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.

Defining Forwarders

You can specify a domain for which forwarding should occur. The forwarder definition is by a list of names of servers or a list of IP addresses with an optional port number, or both.

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

Tip To force a caching DNS server to only talk to a forwarder, define a forwarder for the DNS root (.).

Note CDNS by default does not allow access to AS112 and RFC1918 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.

Local Basic or Advanced 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 in the**Forwarders** pane to open the Add DnsForwarder dialog box.

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

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 then click **Add Address**.

Step 5 Click **Save**.

CLI Commands

Use the following cdns commands to:

- Specify the address (or space-separated addresses) of nameservers to use as forwarders, use **cdns addForwarder**.
- List the current forwarders, use **cdns listForwarders**.
- Edit your forwarder list, you must remove any offending forwarder and reenter it.
- Remove a forwarder or list of forwarders, use **cdns removeForwarder**.

Note For any change to the forwarders to take effect, you should restart the CDNS server.

Using Exceptions

If you do not want the CDNS 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.

Let us say that example.com has four subsidiaries: Red, Blue, Yellow, and Green. Each has its own domain under the .com domain. When users at Red want to access resources at Blue, their CDNS 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 CDNS server reload to take effect.

Local Basic or Advanced 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 DnsException dialog box.

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

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, CDNS 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.**

Deleting Exception List

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 DNS Caching server to use the standard name resolution for querying root name servers for names outside the domain. IP Express sends non-recursive queries to these servers.

Use the following cdns commands to:

- Add the resolution exception domains and the IP addresses of servers, separated by spaces, use **cdns addException domain [prime=on|off] [views=on|off] addr**. The addresses can be IPv4 or IPv6 with an optional port number (i.e. <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 DNS Caching server to use the standard name resolution for a zone.
- List the domains that are configured to have exceptional resolution of their names, use **cdns listExceptions.**
- Remove an entry for exceptional resolution of addresses within a domain, use **cdns removeException**. You can remove an individual server by specifying it, or the exception itself by just specifying its name.
- Replace an exception, you must first remove the current exception and then add a new one.

For any change to resolution exceptions to take effect, you must restart the CDNS 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 a IPv6 client queries for AAAA records, but none are found. It also handles reverse queries for the NAT64 prefix(es).

In Cisco Prime IP Express 8.3 and later, 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 IP Express is installed on all the Caching DNS servers.
- If DNS firewall redirect is also enabled, the Caching DNS redirect takes precedence over DNS64 functionality.

Local 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. This opens 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.

Step 4 Click **Add DNS64** to save the configuration item. The Edit DNS64 *name* 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 **cdns64 <name>create *[acl-match-clients=<ACL> prefix=<IPv6 prefix>]***. (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
```

Managing DNSSEC

DNSSEC enables the server to determine the security status of all Resource Records that are retrieved. You can manage DNSSEC only in the Advanced mode. 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 IP Express DNS Caching 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 DNS caching server should fetch the DNSKEYs earlier in the validation process, when a DS record is encountered.

Local Basic or Advanced Web UI

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

Step 2 Enable DNSSEC validation by selecting the enabled option.

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

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

CLI Commands

- To create DNSSEC in the DNS Caching server, use **cdnssec create**. To enable cdnssec, 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 dnssec** in the CLI).
- Use **cdns set neg-cache-size** to set Negative Cache Size.

Setting up Caching DNS and Authoritative DNS Server on Same Operating System

In Cisco Prime IP Express 9.0 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 Running Caching DNS and Authoritative DNS on the Same Server.

Managing DNS Firewall

DNS Firewall provide a mechanism 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.