. This tab also contains information about the number of times a client was rate limited.

Note The length of the list is controlled by Client Report Max and Domain Report Max attributes.

Local Advanced Web UI

Step 1 From the **Design** menu, choose **Rate Limiting** under the **Cache DNS** submenu to open the Manage Caching Rate Limiting page.

Step 2 Modify the attributes in the **Client Rate Limiting** and **Domain Rate Limiting** categories as per your requirements:

- To enable Client Rate Limiting, find the *client-rate-limiting* attribute under the **Client Rate Limiting** section, and enable it by selecting the **on** option.
- To enable Domain Rate Limiting, find the *domain-rate-limiting* attribute under the **Domain Rate Limiting** section, and enable it by selecting the **on** option.

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

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

Per Domain Limit

You can specify a list of domains to be rate limited with their associated rate limit values. This applies to a domain, its subdomains, or both. These domains use a rate limit other than *domain-rate-limiting-qps*. You can specify a list by adding domains using the **Add** button under the **Per Domain Limit** section.

Note When specifying Per Domain Limit, it is important that the domain names match a DNS zone.

Local Advanced Web UI

On the Rate Limiting Settings tab, under the **Domain Rate Limiting** section, click the **Add** button next to **Per Domain Limit**. In the Add Domain dialog box, enter the domain name (the name of the zone), rate limit value, and specify whether it applies to a domain, its subdomains, or both. Then, click the **Add** button. Click **Save** on the Rate Limiting Settings tab to save the changes.

CLI Commands

- Use **cdns-rate-limit enable client-rate-limiting** to enable the client rate limiting feature.
- Use **cdns-rate-limit set client-rate-limiting-qps**=*value* to set the QPS value for the client rate limiting. For example:

```
nrcmd> cdns-rate-limit set client-rate-limiting-qps=1000
```

- Use **cdns-rate-limit set domain-rate-limiting-qps**=*value* to set the QPS value for the domain rate limiting. For example:

```
nrcmd> cdns-rate-limit set domain-rate-limiting-qps=500
```

- Use **cdns-rate-limit add** [**domain**=]<*domain*> [[**applies-to**=]*domain* | *subdomain* | **both**] [[**rate-limit**=]*rate-limit*] to specify Rate Limit for the *domain-rate-limiting-list* attribute. For example:

```
nrcmd> cdns-rate-limit add example.com both 1000
```

- Use **cdns-rate-limit list** to display the list of domains that use a rate limit other than *domain-rate-limiting-qps*.
- Use **cdns getStats rate-limit** to get rate limiting statistics.

Managing DNS Views

The Cisco Prime Network Registrar Caching DNS server can associate the client requests to the appropriate views on behalf of the Authoritative DNS server. This is done by configuring the DNS Views on the Caching DNS server and setting the *uses-views* attribute on the List/Add Exceptions page to **true**. The Caching DNS server maps the client to the appropriate view and tags the queries forwarded to the Authoritative DNS server with the appropriate view. Therefore, in these cases, the view mapping is done by the Caching DNS server.

Note The Caching DNS server only maps clients to *acl-match-clients*. The *acl-match-destinations* attribute is ignored.

DNS Views and Exception settings are automatically synced/set by zone distribution.

For more information on DNS Views, see Managing DNS Views.

Setting up Caching DNS and Authoritative DNS Servers on the Same Operating System

In Cisco Prime Network Registrar 10.0 and later, both the Caching DNS and Authoritative DNS servers can run on the same operating system, without the need for two separate virtual or physical machines. For more information on DNS firewall, see Managing DNS Firewall.

Managing DNS Firewall

Cisco Prime Network Registrar DNS Firewall provides a mechanism to control the domain names, IP addresses, and name servers that are allowed to function on the network. For more information on DNS firewall, see Managing DNS Firewall.

Configuring Caching DNS to Use Umbrella

Cisco Umbrella provides the first line of defense against threats on the Internet. To switch to Umbrella from Cisco Prime Network Registrar Caching DNS server, you need to create a forwarder for the "." domain using the following CLI commands:

```
nrcmd> cdns-forwarder . create addr=208.67.222.222,208.67.220.220
nrcmd> cdns reload
```

Once configured, the Cisco Prime Network Registrar Caching DNS server will forward all resolution queries to Cisco Umbrella (the server will still respond with locally cached answers). It can be used in conjunction with DNS firewall for queries not explicitly blocked by the firewall.

Starting with Cisco Prime Network Registrar 11.1, you can enable/disable forwarder as a Cisco Umbrella CDNS forwarder using the *cisco-umbrella* attribute. You can also use the following CLI command:

```
nrcmd> cdns-forwarder . enable cisco-umbrella
```

Umbrella security events are logged when **cisco-umbrella** is selected for *security-event-log-settings* in the Security Events section.

Note Exceptions will operate as usual. Local resolution through exceptions will bypass the Umbrella servers.

Note Cisco Umbrella addresses are:

- IPv4 addresses: 208.67.222.222 and 208.67.220.220
- IPv6 addresses: 2620:119:35::35 and 2620:119:53::53

For more information, go to umbrella.cisco.com.