Managing Authoritative DNS Server

This chapter explains how to set the Authoritative DNS server parameters. Before you proceed with the tasks in this chapter, read Managing Zones which explains how to set up the basic properties of a primary and secondary zone.

- Running DNS Authoritative Server Commands, page 1
- Setting General DNS Server Properties, page 3
- Setting Advanced Authoritative DNS Server Properties, page 6
- Setting up Caching DNS and Authoritative DNS Server on Same Operating System, page 9
- Managing DNS Firewall, page 11
- Troubleshooting DNS Servers, page 16

Running DNS Authoritative Server Commands

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

- **Force all zone transfers—**A secondary server periodically contacts its master server for changes. See Enabling Zone Transfers.
- **Scavenge all zones—**Cisco Prime IP Express provides a feature to periodically purge stale records. See the *"Scavenging Dynamic Records" section in Cisco Prime IP Express 8.3 DHCP User Guide*.
- **Synchronize All HA Zones—**Synchronizes all the HA zones. You have the option to choose the type of synchronization. The **Use Server Algorithms** option is checked by default. You can override this by checking either **Push All Zones From Main to Backup** check box or **Pull All Zones From Backup to Main** check box.

Note The **Synchronize All HA Zones** command is an **Expert** mode command which you can see only if the server is an HA main server. You cannot see this command if it is an HA backup server. You can also, synchronize zones separately, which you can do from the Zone Commands for Zone page (see Synchronizing HA DNS Zones).

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 DNS Server Network Interfaces

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

Local Advanced Web UI

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

Step 2 Click **Local DNS Server** on the Manage Servers pane to open the Local DNS Server page.

Step 3 Click the **Network Interfaces** tab for the DNS server 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 Clicking the name of the configured interface opens a new page, where you can change the address 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 Manage Servers page.

Note The IPv6 functionality in DNS requires IPv4 interfaces to be configured except if the DNS server is isolated and standalone (it is its own root and is authoritative for all queries).

Setting DNS Server Properties

You can set properties for the DNS server, along with those you already set for its zones. These include:

- **General server properties—**See Setting General DNS Server Properties, on page 3
- **Delegation-only zones—**See Specifying Delegation-Only Zones, on page 3
- **Round-robin server processing—**See Enabling Round-Robin, on page 3
- **Subnet sorting—**See Enabling Subnet Sorting, on page 4
- **Enabling incremental zone transfers—**See Enabling Incremental Zone Transfers (IXFR) , on page 4

- **Enabling NOTIFY packets—**See Enabling NOTIFY, on page 5

Note To enable GSS-TSIG support, you must set TSIG-Processing to none, and GSS-TSIG processing to 'ddns, query' to support both ddns and query.

Setting General DNS Server Properties

You can display DNS general server properties, such as the name of the server cluster or host machine and the version number of the Cisco Prime IP Express DNS server software. You can change the internal name of the DNS server by deleting the current name and entering a new one. This name is used for notation and does not reflect the official name of the server. Cisco Prime IP Express uses the server IP address for official name lookups and for DNS updates (see the *"Managing DNS Update" chapter in Cisco Prime IP Express 8.3 DHCP User Guide*).

The following subsections describe some of the more common property settings. They are listed in Setting DNS Server Properties, on page 2.

Local Basic or Advanced Web UI

Step 1 To access the server properties, choose **DNS Server** from the **Deploy** menu to open the Manage DNS Authoritative Server page. The page displays all the DNS server attributes.

Step 2 Modify the attributes as per your requirements.

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

CLI Commands

Use **dns** [**show**] to display the DNS server properties.

Specifying Delegation-Only Zones

You can instruct the server to expect only referrals when querying the specified zone. In other words, you want the zone to contain only NS records, such as for subzone delegation, along with the apex SOA record of the zone. This can filter out “wildcard” or “synthesized” data from authoritative nameservers whose undelegated (in-zone) data is of no interest. Enable the DNS server *delegation-only-domains* attribute for this purpose.

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.

Tip Adjust the switchover rate from one round-robin server to another using the TTL property of the server A record.

Local Basic or Advanced Web UI

On the Manage DNS Authoritative Server page, under the Miscellaneous Options and Settings section, find the Enable round-robin (*round-robin)* attribute. It is set to enabled by default in Basic mode.

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**.

Enabling Subnet Sorting

If you enable subnet sorting, as implemented in BIND 4.9.7, the Cisco Prime IP Express DNS server confirms the client network address before responding to a query. If the client, server, and target of the query are on the same subnet, and the target has multiple A records, the server tries to reorder the A records in the response by putting the closest address of the target first in the response packet. DNS servers always return all the addresses of a target, but most clients use the first address and ignore the others.

If the client, DNS server, and target of the query are on the same subnet, Cisco Prime IP Express first applies round-robin sorting and then applies subnet sorting. The result is that if you have a local response, it remains at the top of the list, and if you have multiple local A records, the server cycles through them.

Local Basic or Advanced Web UI

On the **Manage DNS Authoritative Server** page, in A-Z view, find the Enable subnet sorting (*subnet-sorting)* attribute, set it to enabled, then click **Save**.

CLI Commands

Use **dns enable subnet-sorting** or **dns disable subnet-sorting** (the preset value).

Enabling Incremental Zone Transfers (IXFR)

Incremental Zone Transfer (IXFR, described in RFC 1995) allows only changed data to transfer between servers, which is especially useful in dynamic environments. IXFR works together with NOTIFY (see Enabling NOTIFY, on page 5) to ensure more efficient zone updates. IXFR is enabled by default.

Primary zone servers always provide IXFR. You should explicitly enable IXFR on the server (you cannot set it for the primary zone) only if the server has secondary zones. The DNS server setting applies to the secondary zone if there is no specific secondary zone setting.

Local Basic or Advanced Web UI

On the Manage DNS Authoritative Server page, under the Zone Default Settings section, you can find the Request incremental transfers (IXFR) attribute. It is set it to enabled by default. For a secondary zone, you can also fine-tune the incremental zone transfers by setting the *ixfr-expire-interval* attribute.

This value is the longest interval the server uses to maintain a secondary zone solely from IXFRs before forcing a full zone transfer (AXFR). The preset value of one week is usually appropriate. Then, click **Save**.

CLI Commands

Use **dns enable ixfr-enable**. By default, the *ixfr-enable* attribute is enabled.

Restricting Zone Queries

You can restrict clients to query only certain zones based on an access control list (ACL). An ACL can contain source IP addresses, network addresses, TSIG keys (see the *"Transaction Security" section in Cisco Prime IP Express 8.3 DHCP User Guide*), or other ACLs. The *restrict-query-acl* on the DNS server serves as a default value for zones that do not have the *restrict-query-acl* specifically set.

Enabling NOTIFY

The NOTIFY protocol, described in RFC 1996, lets the Cisco Prime IP Express DNS primary server inform its secondaries that zone changes occurred. The NOTIFY packets also include the current SOA record for the zone giving the secondaries a hint as to whether or not changes have occurred. In this case, the serial number would be different. Use NOTIFY in environments where the namespace is relatively dynamic.

Because a zone master server cannot know specifically which secondary server transfers from it, Cisco Prime IP Express notifies all nameservers listed in the zone NS records. The only exception is the server named in the SOA primary master field. You can add additional servers to be notified by adding the IPv4 addresses to the notify-set on the zone configuration.

Note For NS records that point at names that the DNS server is not authoritative for, those IP addresses need to be explicitly set in the notify-set if the user wants those servers to get notifies.

You can use IXFR and NOTIFY together, but this is not necessary. You can disable NOTIFY for a quickly changing zone for which immediate updates on all secondaries does not warrant the constant NOTIFY traffic. Such a zone might benefit from having a short refresh time and a disabled NOTIFY.

Local Basic or Advanced Web UI

Step 1 On the **Manage DNS Authoritative Server** page, under the **Zone Transfer Settings** section, find the *notify* attribute (Expert mode only), then check the **Enabled** check box to enable it.

Step 2 Set any of the other NOTIFY attributes (*notify-defer-cnt* , *notify-min-inverval* , *notify-rcv-interval* , *notify-send-stagger* , *notify-source-address* , *notify-source-port* , and *notify-wait*).

Step 3 Click **Save**.

Step 4 To add nameservers in addition to those specified in NS records, from the **Design** menu, choose **Forward Zones** under the **Auth DNS** submenu.

Step 5 Click the zone in the Forward Zones pane to open the Edit Zone page.

Step 6 Add a comma-separated list of IP addresses of the servers using the *notify-set* attribute on the Edit Zone page.

Step 7 Set the *notify* attribute to true.

Step 8 Click **Save** on that page.

CLI Commands

Use **dns enable notify**. NOTIFY is enabled by default. You can also enable NOTIFY at the zone level, where you can use **zone** *name* **set notify-set** to specify an additional comma-separated list of servers to notify beyond those specified in NS records.

Setting Advanced Authoritative DNS Server Properties

You can set these advanced server properties:

- **SOA time-to-live—**See Setting SOA Time to Live, on page 6
- **Secondary server attributes—**See Setting Secondary Refresh Times, on page 7
- **Port numbers—**See Setting Local and External Port Numbers, on page 8
- **Handle Malicious DNS Clients—**See Handling Malicious DNS Clients, on page 8

Setting SOA Time to Live

The SOA record time to live (TTL) is usually determined by the zone default TTL. However, you can explicitly set the SOA TTL, which sets the maximum number of seconds a server can cache the SOA record data. For example, if the SOA TTL is set for 3600 seconds (one hour), an external server must remove the SOA record from its cache after an hour and then query your nameserver again.

Cisco Prime IP Express responds to authoritative queries with an explicit TTL value. If there is no explicit TTL value, it uses the default TTL for the zone, as set by the value of the *defttl* zone attribute.

Normally, Cisco Prime IP Express assumes the default TTL when responding with a zone transfer with RRs that do not have explicit TTL values. If the default TTL value for the zone is administratively altered, Cisco

Prime IP Express automatically forces a full zone transfer to any secondary DNS server requesting a zone transfer.

Local Basic or Advanced and Regional Web UI

Step 1 On the List/Add Zone page, set the Zone Default TTL, which defaults to 24 hours.

Step 2 If you want, set the SOA TTL, which is the TTL for the SOA records only. It defaults to the Zone Default TTL value.

Step 3 You can also set a TTL value specifically for the NS records of the zone. Set the NS TTL value under Nameservers. This value also defaults to the Zone Default TTL value.

Step 4 Click **Save**.

CLI Commands

Use **zone** *name* **set defttl**.

Setting Secondary Refresh Times

The secondary refresh time is how often a secondary server communicates with its primary about the potential need for a zone transfer. A good range is from an hour to a day, depending on how often you expect to change zone data.

If you use NOTIFY, you can set the refresh time to a larger value without causing long delays between transfers, because NOTIFY forces the secondary servers to notice when the primary data changes. For details about NOTIFY, see Enabling NOTIFY, on page 5.

Local Basic or Advanced and Regional Web UI

On the List/Add Zone page, set the Secondary Refresh field to the refresh time, which defaults to three hours. Make any other changes, then click **Save**

CLI Commands

Use **zone** *name* **set refresh**. The preset value is 10800 seconds (three hours).

Setting Secondary Retry Times

The DNS server uses the secondary retry time between successive failures of a zone transfer. If the refresh interval expires and an attempt to poll for a zone transfer fails, the server continues to retry until it succeeds. A good value is between one-third and one-tenth of the refresh time. The preset value is one hour.

Local Basic or Advanced and Regional Web UI

On the List/Add Zone page, set the Secondary Retry field to the retry time, which defaults to one hour. Make any other changes, then click **Save**.

CLI Commands

Use **zone** *name* **set retry**.

Setting Secondary Expiration Times

The secondary expiration time is the longest time a secondary server can claim authority for zone data when responding to queries after it cannot receive zone updates during a zone transfer. Set this to a large number that provides enough time to survive extended primary server failure. The preset value is seven days.

Local Basic or Advanced and Regional Web UI

On the List/Add Zone page, set the Secondary Expire field to the expiration time, which defaults to seven days. Make any other changes, then click **Save**.

CLI Commands

Use **zone** *name* **set expire**.

Setting Local and External Port Numbers

If you are experimenting with a new group of nameservers, you might want to use nonstandard ports for answering requests and asking for remote data. The local port and external port settings control the TCP and UDP ports on which the server listens for name resolution requests, and to which port it connects when making requests to other nameservers. The standard value for both is port 53. If you change these values during normal operation, the server will appear to be unavailable.

The full list of default ports is included in the *"Default Ports for Cisco Prime IP Express Services" section in Cisco Prime IP Express 8.3 Administrator Guide*.

Local Basic or Advanced Web UI

On the Manage DNS Authoritative Server page, in A-Z view, find the Listening Port (*local-port-num)* and Remote DNS servers port (*remote-port-num)* attributes, set them to the desired values (they are both preset to 53), then click **Save**.

Handling Malicious DNS Clients

When trying to resolve query requests, DNS servers may encounter malicious DNS clients. A client may flood the network with suspicious DNS requests. This affects the performance of the local DNS server and remote nameservers.

Using Cisco Prime IP Express, you can resolve this problem by barring malicious clients. You can configure a global ACL of malicious clients that are to be barred, using the blackhole-acl attribute.

Local Basic or Advanced Web UI

On the Manage DNS Authoritative Server page, expand Miscellaneous Options and Settings to view various attributes and their values. For the blackhole-acl attribute value, enter, for example, 10.77.240.73. Then click **Save**.

Tuning DNS Properties

Here are some tips to tune some of the DNS server properties:

- ***Notify send min. interval* DNS server attribute (*notify-min-interval* in the CLI)—**Minimum interval required before sending notification of consecutive changes on the same zone to a server. The preset value is two seconds. For very large zones, you might want to increase this value to exceed the maximum time to send an outbound full zone transfer. This is recommended for secondary servers that receive inbound incremental zone transfers and send out full transfers to other secondaries. These include older BIND servers that do not support incremental zone transfers. Inbound incremental transfers may abort outbound full transfers.
- ***Notify delay between servers* DNS server attribute (*notify-send-stagger* in the CLI)—**Interval to stagger notification of multiple servers of a change. The preset value is one second, but you may want to raise it to up to five seconds if you need to support a large number of zone transfers distributed to multiple servers.
- ***Notify wait for more changes* DNS server attribute (*notify-wait* in the CLI)—**Time to delay, after an initial zone change, before sending change notification to other nameservers. The preset value is five seconds, but you may want to raise it to 15, for the same reason as given for the *notify-min-interval* attribute.
- ***Max. memory cache size* DNS server attribute (*mem-cache-size* in the CLI)—**Size of the in-memory record cache, in kilobytes. The preset value is 50 MB and this is used to make queries for Authoritative DNS server faster. the rule of thumb is to make it as large as the number of authoritative RRs.
- **Maximum UDP payload size DNS server attribute (*max-udp-payload-size*)—**The maximum UDP payload size of the DNS server that responds to the client. You can modify this attribute from a minimum of 512 bytes to a maximum of 4 KB. The default value for this attribute is set to the maximum, that is, 4 KB on the DNS server.
- **IXFR check box in the Foreign Servers section of the Edit DNS Server page, or remote-dns *address/mask* create ixfr in the CLI—**Adding an entry for a server or group of servers allows controlling whether or not IXFR should occur when doing zone transfers from those servers.

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

When Cisco Prime IP Express is deployed in small-sized LANs, you can run both the Caching DNS and Authoritative DNS servers on the same operating system, without the need for two separate virtual or physical machines.

This configuration is feasible only for smaller networks where it may be difficult to add and maintain a standalone Caching DNS server. To enable this configuration, you must have:

- At least two interfaces-one each for the Caching DNS and the Authoritative DNS servers.
- Hybrid-mode configuration enabled on the Authoritative DNS server.

Note

- You must reload the Authoritative DNS server after you enable the hybrid-mode configuration.
- Cisco Prime IP Express provides separate licenses for CCM, Authoritative DNS, Caching DNS, DHCP, and IPAM services or for combinations of these services. For more details on the Licensing, see the *License Files* section in the Overview chapter of the *Cisco Prime IP Express Installation Guide*.

When the hybrid-mode configuration is enabled, the Caching DNS server detects the Authoritative DNS server on the same operating system and configures the in-memory exceptions for the Authoritative DNS server zones. Hybrid-mode configuration entails the following:

- The Caching DNS server does not maintain the cache for the Authoritative DNS zones regardless of the TTL. The Caching DNS server queries the Authoritative DNS server each time to assure that the cached information always matches the data on the Authoritative DNS server.
- The Authoritative DNS server overrides the exceptions that are on configured on the Caching DNS server for the Authoritative DNS zones.
- The Caching DNS server reloads whenever the Authoritative DNS server is reloaded.

Note When both the Caching DNS and the Authoritative DNS servers are run on a single operating system, the required memory needs to be doubled to support both servers. In addition, there should enough, dedicated, disk space for the Authoritative DNS zones, RRs, and the additional log files. For more information, see the Installation Requirements section in *Cisco Prime IP Express Installation Guide*.

Local Advanced Web UI

Step 1 To configure the network interfaces on the Authoritative and the Caching DNS servers, do the following:

Note You must have at least two interfaces-one each for the Caching DNS and the Authoritative DNS servers to enable the hybrid-mode configuration.

1. From the **Operate** menu, choose **Manage Servers** to open the Manage Servers page.
2. Click **Local DNS Server** in the Manage Servers pane.
3. Click the **Network Interfaces** tab and configure the available network interfaces for DNS.

   Note The loopback interface (127.0.0.1/8, ::1/128) should be configured on the Authoritative DNS server for the DNS hybrid mode.
4. Click **Local CDNS Server** in the Manage Servers pane.

5 Click the **Network Interfaces** tab and configure the available network interfaces for the Caching DNS server.

Step 2 To enable the hybrid-mode configuration on the Authoritative server, do the following:

1 From the **Deploy** menu, choose **DNS Server** to open the Manage DNS Authoritative Server page.

2 Click **Local DNS Server** in the DNS Server pane to open the Edit Local DNS Server page.

3 Set the *Hybrid Mode* attribute to **true**.

Step 3 Reload the Authoritative DNS server to enable the hybrid-mode configuration.

CLI Commands

Use **dns set *hybrid-mode=enabled*** to enable the hybrid-mode configuration on the Authoritative DNS server.

Managing DNS Firewall

DNS firewall controls the domain names, IP addresses, and name servers that are allowed to function on the network. This enables Internet Service Providers (ISP), enterprises, or organizations to define lists of FQDNs, IP addresses, subnets and prefixes of end nodes, and configure rules to secure the network by redirecting the resolution of DNS name away from known bad domains or non-existing domains (NXDOMAIN).

Every query to a Caching DNS server is first verified against the list of DNS firewall rules in the order of priority. To ensure that the caching DNS server redirects queries for non-existing or known bad domains, you can create DNS firewall rules. The DNS firewall rule comprises of a priority, an ACL, an action, and a list of domains and takes precedence over exceptions and forwarders. You can configure the following actions for these queries:

- **Drop** - Drops the resource record query.
- **Refuse** - Responds with no data and the REFUSED status.
- **Redirect** - Redirects A or AAAA queries to the specified IP address.
- **Redirect-nxdomain** - Redirect to a specific A or AAAA address if the queried domain does not exist.
- **RPZ** - Use Response Policy Zones (RPZ) rules.

When a resource record query matches the criteria of rule, the specified action is taken. If the resource record query action results for redirect-nxdomain, the query is performed in the normal process and if it results in an NXDOMAIN status, then it is redirected to the specified destination.

Note The firewall rules such as Drop, Refuse, Redirect, and the RPZ query-name trigger take place before regular query processing and therefore take precedence over forwarders and exceptions. The other actions and triggers are applied during or after regular query processing.

DNS Response Policy Zone (RPZ) Firewall Rules

The DNS firewall rules can be set up for specially designated zones on the Authoritative DNS server. The RPZ and RR data combined with DNS resolver effectively creates a DNS Firewall to prevent misuse of the DNS server. The RPZ firewall rule comprises of a trigger (query-name, ip-answers, ns-name, and ns-ip) and a corresponding action.

The RPZ firewall rules utilize both the Authoritative DNS and the Caching DNS servers to provide the RPZ functionality. The Authoritative DNS server stores the data for RPZ and the rules whereas the Caching DNS server takes the client queries and applies these rules.

DNS RPZ Zones

We recommend that you create a separate forward zone on the authoritative server for RPZ. The zone can be either primary or secondary and the data can either be manually entered or transferred from a third party RPZ provider. The zones can be named as **rpz.<customer-domain>** to avoid conflict with domain names in the Global DNS space. In Query Settings, enable the RPZ to make this domain as RPZ domain.

Note If the RPZ comes via zone transfer it must be named the same as at the source. If using a commercial RPZ provider, the name is specified by the provider.

The RPZ RR names can take the following forms:

Table 1: RPZ Triggers

RPZ Trigger	RR Name	Example	Example RR Name
Domain being queried	<domain>.rpz.<customer-domain>	Domain www.baddomain.com	www.baddomain.com.rpz.cisco.com
Name Server to query	<ns-domain-name>.rpz-nsdname.rpz.<customer-domain>	Name Server ns.baddomain.com	ns.baddomain.com.rpz-nsdname.rpz.cisco.com
Name Server IP to query	32.<reversed-ip>.rpz-nsip.rpz.<customer-domain>	Name Server Address 192.168.2.10	32.10.2.168.192.rpz-nsip.rpz.cisco.com
Name Server IP to query	32.<reversed-ip>.rpz-nsip.rpz.customer-domain>	Name Server Address 2001:db8:0:1::57	128.57.zz.1.0.db8.2001.rpz-nsip.rpz.cisco.com
A Records in Answer Section of Response	32.<reversed-ip>.rpz-ip.rpz.<customer-domain>	A answer record 192.168.2.10	32.10.2.168.192.rpz-ip.rpz.cisco.com
A Records in Answer Section of Response	<subnet-mask>.<reversed-ip>.rpz-ip.rpz.<customer-domain>	A answer record in subnet 192.168.2.0/24	24.0.2.168.192.rpz-ip.rpz.cisco.com

AAAA Records in Answer Section of Response	128.<reversed-ip>.rpz-ip.rpz.<customer-domain>	AAAA answer record 2001:db8:0:1::57	128.57.zz.1.0.db8.2001.rpz-ip.rpz.cisco.com
AAAA Records in Answer Section of Response	<prefix-length>.<reversed-ip>.rpz-ip.rpz.customer-domain>	AAAA answer record in prefix 2001:db8.0.1::/48	27.zz.1.0.db8.2001.rpz-ip.rpz.cisco.com

This zone contains all the RRs related to black listing query names. Blocking IP addresses and ranges must be done within the rpz-ip label (i.e. rpz-ip.rpz.cisco.com). The same logic can be applied to blocking name servers using the rpz-nsdname and rpz-nsip labels.

Note rpz-ip, rpz-nsdname, and rpz-nsip are just another label and is not a real subdomain or separate zone. No delegation points will exist at this level and CDNS relies on finding all the data within the referenced zone.

Note When using rpz-nsdname and rpz-nsip, the corresponding rule is applied to the original query and will therefore change the answer section. In cases when the final answer is determined from the RPZ rule(s), the rpz zone SOA will be included in the authority section.

When the Caching DNS server is configured to use RPZ, it queries the Authoritative DNS server to lookup the RPZ rules. The Caching DNS server formulates the correct query name, interprets the query response as an RPZ rule, and applies the rule to the client query. If the RPZ rule causes Caching DNS server to rewrite the client response, this data is cached to make future lookups faster. The Caching DNS server RPZ configuration determines which RPZ trigger should be used. If no RPZ rule is found, the query proceeds normally.

In addition, RPZ overrides can be configured on the Caching DNS server. This enables the Caching DNS server to override the RPZ action returned by the Authoritative DNS server. This is useful when you do not have control over the Authoritative DNS data as is the case when the data is pulled from a third party. When the Caching DNS server gets a match from the Authoritative DNS server for the RPZ query, it performs the override action rather than the rule action specified in the RR data.

DNS RPZ Actions

RPZ rules are created using standard DNS RRs, mostly CNAME RRs. However, for redirecting you can use any type of RR. The RR name follows the format based on the RPZ trigger as described in the DNS RPZ Zones section. The rdata defines the rule action to be taken. The following table describes the RPZ actions.

Table 2: RPZ Actions

RPZ Rule Action	RPZ RR RData	RPZ RR Example

NXDOMAIN	CNAME .	www.baddomain.com.rpz.cisco.com. 300 CNAME .
NODATA	CNAME *.	www.baddomain.com.rpz.cisco.com. 300 CNAME *.
NO-OP (whitelist)	CNAME rpz-passthru. CNAME FQDN	www.gooddomain.com.rpz.cisco.com. 300 CNAME rpz-passthru. www.gooddomain.com.rpz.cisco.com. 300 CNAME www.gooddomain.com.
DROP	CNAME rpz-drop.	www.baddomain.com.rpz.cisco.com. 300 CNAME rpz-drop.
Redirect	<any RR type> <redirect-data>	www.wrongdomain.com.rpz.cisco.com. 300 CNAME walledgarden.cisco.com. www.baddomain.com.rpz.cisco.com. 300 A 192.168.2.10 www.baddomain.com.rpz.cisco.com. 300 AAAA 2001:db8:0:1::57

DNS RPZ Best Practices

- CPIPE Authoritative DNS and Caching DNS are used for end to end RPZ solutions.
- The ***restrict-query-acl*** on the RPZ zone must include only the Caching DNS address and localhost.
- Zone transfers (***restrict-xfer-acl*****)** must be either completely denied or restricted only to a specific set of servers.
- RPZ zone must not be delegated from the parent zone. It must be hidden and only available to a specially configured Caching DNS.
- There must be no RPZ nameserver address record to avoid caching and keeping the name server.
- The name server record must point to a localhost.
- The number of RPZ zones must preferably be confined to 2-3 but not the configuration. The sequence to process a query increases linearly with the addition of each RPZ to a Caching DNS.
- The default TTL, for manually created RPZ zones, must reflect the rate of change in the zone data. The recommended rate ranges from 5m to 2h.
- The Caching DNS server must revise its max-cache-ttl settings to assure that the cached information is from a reliable source and can be trusted. This setting should be in line with the default TTL of 5m to 2h.
- The Authoritative DNS servers must enable NOTIFY, IXFR, AXFR and TSIG for zone transfers of distributed RPZ data.

Setting Up DNS Firewall Rules

To add or edit DNS firewall rules:

Local Basic or Advanced Web UI

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

Step 2 Click the **Add DNS Firewall Rule** icon in the DNS Firewall pane to open the Add DNS Firewall dialog box.

Step 3 Enter a rule name in the Rule Name field and specify the action type.

Note The drop and refuse actions are applicable to all the queries for the specified domains, while the redirect and redirect-NXDOMAIN rules are applicable only to the queries of A and AAAA records.

Step 4 Click **Add DNS Firewall** to save the firewall rule. The List/Add DNS Firewall Rules page appears with the newly added firewall rule.

Note The rules with the action **refuse** do not use a domain or destination IP address.

Step 5 If you selected the **drop** or **redirect** action:

- Enter the ACL List, and click the **Add** icon to add the domains that need to be monitored for the drop or redirection
- For the **redirect** action, you also need to enter the IPv4 Destination or IPv6 Destination.

Step 6 If you selected the **rpz** action:

1 Enter the RPZ Zone Name and the name of RPZ server.

Note The recommended RPZ zone name should be **rpz.<customer-domain>** to avoid conflicting with domain names in the Global DNS space.

2 Select the RPZ Trigger from the options and the corresponding override action.

Step 7 Click **Save** to save your settings, or click Revert to cancel the changes .

Note To delete a DNS Firewall rule, select the rule on the DNS Firewall pane, click the **Delete** icon, and then confirm the deletion.

CLI Commands

Use the following CLI commands to:

- Add the DNS firewall rules, separated by spaces, use **cdns-firewall** *rule-name* **create**.
- List the domains the domain redirect rule, use **cdns-firewall list**.
- Remove domain redirect rule, use **cdns-firewall** *rule-name* **delete**.

Changing Priority of DNS Firewall Rules

When you create a set of DNS firewall rules, you can specify the priority in which order the rules will apply. To set the priority or reorder the rules:

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

Step 2 Click the **Reorder DNS Firewall Rules** icon in the DNS Firewall pane to open the Reorder dialog box.

Step 3 Set the priority for the DNS Firewall rules by either of the following methods:

- Select the rule and click the Move up or Move down icon to reorder the rules.
- Select the rule and click the Move to button, and enter the row number to move the rule.

Step 4 Click **Save** to save the reordered list.

Troubleshooting DNS Servers

Useful troubleshooting hints and tools to diagnose the DNS server and ways to increase performance include:

- **Restoring a loopback zone—**A loopback zone is a reverse zone that enables a host to resolve the loopback address (127.0.0.1) to the name *localhost* . The loopback address is used by the host to enable it to direct network traffic to itself. You can configure a loopback zone manually or you can import it from an existing BIND zone file.
- **Listing the values of the DNS server attributes—**Click **DNS**, then **DNS Server** to open the Edit DNS Server page in the web UI. In the CLI, use **dns show**.
- **Adjusting certain attribute values that could have inherited preset values from previous releases during an upgrade—**The DNS server operating with legacy preset values for critical settings are probably not optimal for current systems and can cause performance issues. We strongly recommend that you update the legacy settings to use the new preset values. The table below lists the old and new preset values, along with a recommended setting for each attribute.

Table 3: DNS Attributes with Changed Preset Values

DNS Attribute	7.0 Preset Value	7.1 Preset Value	Recommended Setting
axfr-multirec-default	on	on	on
mem-cache-size	10000 (KB)	50000 (KB)	50000 (KB)

For many of these attributes, you must enter Expert mode in the web UI or use **set session visibility=3** in the CLI. To change the preset value to the current one, unset the attribute. To change to the recommended setting, change the attribute value.

Be sure to reload the DNS server after saving the settings.

- **Choosing from the DNS log settings to give you greater control over existing log messages—**Use the *Log settings* attribute on the Edit DNS Server page in the web UI, or dns set log-settings in the CLI, with one or more of these keyword or numeric values, separated by commas (see table below). Restart the server if you make any changes to the log settings.

Table 4: DNS Log Settings

Log Setting	Description
config	Server configuration and deinitialization.
ddns	High level dynamic update messages.
xfr-in	Inbound full and incremental zone transfers.
xfr-out	Outbound full and incremental zone transfers.
notify	NOTIFY transactions.
datastore	Data store processing that provides insight into various events in the server embedded databases.
scavenge	Scavenging of dynamic RRs (see the Scavenging Dynamic Records section in *Cisco Prime IP Express 8.3 DHCP User Guide*).
scavenge-details	More detailed scavenging output (disabled by default).
server-operations	General high-level server events, such as those pertaining to sockets and interfaces.
ddns-refreshes	DNS update refreshes for Windows clients (disabled by default).
ddns-refreshes-details	RRs refreshed during DNS updates for Windows clients (disabled by default).
ddns-details	RRs added or deleted due to DNS updates.
tsig	Logs events associated with Transaction Signature (TSIG) DNS updates (see the Transaction Security section in *Cisco Prime IP Express 8.3 DHCP User Guide*).
tsig-details	More detailed logging of TSIG DNS updates (disabled by default).

Log Setting	Description
activity-summary	Summary of activities in the server. You can adjust the interval at which these summaries are taken using the *activity-summary-interval* attribute, which defaults to five-minute intervals (you can adjust this interval using **dns set activity-summary-interval**).
query-errors	Logs errors encountered while processing DNS queries.
config-details	Generates detailed information during server configuration by displaying all configured and assumed server attributes (disabled by default).
incoming-packets	Incoming data packets.
outgoing-packets	Outgoing data packets.
xfer-in-packets	Incoming full zone transfer (XFR) packets.
query-packets	Incoming query packets.
notify-packets	NOTIFY packets.
ddns-packets	DNS Update packets.
xfer-out-packets	Outgoing XFR packets.
ha-details	Generates detailed logging of High-Availability (HA) DNS information.
scp	Allows log messages associated with SCP message handling.
optRR	Causes logging related to OPT RR processing.
ha-messages	Enables detailed logging of HA messages.

- **Using the nslookup utility to test and confirm the DNS configuration—**This utility is a simple resolver that sends queries to Internet nameservers. To obtain help for the **nslookup** utility, enter **help** at the prompt after you invoke the command. Use only fully qualified names with a trailing dot to ensure that the lookup is the intended one. An **nslookup** begins with a reverse query for the nameserver itself, which may fail if the server cannot resolve this due to its configuration. Use the **server** command, or specify the server on the command line, to ensure that you query the proper server. Use the **–debug**, or better yet, the **–d2**, flag to dump the responses and (with **–d2**) the queries being sent.
- **Using the dig utility to troubleshoot DNS Server —**dig (domain information groper) is a flexible tool for interrogating DNS name servers. It performs DNS lookups and displays the answers that are returned from the name server(s) that were queried. Most DNS administrators use dig to troubleshoot DNS

problems because of its flexibility, ease of use, and clarity of output. To obtain help for the **dig** utility, enter **help** at the prompt after you invoke the command.

Although dig is normally used with command-line arguments, it also has a batch mode of operation for reading lookup requests from a file. Unlike earlier versions, the BIND9 implementation of dig allows multiple lookups to be issued from the command line. Unless you specifically query a specific name server, dig tries each of the servers listed in /etc/resolv.conf. When no command line arguments or options are given, dig performs an NS query for the root ".". A typical invocation of dig looks like: dig @server name type where server is the name or IP address of the name server to query.