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

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 9.0 DHCP User Guide*.
- **Synchronize All HA Zones—**Synchronizes all the HA zones. You have the option to choose the type of synchronization. The **Push All Zones From Main to Backup** option is checked by default. You can override this by checking **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
- **Round-robin server processing—**See Enabling Round-Robin, on page 3
- **Subnet sorting—**See Enabling Subnet Sorting, on page 5
- **Enabling incremental zone transfers—**See Enabling Incremental Zone Transfers (IXFR) , on page 5
- **Enabling NOTIFY packets—**See Enabling NOTIFY, on page 6

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 9.0 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.

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

Enabling Weighted Round-Robin

When a nameset is configured with multiple RRs of the same type, a weighted round-robin algorithm can be used to determine which RR is returned in a query response. To control the response behavior, administrators must be able to set weighted values on these RRs. In addition, the order in which multiple records are returned may be used by client applications and need to be controlled by administrators.

Order and *weight* attributes available only in advanced mode, and attribute timestamp is available only in expert mode.

Order

Attribute *order* specifies the sort order for the RR, compared to other RRs of the same type in the nameset. RRs with same type will be listed in ascending order, this will also be the order that RRs are returned when queried.

Weight

RR weight can be used in situations where it is important to have certain like services used more often than other (i.e. a web server) since many clients will use the RR that is first in the DNS response. Attribute *weight* specifies the relative importance of this RR, compared to other RRs of the same type in the nameset. RRs with higher weight will be used more often in query responses for the name and type. For example, if weight for the RR is set to 5 and weight for another RR is set to 1, then RR will be used 5 times before the other RR is used once. RRs with a weight of 0 (zero) are always listed last and not included in the round robin operation.

Note The default weight on RRs is 1. When round robin is enabled (either DNS server or zone level), the RRs are returned in the first position once for each query (i.e. traditional round robin).

If all the weights on RRset are set to 0, then RR set does not round robin and we return the set to the client based on order (Round robin disabled at RRset level).

Timestamp

Attribute timestamp records the last time the RR was added or refreshed via DNS update.

Weight, order and timestamp can only be set on primary zones. Weight, order and timestamp are transferred to HA backup and to the secondary servers, these attributes are not transferred when one of the server in HA or secondary server are prior to 9.0 cluster. If you wish not to transfer order and weight, then disable Transfer RR Meta Data (xfer-rr-meta-data) attribute present in the DNS Server (you must do this in secondary DNS Server). In secondary zone "weight", "order" are available and the "resource records" are non-editable.

Local Basic or Advanced Web UI

Step 1 From the **Design** menu, choose **Forward Zones or Reverse Zones** under the Auth DNS submenu.

Step 2 In the Forward Zone pane, click the **zone name** to open the edit zone page.

Step 3 Add the RR name, TTL (if not using the default TTL), type, and data as appropriate.

Step 4 Click **Resource Records** tab.

Step 5 Once the RRs are created, weight and order can be set by editing the RRs (click on the pencil icon).

Note The *timestamp* attribute is available only in expert mode and it is read-only.

CLI Commands

Use the following command to set the weight and order:

```
Zone <zone> addRR <rr-name> <rr-type> <rr-ttl> <rr-data> [weight=<rr-weight>] [order=<rr-order>]
```

Use the following command to modify the resource records:

```
zone <name> modifyRR <name> <type> [<data>] <attribute>=<value> [<attribute> =<value> ...]
```

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 6) 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 is 0, as we always use IXFR and it is enabled, we don't periodically change to AXFR. 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 9.0 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* explicitly 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 and IPv6 addresses to the notify-list on the zone configuration.

Note In order for notifies to be sent to hidden name servers (i.e. those that are not listed as NS RRs in the zone), their IP addresses need to be listed in the notify-list and notify setting needs to be set to `notify-list` or `notify-all`.

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 Advanced Web UI

Step 1 On the **Manage DNS Authoritative Server** page, under the **Zone Transfer Settings** section, find the *notify* attribute and select the value from the drop-down list.

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** or **Reverse Zones** or **Secondary 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-list* attribute on the Edit Zone page.

Step 7 Select the value from the *notify* drop-down list.

Step 8 Click **Save**.

CLI Commands

Use **dns set notify**=***value***. NOTIFY is enabled by default. You can also enable NOTIFY at the zone level, where you can use **zone** *name* **set notify-list** 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 7
- **Secondary server attributes—**See Setting Secondary Refresh Times, on page 8
- **Port numbers—**See Setting Local and External Port Numbers, on page 9
- **Handle Malicious DNS Clients—**See Handling Malicious DNS Clients, on page 9

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 *deftl* 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 6.

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 default 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 default 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 default 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 9.0 Administrator Guide*.

Local Advanced Web UI

On the Manage DNS Authoritative Server page, under the Network Settings section, find the Listening Port (*local-port-num)* and Remote DNS servers port (*remote-port-num)* attributes, set them to the desired values (they both have default value of 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 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 500000 KB (500 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.
- **EDNS maximum payload size DNS server attribute (*edns-max-payload*)—** Specifies the sender's maximum UDP payload size, which is defined as the number of octets of the largest UDP packet that can be handled by a requestor. 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.

Running Caching DNS and Authoritative DNS on the Same Server

Cisco Prime IP Express includes a Hybrid DNS feature that allows you to run both the Caching DNS and Authoritative DNS servers on the same operating system without two separate virtual or physical machines. This feature allows the Caching DNS to auto-detect the Authoritative DNS server and its zones without creating exceptions.

Note Cisco recommends that hybrid mode is only for smaller sized deployments. For larger deployments, Cisco recommends separating Caching and Authoritative DNS on separate physical machines or VMs.

Following prerequisites must be met for hybrid mode to work correctly:

- The local cluster must be licensed for both Caching and Authoritative DNS.
- Caching DNS and Authoritative DNS must have their own configured unique and separate network interfaces. The loopback interface (127.0.0.1/8, ::1/128) should be configured on the Authoritative DNS server.

Once the prerequisites have been met, hybrid mode can be enabled on the Authoritative DNS server.

When you enable hybrid mode, the following results occur:

1. Whenever the Authoritative DNS server is reloaded, it causes the Caching DNS server to be reloaded.
2. The Caching server reads the Authoritative servers interface list to detect which IP to send requests to.
3. The Caching server auto detects all zones (forward, reverse and secondary) and auto creates in memory exceptions for those zones.
4. The Caching server will not cache hybrid mode responses regardless of the RRs TTL value. This ensures that the responses it returns to clients reflect the most up-to-date information.

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. This setting is only supported for Linux deployments.

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 in the Hybrid Mode section 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. Use **dns-interface set** *attribute=value* or **cdns-interface set** *attribute=value* to set the interfaces.

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—** These preset values are probably not optimal for current systems and can cause performance issues. We strongly recommend that you to update the settings to use the new preset values. Example: The present value of maximum memory cache size DNS server attribute (mem-cache-size) is updated to 500 MB.

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 server-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 1: DNS Log Settings

Log Setting	Description
activity-summary	This setting enables logging of DNS statistic messages at the interval specified by activity-summary-interval. The type of statistics logged can be controlled with **activity-counter-log-settings and activity-summary-type**).
config	This setting enables logging of DNS server configuration and de-initialization messages.
config-details	This setting enables logging of detailed configuration messages (i.e. detailed zone configuration logging).
db	This setting enables logging of database processing messages. Enabling this flag provides insight into various events in the server's embedded databases.

Log Setting	Description
ha	This setting enables logging of HA DNS messages.
notify	This setting enables logging of messages associated with NOTIFY processing.
push-notifications	This setting enables logging associated with DNS Push Notifications.
query	This setting enabled logging of messages associated with QUERY processing.
scavenge	This setting enables logging of DNS scavenging messages.
server-operations	This setting enables logging of general server events, such as those pertaining to sockets and interfaces.
scp	This setting enabled logging associated with SCP messages handling.
tsig	This setting enables logging of events associated Transaction Signature (TSIG).
update	This setting enables logging of DNS Update message processing.
xfr-in	This setting enables logging of inbound full and incremental zone transfers.
xfr-out	This setting enables logging of outbound full and incremental zone transfers.

- **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, use **dig -h** or on Linux, use **man dig**.
- **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.

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.