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 Network Registrar provides a feature to periodically purge stale records. See the *"Scavenging Dynamic Records" section in Cisco Prime Network Registrar 10.0 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
- **Log settings**—See Specifying Log Settings, on page 3
- **Packet logging**—See Enabling Packet Logging, on page 4
- **Top names settings**—See Specifying Top Names Settings, on page 6
- **Round-robin server processing**—See Enabling Round-Robin, on page 7
- **Subnet sorting**—See Enabling Subnet Sorting, on page 9
- **Enabling incremental zone transfers**—See Enabling Incremental Zone Transfers (IXFR) , on page 9
- **Enabling NOTIFY packets**—See Enabling NOTIFY, on page 10

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 Network Registrar 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 Network Registrar uses the server IP address for official name lookups and for DNS updates (see the *"Managing DNS Update" chapter in Cisco Prime Network Registrar 10.0 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.

Specifying Log Settings

The *server-log-settings* attribute determines which events to log in the DNS log files. Default flags are activity-summary, config, update, xfr-in, xfr-out, scp, scavenge, server-operations, and ha.

Logging additional detail about events can help analyze a problem. However, leaving detailed logging enabled for a long period can fill up the log files.

The possible options are:

- **host-health-check**—This setting enables logging associated with DNS Host Health Check.
- **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-detail**—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.
- **dnssec**—This setting enables log messages associated with DNSSEC processing.
- **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.
- **scp**—This setting enabled logging associated with SCP messages handling.
- **server-operations**—This setting enables logging of general server events, such as those pertaining to sockets and interfaces.
- **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.

Enabling Packet Logging

Cisco Prime Network Registrar supports packet logging for Authoritative DNS server to help analyze and debug the Authoritative DNS server activity. The packet logging settings determine the type of packet logging (summary or detail), the type of packets logged, and to which log file the messages are logged. By default, the Authoritative DNS server does not log any packet log messages.

Use the following server level attributes to enable packet logging for the Authoritative DNS server:

Table 1: Authoritative DNS Server Packet Logging Attributes

Attribute	Description
Packet Logging (*packet-logging*)	Determines the type of packet logging that is logged to the DNS logs. The type of DNS packets logged can be controlled with the *packet-log-settings* attribute. • **disabled**—This settings disables logging of DNS packets. • **summary**—This setting enables one line summary logging of DNS packets. • **detail**—This setting enables detailed packet tracing of DNS packets. **Note:** While packet logging can be helpful for debugging and troubleshooting, it does have an impact on DNS server performance. Therefore, Cisco does not recommend leaving packet logging enabled in production environments.
Packet Logging File (*packet-logging-file*)	Determines the destination log of packet log messages when packet logging is enabled. • **dns**—Packet logging messages are logged to the standard DNS log file (name_dns_1_log*). • **packet**—Packet logging messages are logged to a separate DNS packet log file (dns_packet_log*).

Attribute	Description
Packet Log Settings (*packet-log-settings*)	Determines the type of DNS messages to log if packet logging has been enabled. Packet logging can be enabled by configuring the *packet-logging* attribute. • **all-in**—This setting enables logging of all incoming packets. **Note:** This is equivalent to enabling all the -in settings. • **all-out**—This setting enabled logging of all outgoing packets. **Note:** This is equivalent to enabling all the -out settings. • **ha-in**, **ha-out**—These settings enable logging of HA DNS messages except for HA heartbeat and frame ACK messages which are controlled by the ha-heartbeat-in, ha-heartbeat-out and ha-frameack-in, ha-frameack-out settings, respectively. • **ha-heartbeat-in**, **ha-heartbeat-out**—These settings enable logging of HA DNS heartbeat messages. • **ha-frameack-in**, **ha-frameack-out**—These settings enable logging of HA DNS frame ACK messages. • **notify-in**, **notify-out**—These settings enable logging of DNS NOTIFY messages. • **push-notifications-in**, **push-notifications-out**—These settings enable logging of DNS Push Notification messages. • **update-in**, **update-out**—These settings enable logging of DNS UPDATE messages. • **xfr-in**, **xfr-out**—These settings enable logging of DNS IXFR and AXFR messages.

Local Advanced Web UI

Step 1 On the Manage DNS Authoritative Server page, under the **Packet Logging** section, select the value for **packet-logging** from the drop-down list. The value can be **summary** or **detail**.

Step 2 For the *packet-log-settings* attribute, check the desired check boxes.

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

CLI Commands

Use **dns set packet-logging=summary** to enable one line summary packet logging.

Use **dns set packet-logging=detail** to enable detailed packet tracing.

Use **dns set packet-log-settings**=*value* to set the type of packets to log when packet logging is enabled.

Note Reloading of Authoritative DNS server is not required for the *packet-logging* and *packet-log-settings* attributes to take effect immediately (similar to log settings). However, the *packet-logging-file* attribute requires a Authoritative DNS server reload.

Specifying Activity Summary Settings

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

You can specify the interval at which to log activity-summary information using the Statistics Interval (*activity-summary-interval*) attribute. Enable the *active-summary* attribute in the server log-settings to set the seconds between DNS activity summary log messages. The *Activity-summary- interval* attribute has a default value of 60 seconds.

The Authoritative DNS server logs sample and/or total statistics based on the option you check for the attribute Statistics Type (*activity-summary-type*). The default value of *Activity-summary -type* attribute is "sample".

The option checked for the attribute Statistics Settings (*activity-counter-log-settings*) controls what activity counters a DNS server uses for logging.

Note *activity-summary-type* and *activity-counter-log-settings* take effect without a reload as soon as the DNS server object or the session is saved.

The possible settings are:

- host-health-check—Log DNS Host Health Check counters.
- cache—Log query cache related counters.
- db—Log database counters.
- ha—Log HA related counters.
- ipv6—Log IPv6 related counters.
- maxconters—Log maxcounters related counters.
- performance—Log performance related counters.
- push-notifications—Log DNS Push Notification counters.
- query—Log query related counters.
- security—Log security related counters.
- system—Log system related counters.
- top-names—Log the top names queried and hit count.
- update—Log DNS Update related counters.

Specifying Top Names Settings

The *top-names* attribute specifies if top names data should be collected. When enabled, a snapshot of the cache hits for the top names that are queried is collected for each interval set by the **top-names-max-age** value. The list of top names that is reported with activity summary statistics is the most current snapshot.

You can specify the maximum age (based on last access time) of a queried name allowed in the list of top names by using the *top-names-max-age*.

Note The *top-names-max-age* attribute has a default value of 60 seconds.

You can specify the maximum number of entries in the list of top names queried by using the attribute *top-names-max-count*. This limit is applied to the lists of top names that are logged or returned as part of activity summary. You can specify the number of DNS cached records inspected in one batch by using the attribute *top-names-batch-size* (only in **expert mode**).

Local Basic or Advanced Web UI

To enable Top Names, on the **Edit Local DNS Server** tab, under the **Top Names Settings** category, find the *top-names* attribute and enable it by selecting the "enabled" option and then click **Save** to save the changes.

Top Names

By selecting the "Top Names" tab, the relevant information with respect to top N domains and other important statistics attributes will be displayed.

Local Basic or Advanced Web UI

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

Step 2 Select **DNS Server** in the Manage Servers pane.

Step 3 Click on the **Top Names** tab available in the Local DNS Server page.

CLI Commands

Use **dns getStats top-names** to view the Top Names statistics.

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 10.0 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 Network Registrar 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 Network Registrar 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 10) 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 Network Registrar 10.0 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 Network Registrar 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 Network Registrar 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.

Managing Authoritative DNSSEC

DNS Security Extensions (DNSSEC) provides origin authority, data integrity, and authenticated denial of existence. With DNSSEC, the DNS protocol is much less susceptible to certain types of attacks, particularly DNS spoofing attacks. DNSSEC provides protection against malicious or forged answers by adding digital signatures into DNS data, so each DNS response can be verified for integrity and authenticity.

Cisco Prime Network Registrar 9.0 and earlier Authoritative DNS Server do not support signing of zones. From CPNR 10.0, Authoritative DNSSEC support adds authentication and integrity to DNS zones. With this support, CPNR DNS server is able to support both secure and unsecure zones.

To add DNSSEC Security:

1. Choose regional or local management of DNSSEC keys and zones.
2. Review the algorithm, size, lifetime, and intervals set for Authoritative DNSSEC that will be used for default key generation.
3. Create Zone Signing and Key Signing keys if not using internally generated keys.
4. Enable DNSSEC for the required zones.
5. Export the DS RR for the signed zone which must be added to the parent zone, if it is not configured on the same server.

Enabling Authoritative DNSSEC

DNSSEC is enabled by default on the Authoritative DNS Server. It can be disabled by using the *dnssec* attribute in the AuthDnsSec configuration. Disabling this attribute will disable zone signing for all zones, regardless of the zone *dnssec* attribute. By default, zone signing is disabled for all zones. To enable zone signing, the *dnssec* attribute in the zone configuration must be enabled. Once DNSSEC is enabled on the zone, zone signing is performed using core keys by default, or tenant keys specific to the zone tenant, if defined. The CCM server will create new keys for the zones, if there are no keys available.

Note DNSSEC cannot be enabled on a zone if RPZ is enabled and vice versa.

Table 2: Zone Signing Key Attributes

Attribute	Description

zsk-algorithm	Specifies the cryptographic algorithm to be used for the Zone Signing Key. DSA : DSA/RSA-1, value: 3, range: 512-1024 RSASHA1 : RSA/SHA-1, value: 5, range: 512-2048 RSASHA256 : RSA/SHA-256, value: 8, range: 512-2048 RSASHA512 : RSA/SHA-512, value: 10, range: 512-2048
zsk-bits	Specifies the number of bits in the key and must be a multiple of 64. The value depends on the Zone Signing Key algorithm (zsk-algorithm) chosen. DSA : DSA/RSA-1, value: 3, range: 512-1024 RSASHA1 : RSA/SHA-1, value: 5, range: 512-2048 RSASHA256 : RSA/SHA-256, value: 8, range: 512-2048 RSASHA512 : RSA/SHA-512, value: 10, range: 512-2048
zsk-lifetime	Specifies the lifetime of a Zone Signing Key (ZSK). This defines the time interval where the key is used to sign zones. It is used to determine the deactivation-date when a ZSK key is created. The configured value MUST be greater than the zsk-rollover-interval. A value that is 10 times greater is recommended.
zsk-rollover-interval	Specifies the time interval for the Zone Signing Key (ZSK) rollover process. It determines the lead time for the new key prior to the current key deactivation-date. Configured interval should be more than maximum TTL of the zones plus the propagation delay, to avoid bogus zone information.
zsk-rollover-wait-interval (Available in Expert mode only)	Specifies the wait time before a Zone Signing Key (ZSK) can be removed, after the ZSK deactivation-date. This interval is used to determine the expiration-date for the ZSK key. It should be 2 times the maximum zone TTL to ensure all secondary servers are up-to-date. If set to 0, the ZSK expiration-date will also be set to 0. This setting disables automatic ZSK key removal.

Table 3: Key Signing Key Attributes

Attribute	Description
ksk-algorithm	Specifies the cryptographic algorithm to be used for the Key Signing Key. DSA : DSA/RSA-1, value: 3, range: 512-1024 RSASHA1 : RSA/SHA-1, value: 5, range: 512-2048 RSASHA256 : RSA/SHA-256, value: 8, range: 512-2048 RSASHA512 : RSA/SHA-512, value: 10, range: 512-2048

ksk-bits	Specifies the number of bits in the key and must be a multiple of 64. The value depends on the Key Signing Key algorithm (ksk-algorithm) chosen. DSA : DSA/RSA-1, value: 3, range: 512-1024 RSASHA1 : RSA/SHA-1, value: 5, range: 512-2048 RSASHA256 : RSA/SHA-256, value: 8, range: 512-2048 RSASHA512 : RSA/SHA-512, value: 10, range: 512-2048
ksk-rollover-interval	Specifies the time interval for the Key Signing Key (KSK) rollover process. It determines the lead time for the new key prior to the current key deactivation-date.

Local Advanced or Expert Web UI

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

Step 2 Manage Authoritative DNSSEC page displays **Zone Signing Key** and **Key Signing Key** sections. Modify the attributes in these sections as per your requirements.

Step 3 Click **Save** to save your settings.

CLI Commands

"DNSSEC controls and configures DNSSEC processing in the Authoritative DNS server.

```
dnssec set <attribute>=<value> [<attribute>=<value>...]
```

When connected to a regional cluster, you can use the following pull and push commands.

dnssec pull *cluster-name* [**-report-only** | **-report**]

dnssec push *cluster-name* [**-report-only** | **-report**]

`"zone <zonename> signZone"` command can be used to enable DNSSEC or resign a zone when executed in expert mode.

Managing Authoritative DNSSEC Keys

To configure DNSSEC protected zones, a key must first be created. The zone is then signed using the key. You can create a key manually to customize the key attributes. Otherwise, the CCM server will create new keys automatically, as needed.

The *key-rollover* attribute in Authoritative DNSSEC page can be set to local or regional management. The default is local. The *key-rollover* attribute specifies whether the regional or local cluster should perform Zone Signing Key (ZSK) rollover. With local rollover management, keys are managed on the local primary or HA main. The keys are copied to the HA backup via CCM HA sync. If zones are distributed across several primary servers, there will be many more keys to manage. With regional rollover management, keys are managed on the regional server and pushed to the local clusters. This lets you to manage a common set of keys for your distributed primary servers. With central zone management, you can also stage zone edits and pre-sign zones

before synchronizing the changes with the local DNS servers. Keys are auto-synched from regional to local when DNS edit mode is set to synchronous in the Regional CCM server.

Rollover of Zone Signing Key is an automated process. Rollover of KSK has to be performed manually, the rollover-ksk command is used to start the Key Signing Key rollover process. You can provide your own key or allow CCM to generate keys.

dns rollover-ksk [*tenant-id*=<**value**>][**next-key**=<*keyname*>]

Note In a lab setting, you can use the expert mode command **zone name removeSignature** to remove all signature RRs and disable DNSSEC for the zone. This command should not be used for operational DNSSEC zones. Operational DNSSEC zones that will no longer be signed need to let signature records expire before they are deleted, following the guidelines in RFC 6781 - DNSSEC Operational Practices, Version 2.

Table 4: Key Timelines Attributes

Attribute	Description
activation-date	Specifies the activation date and time for this key. Beginning at this date and time, the key will be used to sign RR Sets.
deactivation-date	Specifies the deactivation date and time for this key. Until this date and time, the key will be used to sign RR Sets. This attribute must be 0 for Key Signing Keys. Key Signing Keys remain active until the key rollover process is initiated.
expiration-date	Specifies the date and time this Zone Signing Key is scheduled to be removed. If 0, automatic removal is disabled and the key must be deleted by user action. This attribute must be 0 for Key Signing Keys. Key Signing Keys remain active until the key rollover process is initiated. When the rollover process is complete, the key can be deleted by user action.

Local or Regional Advanced or Expert Web UI

Step 1 From the **Design** menu, choose **Auth DNSSEC Keys** under the **Security** submenu to open the List/Add Authoritative DNSSEC Keys page.

Step 2 Set the attribute *enable-signing* value to **true** to enable the key and to sign the zones.

Step 3 Click **Save**.

Step 4 This page displays **Key Timelines** section, where you can find the Key Timelines attributes. You can enter the deactivation date and removal date as required.

Step 5 Click **Save** to save your settings.

CLI Commands

The **dnssec-key** command creates and manages Authoritative Domain Name System Security Extensions (DNSSEC) keys for zone signing.

dnssec-key <*name*> **create** [<*attribute*>=<*value*>...]

dnssec-key <*name*> **delete** [**-force]**

dnssec-key <*name*> **show**

dnssec-key <*name*> **set** <*attribute*>=<*value*> [<*attribute*>=<**value**>...]

To check the current status of DnsSecKeys related to rollover process use the command "**dnssec-key getStatus**".

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.

dnssec-key <*name* | **all**> **pull** <**replace** | **exact**> *cluster-name* [**-report-only** | **-report**]

dnssec-key <*name* | **all**> **push** <**replace** | **exact**> *cluster-name* [**-report-only** | **-report**]

dnssec-key *name* **reclaim** *cluster-list* [**-report-only** | **-report**]

Exporting DS Record

Export DS record is available for the DNSSEC enabled zone. If the parent zone is found on the authoritative server, the DS record will be added to the zone automatically. If multiple authoritative servers are deployed, and the parent zone is on another local cluster, you can manage the zones on the regional server to automatically update the parent zone. If the parent zone is externally-owned, you must provide the DS resource record to be added by the external organization. Follow the below steps to Export DS record.

Step 1 From the **Design** menu, choose **Forward Zones** under the **Auth DNS** submenu to open the Edit Zone page.

Step 2 On the Edit Zone page, under the **DNSSEC Settings**, set the **DNSSEC** value to **true** to enable the DNSSEC.

Step 3 Click **Save** to save your settings.

Step 4 Click the **save** icon available next to the **DS Record** to export DS record.

CLI Commands

After you export DS record you need to publish the same to parent zone by using the following command:

```
export dnssec-ds <zone name> <filename>
```

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 16
- **Secondary server attributes**—See Setting Secondary Refresh Times, on page 16
- **Port numbers**—See Setting Local and External Port Numbers, on page 17
- **Handle Malicious DNS Clients**—See Handling Malicious DNS Clients, on page 18

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 Network Registrar 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 Network Registrar 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 Network Registrar 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 10.

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 Network Registrar Services" section in Cisco Prime Network Registrar 10.0 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 Network Registrar, 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 Network Registrar 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.

Note When you are in Hybrid mode configuration, SNMP queries to CPNR will retrieve only the Caching DNS server static values and not the Authoritative DNS server static values.

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 In Hybrid mode the Caching DNS and the Authoritative DNS servers must be configured with their own separate network interfaces. Using the loopback interface for Authoritative DNS server is supported only for Linux deployments and when the Authoritative DNS server does not require direct access for queries, notifies or zone transfers.

a. From the **Operate** menu, choose **Manage Servers** to open the Manage Servers page.

b. Click **Local DNS Server** in the Manage Servers pane.

c. 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.

d. Click **Local CDNS Server** in the Manage Servers pane.

e. 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:

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

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

c. 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 5: 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.

Log Setting	Description
config-details	This setting enables logging of detailed configuration messages (i.e. detailed zone configuration logging).
DNSSEC	This setting enables log messages associated with DNSSEC processing.
Host-health-check	This setting enables logging associated with DNS Host Health Check.
db	This setting enables logging of database processing messages. Enabling this flag provides insight into various events in the server's embedded databases.
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.