THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS” WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2015 Cisco Systems, Inc. All rights reserved.
CONTENTS

PART I

Introduction 11

CHAPTER 1

Introduction to the Domain Name System 1

How DNS Works 1

Overview of Concepts in DNS 2

Domains 2

Learning ExampleCo Address 2

Establishing a Domain 3

Difference Between Domains and Zones 3

Nameservers 4

Reverse Nameservers 6

Authoritative and Caching DNS servers 6

High-Availability DNS 6

EDNS 6

DNS Views 7

CHAPTER 2

DNS Server Status Dashboard 9

Opening the Dashboard 9

Display Types 9

General Status Indicators 10

Graphic Indicators for Levels of Alert 10

Magnifying and Converting Charts 11

Legends 11

Tables 11

Line Charts 11

Stacked Area Charts 13

Cisco Prime Network Registrar 8.3 Caching and Authoritative DNS User Guide
CHAPTER 4

Advanced Caching DNS Server 31

Defining Forwarders 31
  Local Basic or Advanced Web UI 31
  CLI Commands 32

Using Exceptions 32
  Local Basic or Advanced Web UI 32

Managing DNS64 33
  Local Advanced Web UI 34
  CLI Commands 34

Managing DNSSEC 34
  Local Basic or Advanced Web UI 35

Setting up Caching DNS and Authoritative DNS Server on Same Operating System 35

Managing DNS Firewall 35

CHAPTER 5

Caching DNS Metrics 37

DNS Queries Type 37
  How to Interpret the Data 37

DNS Queries Responses 37
  How to Interpret the Data 38
  Troubleshooting Based on the Results 38

DNS Incoming Queries 38
  How to Interpret the Data 38

DNS Recursive Query Time 38
  How to Interpret the Data 39
  Troubleshooting Based on the Results 39

DNS Caching 39
  How to Interpret the Data 39
  Troubleshooting Based on the Results 39

Caching DNS General Indicators 39
  How to Interpret the Data 40
  Troubleshooting Based on the Results 40

DNS Caching Server Queries Per Second 40
PART III

CHAPTER 6

Managing Authoritative DNS Server 43

Running DNS Authoritative Server Commands 43
Configuring DNS Server Network Interfaces 44
Setting DNS Server Properties 44
Setting General DNS Server Properties 45
   Local Basic or Advanced Web UI 45
Specifying Delegation-Only Zones 45
Enabling Round-Robin 45
Enabling Subnet Sorting 46
Enabling Incremental Zone Transfers (IXFR) 46
Restricting Zone Queries 47
Enabling NOTIFY 47
Setting Advanced Authoritative DNS Server Properties 48
   Setting SOA Time to Live 48
   Setting Secondary Refresh Times 48
   Setting Secondary Retry Times 49
   Setting Secondary Expiration Times 49
   Setting Local and External Port Numbers 49
Handling Malicious DNS Clients 50
Tuning DNS Properties 50
Setting up Caching DNS and Authoritative DNS Server on Same Operating System 51
   Local Advanced Web UI 52
   CLI Commands 52
Managing DNS Firewall 52
   Setting Up DNS Firewall Rules 56
Troubleshooting DNS Servers 57

CHAPTER 7

Managing High Availability DNS 61

Introduction to HA DNS Processing 61
Creating High Availability DNS Pairs 63
   Local Basic or Advanced and Regional Web UI 63
CLI Commands  64

HA DNS Configuration Synchronization  64
   Pre-install Cisco Prime Network Registrar on the HA DNS backup server  65
   Pre-migration Steps for HA DNS Main Server  65
   Restart Cisco Prime Network Registrar on the HA DNS Main Server  65
   Copy Cisco Prime Network Registrar Database Files to HA DNS Backup Server  66
   Reconfigure Cisco Prime Network Registrar on the HA DNS Backup Server  66
   Configure Cisco Prime Network Registrar HA DNS on the HA DNS Main Server  67
   Reload the DNS Servers  67
   Synchronizing HA DNS Zones  67
      Local Advanced Web UI  67
      CLI Commands  68
   Enable Logging of HA DNS Information  68
   Viewing HA DNS Statistics  68
      Local Basic or Advanced Web UI  68
      CLI Commands  68

Managing Zones  69

   Managing Primary DNS Servers  70
      Related Topics  70
   Creating and Applying Zone Templates  70
      Local Basic or Advanced and Regional Web UI  70
   Staged and Synchronous Modes  72
      Local and Regional Web UI  72
      CLI Commands  73
   Configuring Primary Forward Zones  73
      Creating Primary Zones  73
      Editing Primary Zones  76
   Confirming Zone Nameserver Configuration  76
   Synchronizing Zones  76
   Zone Commands  76
   Importing and Exporting Zone Data  77
   Configuring Primary Reverse Zones  79
      Related Topics  79
Chapter 12

Authoritative DNS Metrics 115

DNS Outbound Zone Transfers 115
- How to Interpret the Data 115
- Troubleshooting Based on the Results 115

DNS Inbound Zone Transfers 116
- How to Interpret the Data 116
- Troubleshooting Based on the Results 116

DNS Network Errors 116
- How to Interpret the Data 117
- Troubleshooting Based on the Results 117

DNS Related Servers Errors 117
- How to Interpret the Data 117
- Troubleshooting Based on the Results 117

DNS General Indicators 117
- How to Interpret the Data 118
- Troubleshooting Based on the Results 118

DNS Queries Per Second 118

Appendix A

Resource Records 119
PART

Introduction

• Introduction to the Domain Name System, on page 1
• DNS Server Status Dashboard, on page 9
Introduction to the Domain Name System

The Domain Name System (DNS) handles the growing number of Internet users. DNS translates names, such as www.cisco.com, into IP addresses, such as 192.168.40.0 (or the more extended IPv6 addresses), so that computers can communicate with each other. DNS makes using Internet applications, such as the World Wide Web, easy. The process is as if, when phoning your friends and relatives, you could autodial them based on their names instead of having to remember their phone numbers.

- How DNS Works, on page 1
- Overview of Concepts in DNS, on page 2
- Domains, on page 2
- Nameservers, on page 4
- Reverse Nameservers, on page 6
- Authoritative and Caching DNS servers, on page 6
- High-Availability DNS, on page 6
- EDNS, on page 6
- DNS Views, on page 7

How DNS Works

To understand how DNS works, imagine a typical user, John, logging in to his computer. He launches his web browser so that he can view the website at a company, ExampleCo (see the image below). He enters the name of their website—http://www.example.com. Then:

1. John’s workstation sends a request to the DNS server about the IP address of www.example.com.
2. The DNS server checks its database to find that www.example.com corresponds to 192.168.1.4.
3. The server returns this address to John’s browser.
4. The browser uses the address to locate the website.
5. The browser displays the website on John’s monitor.
Overview of Concepts in DNS

This section provides an overview of the concepts in DNS.

Domains

John can access the ExampleCo website because his DNS server knows the www.example.com IP address. The server learned the address by searching through the domain namespace. DNS was designed as a tree structure, where each named domain is a node in the tree. The top-most node of the tree is the DNS root domain (.), under which there are subdomains, such as .com, .edu, .gov, and .mil (see the image below).

The fully qualified domain name (FQDN) is a dot-separated string of all the network domains leading back to the root. This name is unique for each host on the Internet. The FQDN for the sample domain is example.com., with its domain example, parent domain .com, and root domain "." (dot).

Learning ExampleCo Address

When John’s workstation requests the IP address of the website www.example.com (see the image below):
1. The local DNS server looks for the www.example.com domain in its database, but cannot find it, indicating that the server is not authoritative for this domain.
2. The server asks the authoritative root nameserver for the top-level (root) domain “.” (dot).
3. The root nameserver directs the query to a nameserver for the .com domain that knows about its subdomains.
4. The .com nameserver determines that example.com is one of its subdomains and responds with its server address.
5. The local server asks the example.com nameserver for the www.example.com location.
6. The example.com nameserver replies that its address is 192.168.1.4.
7. The local server sends this address to John’s Web browser.

Establishing a Domain

ExampleCo has a website that John could reach because it registered its domain with an accredited domain registry. ExampleCo also entered its domain name in the .com server database, and requested a network number, which defines a range of IP addresses.

In this case, the network number is 192.168.1.0, which includes all assignable hosts in the range 192.168.1.1 through 192.168.1.254. You can only have numbers 0 through 255 (28) in each of the address fields, known as octets. However, the numbers 0 and 255 are reserved for network and broadcast addresses, respectively, and are not used for hosts.

Difference Between Domains and Zones

The domain namespace is divided into areas called zones that are points of delegation in the DNS tree. A zone contains all domains from a certain point downward, except those for which other zones are authoritative.

A zone usually has an authoritative nameserver, often more than one. In an organization, you can have many nameservers, but Internet clients can query only those that the root nameservers know. The other nameservers answer internal queries only.

The ExampleCo company registered its domain, example.com. It established three zones—example.com, marketing.example.com, and finance.example.com. ExampleCo delegated authority for marketing.example.com and finance.example.com to the DNS servers in the Marketing and Finance groups in the company. If someone queries example.com about hosts in marketing.example.com, example.com directs the query to the marketing.example.com nameserver.

In the image below, the domain example.com includes three zones, with the example.com zone being authoritative only for itself.
ExampleCo could choose not to delegate authority to its subdomains. In that situation, the example.com domain is a zone that is authoritative for the subdomains for marketing and finance. The example.com server answers all outside queries about marketing and finance.

As you begin to configure zones by using Cisco Prime Network Registrar, you must configure a nameserver for each zone. Each zone has one primary server, which loads the zone contents from a local configuration database. Each zone can also have any number of secondary servers, which load the zone contents by fetching the data from the primary server. The image below shows a configuration with one secondary server.

**Nameservers**

DNS is based on a client/server model. In this model, nameservers store data about a portion of the DNS database and provide it to clients that query the nameserver across the network. Nameservers are programs that run on a physical host and store zone data. As administrator for a domain, you set up a nameserver with the database of all the resource records (RRs) describing the hosts in your zone or zones (see the image below).
The DNS servers provide name-to-address translation, or name resolution. They interpret the information in a fully qualified domain name (FQDN) to find its address.

Each zone must have one primary nameserver that loads the zone contents from a local database, and a number of secondary servers, which load a copy of the data from the primary server (see the image below). This process of updating the secondary server from the primary server is called a zone transfer.

Even though a secondary nameserver acts as a kind of backup to a primary server, both types of servers are authoritative for the zone. They both learn about hostnames in the zone from the zone authoritative database, not from information learned while answering queries. Clients can query both servers for name resolution.

As you configure the Cisco Prime Network Registrar DNS nameserver, you specify what role you want the server to perform for a zone—primary, secondary, or caching-only. The type of server is meaningful only in context to its role. A server can be a primary for some zones and a secondary for others. It can be a primary or secondary only, or it can serve no zones and just answer queries by means of its cache.

In Cisco Prime Network Registrar, the authoritative and caching services are separated and are handled by two separate servers. The authoritative server holds authoritative zone data and responds only to queries for which it is authoritative. The caching server is the recursive/caching server and does not contain any authoritative zone data.

To configure the:

- Primary nameserver, see Managing Primary DNS Servers, on page 70.
- Secondary nameserver, see Managing Secondary Servers, on page 82.
Reverse Nameservers

The DNS servers described so far perform name-to-address resolution. They can do this easily by searching through their database for the correct address, because they index all the data by name. However, there are times when you need address-to-name resolution so that you can interpret certain output, such as computer log files.

Finding a domain name when you only know the address, however, would require searching the entire namespace. DNS solves this problem by supporting a domain namespace that uses addresses as names, known as the in-addr.arpa or .arpa domain. This reverse zone contains subdomains for each network based on the network number. For consistency and natural grouping, the four octets of a host number are reversed.

The IP address as a domain name appears backward, because the name is in leaf-to-root order. For example, the ExampleCo example domain network number is 192.168.1.0. Its reverse zone is 1.168.192.in-addr.arpa. If you only know the DNS server address (192.168.1.1), the query to the reverse domain would find the host entry 1.1.168.192.in-addr.arpa that maps to example.com.

Reverse domains are handled through Pointer (PTR) RRs, as indicated in the image below.

Figure 8: Reverse Domains

Authoritative and Caching DNS servers

Starting from release 8.0, the DNS server functionality is enhanced to provide separate DNS servers for authorization and caching. With this enhancement, Cisco Prime Network Registrar supports DNS64, DNSSEC, Domain Redirect, full IPv6, and has improved caching performance.

High-Availability DNS

Because there can be only one primary DNS server per zone, failure of this server makes it impossible to update the zone data. These updates can occur on the primary DNS server only; software such as DHCP servers, that update DNS resource records must send the updates directly to the primary. A second primary server can become a hot standby that shadows the main primary. This is called High-Availability (HA) DNS.

EDNS

To send a DNS message above 512 bytes over UDP, you need to use an extension of the DNS protocol known as Extended DNS (EDNS). The EDNS protocol expands the number of flags, label types, and return codes available to the DNS protocol. A version of EDNS specified by RFC 6891 is known as EDNS0. EDNS uses a pseudo resource record known as OPT Resource Record (OPT RR). OPT RR differentiates conventional DNS from EDNS. OPT RRs appear only in the route transmission between DNS clients and servers, they are...
not cached or persisted to disk. A DNS endpoint that marks a DNS packet as EDNS must insert an OPT RR in the additional data section of the DNS request or response.

The Authoritative and the Caching DNS servers support the EDNS0 extension, but no option codes. You can modify the UDP payload size of the DNS server. The minimum UDP payload size of the DNS server is 512 bytes. The maximum UDP packet size is 64 KB, the default and recommended size for the Caching server is 4 KB.

---

**Note**

The DNS Server can handle requests from clients that do not support EDNS0, however, the DNS server is not permitted to use any extended capabilities, when it handles requests from clients that do not support EDNS0. The response to client requests are inserted into a default 512 byte message. Clients may indicate that they support EDNS by including an OPT RR in the query. If a server does not support EDNS (or the support is disabled), the server will return FORMERR and the client retries without EDNS. If an answer is larger than the size that the client has reported (either with EDNS or the default 512 bytes), the server will mark the result as truncated and the client may retry using TCP.

---

**DNS Views**

DNS views allows you to present alternate versions of zone data to different communities of clients using a single name server.

For example, a DNS server for example.com could maintain two views of the zone, where the view of example.com that can be queried internally includes many hosts that do not exist in the external view. Each zone view is treated as an independent copy of the zone. The DNS server, when answering queries on the zone, uses the match criteria defined in each view to determine the matching zone for the client. The query is then answered based on that zone contents. In some cases, the zone contents may only vary slightly between views.

---

**Note**

Cisco Prime Network Registrar 8.2 and later support the DNS views.
DNS Server Status Dashboard

The Cisco Prime Network Registrar status dashboard in the web user interface (web UI) presents a graphical view of the system status, using graphs, charts, and tables, to help in tracking and diagnosis. These dashboard elements are designed to convey system information in an organized and consolidated way, and include:

- Significant protocol server and other metrics
- Alarms and alerts
- Database inventories
- Server health trends

The dashboard is best used in a troubleshooting desk context, where the system displaying the dashboard is dedicated for that purpose and might be distinct from the systems running the protocol servers. The dashboard system should point its browser to the system running the protocol servers.

You should interpret dashboard indicators in terms of deviations from your expected normal usage pattern. If you notice unusual spikes or drops in activity, there could be communication failures or power outages on the network that you need to investigate.

- Opening the Dashboard, on page 9
- Display Types, on page 9
- Customizing the Display, on page 14
- Selecting Dashboard Elements to Include, on page 16

Opening the Dashboard

To open the dashboard in the local web UI, from the Operate menu, choose Dashboard.

Display Types

Provided you have DNS and Caching DNS privileges through administrator roles assigned to you, the preset display of the dashboard consists of the following tables (See the table below for an example):

- System Metrics—See the "System Metrics" section in Cisco Prime Network Registrar 8.3 Administrator Guide.
General Status Indicators

- **DNS General Indicators**—See Caching DNS Metrics, on page 37 and Authoritative DNS Metrics, on page 115.

---

**Tip**

These are just the preset selections. See Selecting Dashboard Elements to Include, on page 16 for other dashboard elements you can select. The dashboard retains your selections from session to session.

---

**Figure 9: Preset Dashboard Elements**

Each dashboard element initially appears as a table or a specific chart type, depending on the element:

- **Table**—See Tables, on page 11.
- **Line chart**—See Line Charts, on page 11.
- **Stacked area chart**—See Stacked Area Charts, on page 13.

---

General Status Indicators

Note the green box next to each dashboard element name in the above image. This box indicates that the server sourcing the information is functioning normally. A yellow box indicates that server operation is less than optimum. A red box indicates that the server is down. These indicators are the same as for the server health on the Manage Servers page in the regular web UI.

---

Graphic Indicators for Levels of Alert

Graphed lines and stacked areas in the charts follow a standard color and visual coding so that you can immediately determine key diagnostic indicators at a glance. The charts use the following color and textural indicators:

- **High alerts or warnings**—Lines or areas in red, with a hatched texture.
- **All other indicators**—Lines or areas in various other colors distinguish the data elements. The charts do not use green or yellow.
Magnifying and Converting Charts

If Magnified Chart is the selected Chart Link, you can magnify a chart in a separate window by clicking the chart. In magnified chart view, you can choose an alternative chart type from the one that comes up initially (see the Other Chart Types section).

**Note**
Automatic refresh is turned off for magnified charts. To get the most recent data, click the Refresh icon next to the word Dashboard at the top left of the page.

To convert a chart to a table, see “Displaying Charts as Tables”. You cannot convert tables to a graphic chart format.

Legends

Each chart initially includes a color-coded legend. To turn off the legend display on the main dashboard page, see the "Displaying or Hiding Chart Legends" section. Removing the legend renders the graphic chart size relatively larger, which can be helpful if you have many charts displayed. You cannot remove legends in magnified views.

Tables

Dashboard elements rendered as tables have data displayed in rows and columns. The following dashboard elements are preset to consist of (or include) tables:

- System Metrics
- DHCP DNS Updates
- DHCP Address Current Utilization
- DHCP General Indicators
- DNS General Indicators
- Caching DNS General Indicators

**Note**
If you view a table in Expert mode, additional data might appear.

Line Charts

Dashboard elements rendered as line charts can include one or more lines plotted against the x and y axes. The three types of line charts are described in the following table.
### Table 1: Line Chart Types

<table>
<thead>
<tr>
<th>Type of Line Chart</th>
<th>Description</th>
<th>Dashboard Elements Rendered</th>
</tr>
</thead>
</table>
| Raw data line chart | Lines plotted against raw data. | • Java Virtual Machine (JVM) Memory Utilization (Expert mode only)  
• DHCP Buffer Capacity  
• DHCP Failover Status (two charts)  
• DNS Network Errors  
• DNS Related Servers Errors |
| Delta line chart | Lines plotted against the difference between two sequential raw data. | • DNS Inbound Zone Transfers  
• DNS Outbound Zone Transfers |
| Rate line chart | Lines plotted against the difference between two sequential raw data divided by the sample time between them. | • DHCP Server Request Activity (see the image below)  
• DHCP Server Response Activity  
• DHCP Response Latency  
• DNS Query Responses  
• DNS Forwarding Errors |

**Tip**
To get the raw data for a chart that shows delta or rate data, enter Expert mode, set the Chart Link to Data Table (see Customizing the Display, on page 14), then click the chart. The Raw Data table is below the Chart Data table.
Stacked Area Charts

Dashboard elements rendered as stacked area charts have multiple related metrics plotted as trend charts, but stacked one on top of the other, so that the highest point represents a cumulative value. The values are independently shaded in contrasting colors. (See the image below for an example of the DHCP Server Request Activity chart shown in Line Charts, on page 11 rendered as a stacked area chart.)

They are stacked in the order listed in the legend, the left-most legend item at the bottom of the stack and the right-most legend item at the top of the stack. The dashboard elements that are pre-set to stacked area charts are:

- DHCP Server Request Activity
- DHCP Server Response Activity
Other Chart Types

The other chart types available for you to choose are:

- **Line**
  — One of the line charts described in Line Charts, on page 11.

- **Stacked Area**—Charts described in the Stacked Area Charts, on page 13.

- **Pie**—Shows a single percentage pie chart of the data averaged over the time sampled.

- **Bar**—Multiple related current value metrics plotted side by side as groups of bars that show the actual data sampled.

- **Stacked Bar**—Addition total of the actual samples. This chart shows more distinct data points than the stacked area chart.

---

**Tip**

Each chart type shows the data in distinct ways and in different interpretations. You can decide which type best suits your needs.

---

Getting Help for the Dashboard Elements

You can open a help window for each dashboard element by clicking the title of the element.

Customizing the Display

To customize the dashboard display, you can:

- Refresh the data and set an automatic refresh interval.
- Expand a chart and render it in a different format.
- Convert a graphic chart to a table.
- Download data to comma-separated value (CSV) output.
- Display or hide chart legends.
- Configure server chart types.
- Reset to default display

Each chart supports:

- Resizing
• Drag and drop to new cell position
• Minimizing
• Closing

Each chart has a help icon with a description of the chart and a detailed help if you click the chart title.

---

**Note**

The changes made to the dashboard/chart will persist only if you click **Save** in the Dashboard window.

---

### Refreshing Displays

Refresh each display so that it picks up the most recent polling by clicking the **Refresh** icon.

### Setting the Polling Interval

You can set how often to poll for data. Click the **Dashboard Settings** icon in the upper-right corner of the dashboard display. There are four options to set the polling interval of the cached data, which polls the protocol servers for updates. (See the below image)

*Figure 12: Setting the Chart Polling Interval*

You can set the cached data polling (hence, automatic refresh) interval to:

- **Disabled** — Does not poll, therefore does not automatically refresh the data.
- **Slow** — Refreshes the data every 30 seconds.
- **Medium** — Refreshes the data every 20 seconds.
- **Fast** (the preset value) — Refreshes the data every 10 seconds.

### Displaying Charts as Tables

You can choose to display a graphic chart as a table when you magnify the chart by clicking it. At the middle of the top of the dashboard display are the controls for the chart links (see the image below)

*Figure 13: Specifying Chart Conversion to Table Format*

Click the **Data Table** radio button. When you click the chart itself, it opens as a table. The preset display format is Magnified Chart.
Exporting to CSV Format

You can dump the chart data to a comma-separated value (CSV) file (such as a spreadsheet) when you magnify the chart by clicking it. In the Chart Link controls at the top of the page, click the CSV Export radio button, then click the chart. A Save As window appears, where you can specify the name and location of the CSV file.

Displaying or Hiding Chart Legends

You can include or exclude the color-coded legends for charts on the main dashboard page. You might want to remove the legends as you become more familiar with the data and track it on a slightly larger chart display. In the upper-right of the dashboard display are the controls for the legend display (see the image below). The preset value is Visible.

Selecting Dashboard Elements to Include

You can decide how many dashboard elements you want to display on the page. At times, you might want to focus on one server activity only, such as for the DHCP server, and exclude all other metrics for the other servers. In this way, the dashboard becomes less crowded, the elements are larger and more readable. At other times, you might want an overview of all server activities, with a resulting smaller element display.

You can select the dashboard elements to display from the main Dashboard page by clicking Chart Selections in the Dashboard Settings dialog (see Figure 15: Selecting Dashboard Elements, on page 17). Clicking the link opens the Chart Selection page (see the figure Selecting Dashboard Elements).

Configuring Server Chart Type

You can set the default chart types on the main dashboard view. You can customize the server charts in the dashboard to display only the specific chart types as default.

To set up default chart type, check the check box corresponding to the Metrics chart that you want to display and choose a chart type from the Type drop-down list. The default chart types are consistent and shared across different user sessions (see the image below).

---

**Note**

You can see either the CDNS or DNS Metrics in the Dashboard Settings > Chart Selection page based on the service configured on the server.

---

**Tip**

The order in which the dashboard elements appear in the Chart Selection list does not necessarily determine the order in which the elements will appear on the page. An algorithm that considers the available space determines the order and size in a grid layout. The layout might be different each time you submit the dashboard element selections. To change selections, check the check box next to the dashboard element that you want to display.
To change selections, check the check box next to the dashboard element that you want to display. Specific group controls are available in the drop-down list, Chart Selection, at the top of the page. To:

- Uncheck all check boxes, choose None.
- Revert to the preset selections, choose Default. The preset dashboard elements for administrator roles supporting DHCP and DNS are:
  - Host Metrics: System Metrics
  - DHCP Metrics: General Indicators
  - DNS Metrics: General Indicators
- Select the DHCP metrics only, choose DHCP (see the "DHCP Metrics" section in Cisco Prime Network Registrar 8.3 DHCP User Guide).
- Select the DNS metrics only, choose DNS (see the "Dashboard and Authoritative DNS Metrics" section in Cisco Prime Network Registrar 8.3 Authoritative and Caching DNS Guide).
- Select the DNS metrics only, choose CDNS (see the "Caching DNS Metrics" section in Cisco Prime Network Registrar 8.3 Authoritative and Caching DNS Guide).
- Select all the dashboard elements, choose All.

Click Save at the bottom of the page to save your choices, or Cancel to cancel the changes.
PART II

Caching DNS Server

• Managing Caching DNS Server, on page 21
• Advanced Caching DNS Server, on page 31
• Caching DNS Metrics, on page 37
Managing Caching DNS Server

This chapter explains how to set the Caching DNS server parameters. Before you proceed with the tasks in this chapter, see Introduction to the Domain Name System, on page 1 which explains the basics of DNS.

- Configuring CDNS Server Network Interfaces, on page 21
- Setting DNS Caching Server Properties, on page 21
- Running DNS Caching Server Commands, on page 29

Configuring CDNS Server Network Interfaces

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

Local Advanced Web UI

Step 1 From the Operate menu, choose Manage Servers under the Servers submenu.
Step 2 Select Local CDNS Server from the Manage Servers pane.
Step 3 Click the Network Interfaces tab 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 Click the name of the configured interface to edit the configured interfaces, where you can change the address, direction 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 Network Interfaces page.

Setting DNS Caching Server Properties

You can set properties for the Caching DNS server. These include:

- General server properties—See Setting General CDNS Server Properties, on page 22
- Log Settings—See Specifying Log Settings, on page 22
Setting General CDNS Server Properties

You can view CDNS general server properties, such as log settings, basic cache settings, SNMP traps, and root nameservers.

The following subsections describe some of the most common property settings. They are listed in Setting DNS Caching Server Properties, on page 21.

Local Basic or Advanced Web UI

Step 1 To access the server properties, choose CDNS Server from the Deploy > DNS submenu to open the Manage DNS Caching Server page.

Step 2 Select Local CDNS Server from the CDNS Server pane, to open the Edit Local CDNS Server page. The page displays all the CDNS server attributes.

Step 3 Click Save to save the CDNS server attribute modifications.

CLI Commands

Use cdns show to display the CDNS server properties (see the cdns command in the CLIGuide.html file in the /docs directory for syntax and attribute descriptions).

Specifying Log Settings

This setting determines which detailed events the Caching DNS server logs, as set using a bit mask. Logging these additional details can help analyze a problem. Leaving detailed logging enabled for a long period, however, can fill the log files and cause the loss of important information.

The possible options are:

- **config**—Controls logging pertaining to server configuration and server de-initialization (unconfiguration).
• **server-ops**—Controls high level logging of server operations.
• **server-detailed-ops**—Controls detailed logging of server operations.
• **scp**—Controls logging pertaining to SCP message processing.
• **activity-summary**—This causes a summary message to appear at an interval specified by activity-summary-interval. The summary provides detailed statistics about the server's operation.
• **query**—Causes logging of all DNS queries to the server.

### Specifying Activity Summary Settings

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.

The Caching DNS server logs sample and/or total statistics based on the option you check for the attribute Statistics Type (`activity-summary-type`).

The `Activity-summary-interval` attribute has a default value of 60 seconds. The default `Activity-summary-type` is sample.

The option checked for the attribute Statistics Settings (`activity-summary-settings`) determines the category of statistics that is logged as part of activity summary. The possible settings are:

- **query**—Logs statistics related to incoming queries.
- **query-type**—Logs statistics on the RR types that are being queried.
- **cache**—Logs statistics on the RR cache.
- **resol-queue**—Logs statistics on the resolution queue.
- **responses**—Logs statistics about query responses.
- **memory**—Logs statistics on memory usage.
- **firewall**—Logs statistics on DNS firewall usage.

### Setting Prefetch Timing

Use the `Prefetch` attribute to set whether message cache elements should be prefetched before they expire to keep the cache up to date. Turning it **on** gives about 10 percent more traffic and load on the machine, but can increase the query performance for popular DNS names.

When prefetch is enabled, records are assigned a prefetch time that is within 10 percent of the expiration time. As the server processes client queries and looks up the records, it checks the prefetch time. Once the record is within 10 percent of its expiration, the server will issue a query for the record in order to keep it from expiring.
Setting Cache TTLs

TTL is the amount of time that any nameserver is allowed to cache data learned from other nameservers. Each record added to the cache arrives with some TTL value. When the TTL period expires, the server must discard the cached data and get new data from the authoritative nameservers the next time it sends a query. TTL attributes, `cache-min-ttl` and `cache-max-ttl` defines the minimum and the maximum time Cisco Prime Network Registrar retains the cached information. These parameters limit the lifetime of records in the cache whose TTL values are very large.

Local Basic or Advanced Web UI

Step 1  On the Edit Local CDNS Server tab, you can find:
- the Maximum Cache TTL (`cache-max-ttl`) attribute, set it to the desired value (the default value is 24 hours)
- the Min Cache TTL (`cache-min-ttl`) attribute, set it to the desired value (the preset value is 0)

Step 2  Click Save to save the changes.

CLI Commands

Use:
- `CDNS set cache-max-ttl` to set the Maximum Cache TTL.
- `CDNS set cache-min-ttl` to set the Minimum Cache TTL.

Defining Root Nameservers

Root nameservers know the addresses of the authoritative nameservers for all the top-level domains. When you first start a newly installed Cisco Prime Network Registrar Caching DNS server, it uses a set of preconfigured root servers, called root hints, as authorities to ask for the current root nameservers.

When Cisco Prime Network Registrar gets a response to a root server query, it caches it and refers to the root hint list. When the cache expires, the server repeats the process. The time to live (TTL) on the official root server records is preconfigured and you can specify a different cache TTL value, (see Setting Cache TTLs, on page 24).

Because the configured servers are only hints, they do not need to be a complete set. You should periodically (every month to six months) look up the root servers to see if the information needs to be altered or augmented.

Local Basic or Advanced Web UI

On the Edit Local CDNS Server tab, under the Root Name Servers category, enter the domain name and IP address of each additional root nameserver, clicking Add Root Namerserver after each one, then click Save.

CLI Commands

Use `cdns addRootHint`.

Cisco Prime Network Registrar 8.3 Caching and Authoritative DNS User Guide
Dynamic Allocation of UDP Ports

The Caching DNS server uses a large number of UDP port numbers, by default approximately 60000 port numbers. These numbers are divided among the processing threads. The large number of port numbers reduce the risk of cache poisoning via Birthday Attacks. The Caching DNS server uses the default pool of UDP ports (2048) and the maximum allowable size of the default pool of UDP ports is 4096.

Currently, Cisco Prime Network Registrar uses the port range from 1024 to 65535. Based on the number of outstanding resolution queries, the Caching DNS server adjusts the pool size by adding or removing ports. The Caching DNS server allocates and releases the UDP ports dynamically when the server is running. If you reload the server, all the UDP ports are released and randomly picked again.

Cisco Prime Network Registrar uses outgoing-range-avoid attribute that allows you to define ports or ranges of ports that will be excluded from use by the DNS server when sending queries.

Note
You need to ensure that UDP ports needed by other applications are in the port exclusion list. Otherwise, these applications may not be able bind to their port(s) if the DNS server is using the port.

Local Basic or Advanced Web UI

On the Edit Local CDNS Server tab, expand Additional Attributes to view various attributes and their values. For the query-source-port-exclusion-list attribute value, enter a range of ports that need to be excluded. Then click Modify Server.

Setting Maximum Memory Cache Sizes

The maximum memory cache size property specifies how much memory space you want to reserve for the DNS in-memory cache. The larger the memory cache, the less frequently the Caching DNS server will need to re-resolve unexpired records.

Local Advanced Web UI

On the Edit Local CDNS Server tab, in the Caching category, set it to the desired value for the RRSet Cache Size (rrset-cache-size), then click Save. The default size is 100MB.

To set the size of the message cache, use the Message Cache Size (msg-cache-size) attribute. The message cache stores query responses. It should generally be twice the size of the RRSet Cache Size (rrset-cache-size).

CLI Commands

- Use `cdns set rrset-cache-size` to set RRSet Cache Size.
- Use `cdns set msg-cache-size` to set Message Cache Size.

Specifying Resolver Settings

Glue record(s) is/are A record(s) for name server(s) that cannot be found through normal DNS processing because they are inside the zone they define. When harden-glue is enabled, the Caching DNS server will ignore glue records that are not within the zone that is queried. The harden-glue attribute is on by default.
Specifying Network Settings

The `listen-ip-version` attribute lets you to choose the ip packets to accept and issue. You can check IPv4, IPv6, both, or none. The `listen-protocol` attribute lets you to choose the packet protocol to answer and issue, UDP, TCP, both, or none.

Specifying Advanced Settings

The `minimal-responses` attribute controls whether the DNS Caching server omits or includes records from the authority and data sections of query responses when these records are not required. Enabling this attribute may improve query performance such as when the DNS server is configured as a caching server.

The `remote-ns-host-ttl` attribute lets you to set the time to live for entries in the host entries in the remote name server cache. They contains roundtrip timing and EDNS support information.

The `remote-ns-cache-numhosts` attribute lets you to set the number of hosts for which information is cached.

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 Advanced Web UI

On the Manage DNS Caching Server page, under the Advanced Settings section, find the Enable round-robin (`round-robin`) attribute.

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`.

Flushing CDNS Cache

The Cisco Prime Network Registrar cache flushing function lets you remove all or a portion of cached data in the memory cache of the server.

Local Basic or Advanced Web UI

**Step 1**

From the **Deploy** menu, choose **CDNS Server** under the **DNS** submenu, to open the Manage DNS Caching Server page.

**Step 2**

On the Manage DNS Caching Server page, click the **Commands** link to open the CDNS Command dialog box. There will be two types of cache flushing commands.

- **Flush the CDNS cache**—allows you to either flush all cache entries for a particular zone or the entire cache if no zone is provided. To remove all data for a specific zone, enter the zone name in the **Zone** field. To clear the whole cache, leave the **Zone** field empty.
- **The Flush Resource Record**—allows you to flush an RR name or an RRSet when the type field is specified.
• Remove common RR types (A, AAAA, NS, SOA, CNAME, DNAME, MX, PTR, SRV, NAPTR, and TXT) from a specific domain—enter the required RR name as the FQDN for the Flush Resource Record command and leave the RR type field empty.
• Remove a specified RR type for a domain—specify the domain in the FQDN field, and the RR type in the RR type field.

Note When no type is specified, the server flushes types A, AAAA, NS, SOA, CNAME, DNAME, MX, PTR, SRV, TXT, and NAPTR.

CLI Commands

To:

• Remove all cached entries at or below a given domain, use `cdns flushCache domain` . If no domain is given, it flushes all RR in the cache.
• Flush RRs from the cache associated with the given RR name, use `cdns flushName name type` . When type is provided, it flushes all entries with the given name and type. If no type if provided, it flushes types A, AAAA, NS, SOA, CNAME, DNAME, MX, PTR, SRV, TXT, and NAPTR.

Detecting and Preventing DNS Cache Poisoning

Cisco Prime Network Registrar enhances the CDNS server performance to address the CDNS related issues such as DNS cache poisoning attacks (CSCsq01298), as addressed in a Cisco Product Security Incident Response Team (PSIRT) document number PSIRT-107064 with Advisory ID cisco-sa-20080708-dns, available at:

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080708-dns

DNS Cache Poisoning Attacks

A cache poisoning attack can change an existing entry in the DNS cache as well as insert a new invalid record into the DNS cache. This attack causes a hostname to point to the wrong IP address. For example, let us say that www.example.com is mapped to the IP address 192.168.0.1, and this mapping is present in the cache of a DNS server. An attacker can poison the DNS cache and map www.example.com to 10.0.0.1. If this happens, if you try to visit www.example.com, you will end up contacting the wrong web server.

A DNS server that uses a single static port for receiving responses to forwarded queries are susceptible to malicious clients sending forged responses.

The DNS transaction ID and source port number used to validate DNS responses are not sufficiently randomized and can easily be predicted, which allows an attacker to create forged responses to DNS queries. The DNS server will consider such responses as valid.

Handling DNS Cache Poisoning Attacks

To reduce the susceptibility to the DNS cache poisoning attack, the DNS server randomizes the UDP source ports used for forwarded queries. Also, a resolver implementation must match responses to the following attributes of the query:

• Remote address.
• Local address.
• Query port.
• Query ID.
• Question name (not case-sensitive).
• Question class and type, before applying DNS trustworthiness rules (see [RFC2181], section 5.4.1).

The response source IP address must match the query's destination IP address and the response destination IP address must match the query's source IP address. A mismatch must be considered as format error, and the response is invalid.

Resolver implementations must:

• Use an unpredictable source port for outgoing queries from a range (either 53, or > 1024) of available ports that is as large as possible and practicable.
• Use multiple different source ports simultaneously in case of multiple outstanding queries.
• Use an unpredictable query ID for outgoing queries, utilizing the full range available (0 to 65535). By default, CDNS uses about 60000 port numbers.

The Expert mode Caching DNS server setting randomize-query-case, when enabled, specifies that when sending a recursive query, the query name is pseudo-randomly camel-cased and the response is checked to see if this camel-casing is unchanged. If randomize-query-case is enabled and the casing has changed, then the response is discarded. The randomize-query-case is disabled by default, disabling this feature.

Local Basic or Advanced Web UI

The DNS server statistics appears on the Statistics tab of the Manage DNS Caching Server Statistics page. The Statistics displays the answers-unwanted values. You can refresh the DNS Caching Server Statistics.

Handling Unresponsive Nameservers

When trying to resolve query requests, Caching DNS servers may encounter unresponsive nameservers. A nameserver may be unresponsive to queries, respond late. This affects the performance of the local DNS server and remote nameservers.

Using Cisco Prime Network Registrar, you can resolve these problems by barring unresponsive nameservers. You can configure a global ACL of unresponsive nameservers that are to be barred, using the acl-do-not-query attribute.

When Cisco Prime Network Registrar receives a list of remote nameservers to transmit a DNS query request to, it checks for the name-servers listed in the acl-do-not-query list and removes them from this list. Conversely, all incoming DNS requests from clients or other nameservers are also filtered against the acl-blacklist.

Using the acl-do-not-query does not affect the configuration of communication with certain servers such as forwarders.

Use the acl-query attribute to specify which clients are allowed to query the server. By default any client is allowed to query the server. A client that is not in this list will receive a reply with status REFUSED. Clients on the acl-blacklist do not get any response whatsoever.
Local Advanced Web UI

On the Edit Local CDNS Caching Server tab, expand **Query Access Control** to view the various attributes and their values. For the Do Not Query (acl-do-not-query) attribute value, enter, for example, 10.77.240.73. Then click **Save**.

Running DNS Caching Server Commands

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

- **Flush the CDNS cache**— This command allows you to flush either all RRs or RRs for a particular zone from the in-memory cache. See Flushing CDNS Cache, on page 26
- **Flush Resource Record**— This command that lets you specify an RR name and optionally a type to remove from the in-memory cache.

---

**Note**

To remove all the entries from the in-memory cache, you need to reload the CDNS server.

---

**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.
CHAPTER 4

Advanced Caching DNS Server

This chapter explains how to set the Caching DNS parameters for the advanced features of the server. Before you proceed with the tasks in this chapter, see Introduction to the Domain Name System, on page 1 which explains the basics of DNS.

- Defining Forwarders, on page 31
- Using Exceptions, on page 32
- Managing DNS64, on page 33
- Managing DNSSEC, on page 34
- Setting up Caching DNS and Authoritative DNS Server on Same Operating System, on page 35
- Managing DNS Firewall, on page 35

Defining Forwarders

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

**Note**

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

**Tip**

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

Local Basic or Advanced Web UI

To define a forwarder:

**Step 1**

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

**Step 2**

Click the **Add Forwarders** icon in the **Forwarders** pane to open the Add DnsForwarder dialog box.

**Step 3**

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

**Note**

To use a forwarder for all external queries, create a forwarder with the name ".".
Step 4  
In the Edit Forwarders page, enter the hostname, and click **Add Host** and enter the IP address for the forwarder then click **Add Address**.

Step 5  
Click **Save**.

---

**CLI Commands**

Use the following `cdns` commands to:

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

---

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

---

**Using Exceptions**

If you do not want the CDNS server to use the standard resolution method to query the nameserver for certain domains, use exceptions. This bypasses the root nameservers and targets a specific server (or list of servers) to handle name resolution.

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

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

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

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

---

**Note**  
Exceptions can contain both IPv4 and/or IPv6 addresses and require a CDNS server reload to take effect.

---

**Local Basic or Advanced Web UI**

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

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

**Step 3**  
In the name field, enter the domain or zone for which an exception is wanted and click **Add DnsException**.
Step 4  In the Edit Exceptions page, enter the hostname in the DNS Name field and click Add Host. To address, enter the IP address in the IP Address field and click Add Address.

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

Step 6  Click Save.

Deleting Exception List

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

CLI Commands

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

Use the following cdns commands to:

- Add the resolution exception domains and the IP addresses of servers, separated by spaces, use cdns addException domain [prime=on|off] [views=on|off] addr. The addresses can be IPv4 or IPv6 with an optional port number (i.e. <addr>[@<port>]) or the name of a server (it must be possible to resolve the server name before it is used). Use this command only if you do not want your DNS Caching server to use the standard name resolution for a zone.
- List the domains that are configured to have exceptional resolution of their names, use cdns listExceptions.
- Remove an entry for exceptional resolution of addresses within a domain, use cdns removeException.
  You can remove an individual server by specifying it, or the exception itself by just specifying its name.
- Replace an exception, you must first remove the current exception and then add a new one.

For any change to resolution exceptions to take effect, you must restart the CDNS server.

Managing DNS64

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

In Cisco Prime Network Registrar 8.3 and later, you can define multiple prefixes for synthesizing AAAA record.

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

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

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

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

**Step 3**  
Enter the Name for the DNS64 configuration item.

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

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

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

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

---

**CLI Commands**

To create DNS64 in the Caching DNS server, use cdns64 <name>create <acl-match-clients>=<ACL> prefix=<IPv6 prefix>. (see the cdns64 command in the CLIGuide.html file in the /docs directory for syntax and attribute descriptions).

---

**Managing DNSSEC**

DNSSEC enables the server to determine the security status of all Resource Records that are retrieved. You can manage DNSSEC only in the Advanced mode. The dnssec attribute enables validation of DNS information.

The domain-insecure attribute defines domain names to be insecure, DNSSEC chain of trust is ignored towards the domain names. So, a trust anchor above the domain name can not make the domain secure with a DS record, such a DS record is then ignored. DNSSEC requires a root trust anchor to establish trust for the DNS root servers. The initial DNSSEC root trust anchor, root.anchor, is stored in the .../data/cdns directory and is the default value of the auto-trust-anchor-file attribute. Additional trust anchors may be added by adding them to the .../data/cdns directory and to the auto-trust-anchor-file if the zone supports automated updates according to RFC 5011 or the trust-anchor-file attribute if not. The cdnssec command controls and configures DNSSEC processing in the Cisco Prime Network Registrar DNS Caching server.

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

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

---

**Note**  
If DNS64 is enabled, enabling DNSSEC is not recommended. DNS64 causes responses to be simulated which may cause DNSSEC validation to fail.
Local Basic or Advanced Web UI

Step 1  From the Design menu, choose DNSSEC under the Security submenu to open the Manage DNSSEC page.
Step 2  Enable DNSSEC validation by selecting the enabled option.
Step 3  The page displays all the DNSSEC attributes. Modify the attributes as per your requirements.
Step 4  Click Save to save your settings.

CLI Commands

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

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

In Cisco Prime Network Registrar 8.3 and later, both the Caching DNS and Authoritative DNS servers can run on the same operating system, without the need for two separate virtual or physical machines. For more information on DNS firewall, see Setting up Caching DNS and Authoritative DNS Server on Same Operating System, on page 51.

Managing DNS Firewall

DNS Firewall provide a mechanism control the domain names, IP addresses, and name servers that are allowed to function on the network. For more information on DNS firewall, see Managing DNS Firewall, on page 52.
These Caching DNS metric elements are available in the dashboard:

- DNS Queries Type, on page 37
- DNS Queries Responses, on page 37
- DNS Incoming Queries, on page 38
- DNS Recursive Query Time, on page 38
- DNS Caching, on page 39
- Caching DNS General Indicators, on page 39
- DNS Caching Server Queries Per Second, on page 40

### DNS Queries Type

The DNS Queries Type dashboard element rendered as a line chart traces the number of queries by type. The chart is available if you choose Caching DNS Metrics: DNS Queries Type in the Chart Selection list.

The resulting line chart plots the following trends:

- **A**—Number of A queries received.
- **AAAA**—Number of AAAA queries received.
- **CNAME**—Number of CNAME queries received.

#### How to Interpret the Data

This chart shows the number of incoming queries of type A, AAAA, CNAME, PTR, and others.

### DNS Queries Responses

The CDNS Query Responses dashboard element rendered as line chart shows the number of responses with NOERROR, NODOMAIN, No Data, Other Errors, Secure, and Unsecure return codes. The display is available if you choose Caching DNS Metrics: DNS Queries Responses in the Chart Selection list.

The resulting line chart plots the following trends:

- **NOERROR**—Number of answers from cache or recursion that result in rcode of NOERROR being returned to client.
- **NXDOMAIN**—Number of answers from cache or recursion that result in rcode of NXDOMAIN being returned to client.
• **NODATA**—Number of answers that result in pseudo rcode of NODATA being returned to client.
• **Other Errors**—Other errors.
• **Secure**—Number of answers that correctly validated.
• **Unsecure**—Number of answers that did not correctly validate.

### How to Interpret the Data

This chart shows the following:

- The number of answers to queries, from cache or from recursion, that had the return code NXDOMAIN.
- The number of answers to queries that had the pseudo return code NODATA. This means the actual return code was NOERROR, but additionally, no data was carried in the answer (making what is called a NOERROR/NODATA answer). These queries are also included in the NOERROR number. Common for AAAA lookups when an A record exists, and no AAAA.
- Number of answers that were secure. The answer validated correctly. The AD bit might have been set in some of these answers, where the client signalled (with DO or AD bit in the query) that they were ready to accept the AD bit in the answer.
- Number of answers that did not correctly validate.

In a normal scenario, NOERROR is the successful response code.

### Troubleshooting Based on the Results

Check the CDNS server configuration if the errors are increasing.

### DNS Incoming Queries

The CDNS Incoming queries by dashboard element rendered as a line chart traces the TCP, IPv6, DNSSSEC, EDNS and Total queries. The chart is available if you choose **Caching DNS Metrics: DNS Incoming Queries** in the Chart Selection list.

The resulting line chart plots the following trends:

- **TCP**—Total number of queries received over TCP by the CDNS Server.
- **IPv6**—Total number of queries received over IPv6 by the CDNS Server.
- **EDNS**—Number of queries with EDNS OPT RR present.
- **DNSSEC**—Number of queries with EDNS OPT RR with DO (DNSSEC OK) bit set.
- **Total**—Total number of queries received by the CDNS Server.

### How to Interpret the Data

This chart shows the number of queries that were made using TCP, IPv6, and DNSSEC towards the CDNS server, number of queries that had an EDNS OPT record present, and the total number of queries received.

### DNS Recursive Query Time

The CDNS Queries by Type dashboard element rendered as a line chart traces the average time to complete a recursive query and the median time to complete a query. The table is available if you choose **Caching DNS Metrics: DNS Recursive Query Time** in the Chart Selection list.

The resulting line chart plots the following trends:
• **Average**—The average time to complete a recursive query.
• **Median**—The median time to complete a recursive query.

**How to Interpret the Data**

Average indicates the time the server took to answer queries that needed recursive processing. Note that the queries that were answered from the cache are not in this average.

Median time indicates the median of the time the server took to answer the queries that needed recursive processing. The median means that 50% of the user queries were answered in less than this time. Because of big outliers (usually queries to non-responsive servers), the average can be bigger than the median.

**Troubleshooting Based on the Results**

Check the connectivity and configuration for the name servers as forwarders or exception lists for the increasing values of the average and median time.

**DNS Caching**

The DNS Caching dashboard element rendered as a line chart traces the cache hits and cache misses. The chart is available if you choose **Caching DNS Metrics: DNS Caching** in the Chart Selection list.

The resulting line chart plots the following trends:

• **Cache Hits**—The total number of queries that were answered from cache.
• **Cache Misses**—The total number of queries that were not found in the cache.

**How to Interpret the Data**

This chart indicates the number of queries that were successfully answered using a cache lookup against the number of queries that needed recursive processing.

**Troubleshooting Based on the Results**

If the cache misses are increasing exponentially, check the CDNS logs for errors. Increasing rates of cache misses can indicate that not enough space is available in memory to store the cached queries for more efficient responses.

**Caching DNS General Indicators**

The Caching DNS General Indicators dashboard element shows the server state, its last and startup reload time, and the total resource record (RR) count. The table is available if you choose **Caching DNS Metrics: Caching DNS General Indicators** in the Chart Selection list.

The resulting line chart plots the following trends-test:

• **Server State**—Up or Down (based on whether statistics are available), and how long the server has been in this state.
• **Last Reload**—How long since the last server reload.
• **Start Time**—Date and time of the last server process (Cisco Prime Network Registrar server agent) startup.
How to Interpret the Data

The data in this chart shows general server health and operational duration. The objective is to make decisions about the server, such as whether it might be time for another reload, perhaps warranted by the number of configured zones.

Troubleshooting Based on the Results

If the server state is Down, all the CDNS chart indicators show a red status box, so no data will be available. In the case of a server that is down, restart the server.

DNS Caching Server Queries Per Second

The DNS Caching Server Queries Per Second dashboard element, rendered as chart, displays queries per second for the Caching DNS server. This chart is available if you choose CDNS Metrics: DNS Caching Server Queries Per Second in the Chart Selection page.
PART III

Authoritative DNS Server

• Managing Authoritative DNS Server, on page 43
• Managing High Availability DNS, on page 61
• Managing Zones, on page 69
• Managing DNS Views, on page 97
• Managing Resource Records, on page 101
• Managing Hosts, on page 111
• Authoritative DNS Metrics, on page 115
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, on page 69 which explains how to set up the basic properties of a primary and secondary zone.

- Running DNS Authoritative Server Commands, on page 43
- Setting General DNS Server Properties, on page 45
- Setting Advanced Authoritative DNS Server Properties, on page 48
- Setting up Caching DNS and Authoritative DNS Server on Same Operating System, on page 51
- Managing DNS Firewall, on page 52
- Troubleshooting DNS Servers, on page 57

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, on page 83.
- **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 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, on page 67).
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 45
- **Delegation-only zones**—See Specifying Delegation-Only Zones, on page 45
- **Round-robin server processing**—See Enabling Round-Robin, on page 45
- **Subnet sorting**—See Enabling Subnet Sorting, on page 46
- **Enabling incremental zone transfers**—See Enabling Incremental Zone Transfers (IXFR), on page 46
- **Enabling NOTIFY packets**—See Enabling NOTIFY, on page 47

**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 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 44.

Local Basic or Advanced Web UI

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>To access the server properties, choose <strong>DNS Server</strong> from the <strong>Deploy</strong> menu to open the Manage DNS Authoritative Server page. The page displays all the DNS server attributes.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Modify the attributes as per your requirements.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Click <strong>Save</strong> to save the DNS server attribute modifications.</td>
</tr>
</tbody>
</table>

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

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 47) 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 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 Network Registrar 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 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 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-interval, 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=value. 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 48
- **Secondary server attributes**—See Setting Secondary Refresh Times, on page 48
- **Port numbers**—See Setting Local and External Port Numbers, on page 49
- **Handle Malicious DNS Clients**—See Handling Malicious DNS Clients, on page 50

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. Databases originating from versions of Cisco Prime Network Registrar earlier than Release 3.5 do not have the defttl zone attribute, and use the minimum TTL in the zone SOA record for the default TTL.

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 47.

**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 Network Registrar Services" section in Cisco Prime Network Registrar 8.3 Administrator Guide.
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 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.

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 Network Registrar 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

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.

Note

- You must reload the Authoritative DNS server after you enable the hybrid-mode configuration.
- Cisco Prime Network Registrar 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 Network Registrar 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 Network Registrar 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 forwards and exceptions. The other actions and triggers are applied during or after regular query processing.

---

**DNS Response Policy Zone (RPZ) Firewall Rules**

Cisco Prime Network Registrar 8.3 and later supports Response Policy Zones (RPZ). 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 2: RPZ Triggers**

<table>
<thead>
<tr>
<th>RPZ Trigger</th>
<th>RR Name</th>
<th>Example</th>
<th>Example RR Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name Server to query</td>
<td><code>&lt;ns-domain-name&gt;.rpz-nsdname.rpz-nsip.&lt;customer-domain&gt;</code></td>
<td>Name Server ns.baddomain.com</td>
<td>ns.baddomain.com.rpz-nsdname.rpz-nsip.cisco.com</td>
</tr>
<tr>
<td>Name Server IP to query</td>
<td><code>32.&lt;reversed-ip&gt;.rpz-nsip.rpz-nsdname.&lt;customer-domain&gt;</code></td>
<td>Name Server Address 192.168.2.10</td>
<td>32.10.2.168.192.rpz-nsip.rpz.cisco.com</td>
</tr>
</tbody>
</table>
This zone contains all the RRs related to blocking 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, on page 53 section. The rdata defines the rule action to be taken. The following table describes the RPZ actions.

Table 3: RPZ Actions

<table>
<thead>
<tr>
<th>RPZ Rule Action</th>
<th>RPZ RR RData</th>
<th>RPZ RR Example</th>
</tr>
</thead>
</table>

DNS RPZ Best Practices

- CPNR 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**—For deployments that were upgraded from Cisco Prime Network Registrar 5.5.x or earlier, the DNS server might be operating with legacy preset values for critical settings. These preset values 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>
<thead>
<tr>
<th>DNS Attribute</th>
<th>7.0 Preset Value</th>
<th>7.1 Preset Value</th>
<th>Recommended Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>axfr-multirec-default</td>
<td>on</td>
<td>on</td>
<td>on</td>
</tr>
<tr>
<td>mem-cache-size</td>
<td>10000 (KB)</td>
<td>50000 (KB)</td>
<td>50000 (KB)</td>
</tr>
</tbody>
</table>

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 5: DNS Log Settings

<table>
<thead>
<tr>
<th>Log Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>config</td>
<td>Server configuration and deinitialization.</td>
</tr>
<tr>
<td>ddns</td>
<td>High level dynamic update messages.</td>
</tr>
<tr>
<td>xfr-in</td>
<td>Inbound full and incremental zone transfers.</td>
</tr>
<tr>
<td>xfr-out</td>
<td>Outbound full and incremental zone transfers.</td>
</tr>
<tr>
<td>notify</td>
<td>NOTIFY transactions.</td>
</tr>
<tr>
<td>datastore</td>
<td>Data store processing that provides insight into various events in the server embedded databases.</td>
</tr>
<tr>
<td>scavenger</td>
<td>Scavenging of dynamic RRs (see the Scavenging Dynamic Records section in <em>Cisco Prime Network Registrar 8.3 DHCP User Guide</em>).</td>
</tr>
<tr>
<td>scavenger-details</td>
<td>More detailed scavenging output (disabled by default).</td>
</tr>
<tr>
<td>server-operations</td>
<td>General high-level server events, such as those pertaining to sockets and interfaces.</td>
</tr>
<tr>
<td>ddns-refreshes</td>
<td>DNS update refreshes for Windows clients (disabled by default).</td>
</tr>
<tr>
<td>ddns-refreshes-details</td>
<td>RRs refreshed during DNS updates for Windows clients (disabled by default).</td>
</tr>
<tr>
<td>ddns-details</td>
<td>RRs added or deleted due to DNS updates.</td>
</tr>
<tr>
<td>tsig</td>
<td>Logs events associated with Transaction Signature (TSIG) DNS updates (see the Transaction Security section in <em>Cisco Prime Network Registrar 8.3 DHCP User Guide</em>).</td>
</tr>
<tr>
<td>tsig-details</td>
<td>More detailed logging of TSIG DNS updates (disabled by default).</td>
</tr>
<tr>
<td>activity-summary</td>
<td>Summary of activities in the server. You can adjust the interval at which these summaries are taken using the <code>activity-summary-interval</code> attribute, which defaults to five-minute intervals (you can adjust this interval using <code>dns set activity-summary-interval</code>).</td>
</tr>
<tr>
<td>query-errors</td>
<td>Logs errors encountered while processing DNS queries.</td>
</tr>
<tr>
<td>config-details</td>
<td>Generates detailed information during server configuration by displaying all configured and assumed server attributes (disabled by default).</td>
</tr>
<tr>
<td>incoming-packets</td>
<td>Incoming data packets.</td>
</tr>
<tr>
<td>outgoing-packets</td>
<td>Outgoing data packets.</td>
</tr>
<tr>
<td>xfer-in-packets</td>
<td>Incoming full zone transfer (XFR) packets.</td>
</tr>
<tr>
<td>query-packets</td>
<td>Incoming query packets.</td>
</tr>
<tr>
<td>notify-packets</td>
<td>NOTIFY packets.</td>
</tr>
<tr>
<td>Log Setting</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ddns-packets</td>
<td>DNS Update packets.</td>
</tr>
<tr>
<td>xfer-out-packets</td>
<td>Outgoing XFR packets.</td>
</tr>
<tr>
<td>ha-details</td>
<td>Generates detailed logging of High-Availability (HA) DNS information.</td>
</tr>
<tr>
<td>scp</td>
<td>Allows log messages associated with SCP message handling.</td>
</tr>
<tr>
<td>optRR</td>
<td>Causes logging related to OPT RR processing.</td>
</tr>
<tr>
<td>ha-messages</td>
<td>Enables detailed logging of HA messages.</td>
</tr>
</tbody>
</table>

- **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.`
CHAPTER 7

Managing High Availability DNS

A second primary server can be made available as a hot standby that shadows the main primary server. This configuration is called High-Availability (HA) DNS. The Cisco Prime Network Registrar web UI and CLI have features with which you can duplicate the primary setup required for HA DNS for the server pair. The server pair is responsible for detecting communication failures and the like. After the HA DNS is configured, the shadowing and error detection is done automatically. In a Cisco Prime Network Registrar deployment where Cisco Prime Network Registrar DHCP is updating Cisco Prime Network Registrar DNS, the failure detection and failover also happens automatically.

- Introduction to HA DNS Processing, on page 61
- Creating High Availability DNS Pairs, on page 63
- HA DNS Configuration Synchronization, on page 64
- Synchronizing HA DNS Zones, on page 67
- Enable Logging of HA DNS Information, on page 68
- Viewing HA DNS Statistics, on page 68

Introduction to HA DNS Processing

In normal state, both the main and backup primary servers are up and running. The main server processes all DNS updates from clients and sends all accepted updates to the hot standby backup. The main server will forward RR updates to the backup server and the backup server only accepts updates from the main in normal state. In normal states, updates from DDNS clients are ignored or dropped by a backup server. Both servers can respond to queries and zone transfer requests. The main and the backup partners always stay in communication to detect availability of the other.

If the main goes down, the backup waits a short time, then begins servicing the DNS updates from clients that the main would normally service and records the updates. When the main returns, the backup sends it the updates, and the main synchronizes with the backup any updates that were not sent and which it had before it went down.

Whenever you add a new zone, both the primary and the secondary servers must be reloaded to automatically synchronize with the HA backup.

The synchronization is done on a per-zone basis. This allows updates to all other zones while a given zone is in the process of getting synchronized.

If the hot standby backup goes down, the main waits a short time, then records the updates that the partner did not acknowledge. When the backup server comes back up, the main sends the recorded updates to the backup.
Both the main and backup can traverse the following states:

- **Startup**—The servers establish communication and agree on the HA version to use. In this state, the servers do not accept DNS updates or RR edits, and they defer scavenging, if enabled.
- **Negotiating**—Each server is waiting for the other to get ready to synchronize. In this state, DNS Updates and RR edits are not allowed.
- **Normal**—Both servers are up and healthy, exchanging DNS updates and heartbeat messages. The main accepts DNS updates and RR edits, sends RR Update messages to the backup, and performs history trimming and scavenging, if enabled. The backup ignores DNS updates, refuses RR edits, but processes RR Update messages from the main server. The backup also performs history trimming, but defers scavenging, if enabled. In this state, the synchronization takes place.
- **Communication-Interrupted**—The server goes into this state after not getting a response or request from the partner during the communication timeout (ha-dns-comm-timeout period (preset to 30 seconds)). The server continues listening for communication from the partner (they both send heartbeat messages every 12 seconds) and tries to connect, meanwhile accepting DNS updates and RR edits and disabling scavenging.
- **Partner-Down**—The server administrator notifies the partner that it will be down for an extended time. This manual intervention is possible only in Communication-Interrupted state. Either server continues listening for communication from the partner and tries to connect, accepts DNS updates and RR edits, and performs scavenging.

When a DNS server starts up, it:

1. Tries to establish a connection with its partner.
2. Transitions to Negotiating state.
3. Transitions to Normal state, after it receives a Negotiating response.

Once the server is in Normal state, the zone level synchronization begins. Zone synchronization is always managed by the Main HA server. The zones traverse through the following states:

- **Sync-Pending State**—A zone enters this state when the HA DNS server transitions to the normal state or if a manual sync is requested. In this state RR updates for the zone will be accepted on the main server, and forwarded to the backup server.
- **Synchronizing State**—The RR synchronization for the zone takes place in the synchronizing state. RR updates are not accepted, and notifies are disabled.
- **Sync-Complete State**—A zone transitions to this state from the synchronizing state once it has successfully synchronized resource record changes with its corresponding zone on the HA DNS backup. In this state, the zone on the HA DNS main server accepts all dynamic DNS update requests, allow resource record configuration changes, and re-enables notifies. Resource record modifications will be forwarded to the backup server.
- **Sync-Failed State**—A zone transitions to the sync-failed state from the synchronizing state if it fails to sync. The zone will accept resource record updates on the main server, and changes will be forwarded to the backup. The server will retry synchronizing the zone after ha-dns-zonesync-failed-timeout. A manual sync request or server restart will also restart zone synchronization.

HA DNS is fully integrated with DHCP servers, and the partners are updated when hosts get added to the network (see the "Managing DNS Update" chapter in Cisco Prime Network Registrar 8.3 DHCP User Guide). From the DHCP side of HA DNS, the DHCP server sends DNS updates to a single DNS server at a time.

DHCP autodetects the main being down and start sending updates to the backup. The DHCP server tries to contact the main DNS server, twice. It tries the backup partner if both of the attempts are unsuccessful.
The backup detects the main server down and starts accepting updates from DDNS clients. When the servers come up again, HA communication will be automatically established and the servers will get into Normal state where they carry out zone synchronization and make sure that both have the same RRs, etc.

If both DNS partners are communicating, the backup server drops the update, whereby the DHCP server times out and retries the main DNS server. If both servers are unreachable or unresponsive, the DHCP server continually retries each DNS partner every 4 seconds until it gets a response.

For zone level sync, an Advanced mode command is added in the local cluster Zone Commands page, if the local cluster is configured as the main HA server. The sync is run using the HA server algorithms by default. In Expert mode, the following three options are provided:

- Sync All RRs using the HA server synchronization algorithms
- Sync All RRs from Main to Backup
- Sync All RRs from Backup to Main

HA DNS status is modified to include the zone synchronization status. Status includes count and percentage of synchronized zones, zones pending synchronization, and zones that have failed synchronization.

Zone status has been modified to also include the HA synchronization status (ha-server-pending, sync-pending, sync-complete, synchronizing, or sync-failed), if HA is configured.

The ha-dns-comm-timeout attribute managed through the HA pair indicates the time required to determine if a partner is unreachable, after network communication is not acknowledged, which triggers the Communication-Interrupted state (see the description of this state in Introduction to HA DNS Processing, on page 61). The preset value is 30s. The server tries to communicate and then back off at multiples of the ha-dns-comm-timeout interval.

### Creating High Availability DNS Pairs

The attributes needed to set up an HA DNS server pair from the main server are:

- **ha-dns** — Enabled or disabled. The preset value is enabled.
- **main** — cluster for the main primary DNS server.
- **backup** — cluster for the backup primary DNS server.

The specific IP addresses for the main or backup is specified only when the cluster IP is only used for management and DNS works on a different interface.

### Local Basic or Advanced and Regional Web UI

#### Step 1
Create a cluster for the backup server.

#### Step 2
From the Deploy menu, choose HA under the DNS submenu to open the View/Add HA DNS Server Pair page.

#### Step 3
Click the Add HA Pair icon in the HA Pairs pane to open the Add HA DNS Server dialog box.

#### Step 4
Enter the name of the server pair in the name field. This can be any identifying text string.

#### Step 5
Click the cluster name of the main DNS server in the Main Server drop-down list.

**Note** If you change the IP address of your local host machine, you must modify the localhost cluster (on the Edit Cluster page) to change the address in the IP Address field. Do not set the value to 127.0.0.1.

#### Step 6
Click the cluster name of the backup DNS server in the Backup Server drop-down list. This cannot be the same as the main server cluster. Set the ha-dns-main-server and ha-dns-backup-server attributes only if the server is configured with
different interfaces for configuration management and update requests. (Configure the HA DNS protocol only with the interface used to service updates.)

**Step 7**
Click **Add HA DNS Server**.

**Step 8**
Once the server pair appears on the List/Add HA DNS Server Pair page, synchronize the servers:

a) Select the HA in the HA Pairs pane and click the Sync HA DNS Server Pair tab.
b) Choose the direction of synchronization (Main to Backup or Backup to Main).
c) Choose the operation type (Update, Complete, or Exact). See the table on the page for details on the operations for each operation type.
d) Click the **Report** button to display the prospective synchronization changes on the View HA DNS Sync Report page.
e) Click Run Complete to complete the synchronization.
f) Click **Return** to return to the List HA DNS Server Pairs page.

**Step 9**
Reload both DNS servers to begin HA communication.

---

**CLI Commands**

Create the HA DNS server pair (**ha-dns-pair** name create mainaddr backupaddr). Then synchronize the servers using **ha-dns-pair** name sync, specifying the synchronization operation (update, complete, or exact) and direction (main-to-backup or backup-to-main). Be sure to reload both DNS servers. For example:

```
nrcmd> ha-dns-pair examplehadnspair create localhost test-cluster
nrcmd> ha-dns-pair examplehadnspair sync exact main-to-backup
nrcmd> dns reload
```

See the **ha-dns-pair** command in the [CLIGuide.html](file) file in the /docs directory for syntax and attribute descriptions. The CLI provides an additional command for the DNS server to set the HA DNS partner down, if necessary, which is possible only while in Communication-Interrupted state:

```
nrcmd> dns setPartnerDown
```

The partner down is useful because it limits the bookkeeping data a server maintains, thus optimizing its performance. When both servers start communicating again, the sync sends all the zone RRs rather than trying to determine individual changes.

---

**HA DNS Configuration Synchronization**

This section describes the migration procedure used to migrate Cisco Prime Network Registrar product databases from the HA DNS main server to the HA DNS backup server. Throughout this procedure the source system is referred as DNS HA main server and destination as DNS HA backup server. When you enable the HA DNS with large DNS configuration, you will notice that the process takes long time to complete. This section provides a workaround, which you can use until the defect is addressed.

---

**Danger**

To perform this process, you must have HA main server and HA backup server running on the same OS, Cisco Prime Network Registrar version, and DNS configuration.
Pre-install Cisco Prime Network Registrar on the HA DNS backup server

You need to pre-install Cisco Prime Network Registrar on the HA DNS backup system before migrating the database directory from the HA DNS main system, to reduce the time required during the Cisco Prime Network Registrar software installation process. During the installation process, the installer will verify whether any previous configuration is up to date with the Cisco Prime Network Registrar data schema for the version being installed. Even if the versions are identical, the time required to perform this verification can be avoided by pre-installing Cisco Prime Network Registrar on the HA DNS backup system.

Pre-migration Steps for HA DNS Main Server

You must ensure that the service of DHCP and TFTP servers are available and running on different systems, especially when there is a large DNS configuration. If the servers are found on the same system, the migration from HA DNS main server to backup server may cause DHCP or TFTP conflicts, and DHCP clients may be destabilized.

Follow the pre-migration steps as below:

**Step 1** Disable the automatic start-on-reboot setting for the DHCP and TFTP server.

**Note** The default setting of start-on-reboot for the TFTP server is disabled.

**Example:**

```
nrcmd> server dhcp disable start-on-reboot
nrcmd> server tftp disable start-on-reboot
```

**Step 2** Stop the Cisco Prime Network Registrar on the HA DNS main server using the Windows Service Control manager (Windows) or nwreglocal script in /etc/init.d (Linux and Solaris).

**Step 3** Once the Cisco Prime Network Registrar is stopped by using Windows Process Manager (Windows) or ps command line utility (Linux/Solaris), navigate to the parent directory of the Cisco Prime Network Registrar data directory, InstallDir\Network Registrar\Local\ (Windows) or /var/nwreg2/local/ on (Linux/Solaris).

**Step 4** Using tar or an equivalent compression utility, bundle up the contents of the data subdirectory. InstallDir is the directory where you have installed your Cisco Prime Network Registrar: tar -cvf cnrdatadir.tar data.

**Tip** Replace all the .bak database backup directories temporarily from HA DNS main server. The HA backup server does not need these backup directories and replacing them reduces the overall archive size. Be sure that you do not replace any other database files other than .bak; otherwise, the HA DNS backup cluster may not function properly.

Restart Cisco Prime Network Registrar on the HA DNS Main Server

**Step 1** Restart the Cisco Prime Network Registrar servers on the HA DNS main system using the Windows Service Control manager (Windows) or nwreglocal script in /etc/init.d (Linux and Solaris).

**Step 2** Restore the DHCP and TFTP server start-on-reboot attribute values to their pre-migration values:

**Example:**
nrcmd> server dhcp enable start-on-reboot
nrcmd> server dhcp start
nrcmd> server tftp enable start-on-reboot
nrcmd> server tftp start

Copy Cisco Prime Network Registrar Database Files to HA DNS Backup Server

Step 1  Use FTP or an equivalent network file copy mechanism to transfer the Cisco Prime Network Registrar database archive that was generated in the previous step to the parent directory of the Cisco Prime Network Registrar data directory (typically C:\NetworkRegistrar\Local\ on Windows, and /var/nwreg2/local/ on Linux/Solaris) on the HA DNS backup server.

Step 2  Ensure that the mechanism used to transfer the database archive preserves binary file data. If FTP sessions default to ASCII mode, change it to binary mode in order to produce a usable database on the HA DNS backup server.

Step 3  Stop the Cisco Prime Network Registrar product on the HA DNS backup server completely using the Windows Service Control Manager (Windows) or nwreglocal script in /etc/init.d (Linux and Solaris). Ensure that the product is completely stopped, either by using the Windows Process Manager or the ps command line utility on Linux/Solaris, navigate to the parent directory of the Cisco Prime Network Registrar data directory (typically C:\NetworkRegistrar\Local\ on Windows, and /var/nwreg2/local/ on Linux/Solaris).

Step 4  Ensure to recursively remove all contents of the existing data directory, to prevent any conflicts with the database archive that is about to be extracted. Using tar or an equivalent utility, extract the contents of the database archive file: tar -xvf cnrdatadir.tar.

Reconfigure Cisco Prime Network Registrar on the HA DNS Backup Server

Step 1  Start the Cisco Prime Network Registrar servers on the HA DNS backup system using the Windows Service Control Manager (Windows) or nwreglocal script in /etc/init.d (Linux and Solaris).

Step 2  Rectify the conflicts, if any, between HA DNS main system and any DHCP or TFTP server configuration settings.

Step 3  The DHCP integrity will be compromised if the DHCP server has a configuration similar to that of HA DNS main system. To know more on increasing the DHCP service availability, refer to the Cisco Prime Network Registrar product documentation. Cisco recommends that you completely remove any DHCP and/or TFTP related configuration on the HA DNS backup system using either the web UI or nrcmd CLI. You can restore the original DHCP and TFTP server-start-on-reboot attribute values, only after you confirm that the configuration values do not conflict with that of the HA DNS main system.

Example:

nrcmd> server dhcp enable start-on-reboot
nrcmd> server tftp enable start-on-reboot (only if it had be previously enabled)

Step 4  Edit the localhost Cluster object in the HA DNS backup server to reflect the values in use on the local server.
Configure Cisco Prime Network Registrar HA DNS on the HA DNS Main Server

**Step 1** In HA DNS main server, define appropriate Cluster objects for both the HA DNS main and HA DNS backup servers.

**Step 2** Create an HA Pair object by specifying appropriate Cluster names for the main and backup DNS server roles, and enable HA DNS for the HA Pair.

**Step 3** Generate the report of changesets and exchange them between the two servers using the default report generation settings (Main-to-backup, Complete).

**Step 4** Perform the changeset synchronization while the list of changesets is displayed.

---

**Reload the DNS Servers**

**Step 1** Reload the DNS servers on both HA DNS systems to initiate the DNS RR synchronization process. Do it either through the Manage Servers page on the HA DNS main cluster when the HA DNS main server's DNS server has finished reloading, or to save a little time, initiate through separate connections to both clusters to perform the reloads in parallel instead of series.

**Step 2** When the DNS servers are synchronizing, Cisco Prime Network Registrar does not allow DNS configuration updates (such as DDNS), but provides DNS queries and zone transfer. You can monitor the DNS server log files on the main and backup clusters to follow the progress of the DNS server synchronization process. The servers are fully operational when HA DNS enters Normal state.

---

**Synchronizing HA DNS Zones**

**Local Advanced Web UI**

To manually synchronize an HA DNS zone:

**Step 1** From the Design menu, choose Forward Zones or Reverse Zones under the Auth DNS submenu to open the List/Add Forward Zones or List/Add Reverse Zones page.

**Step 2** Click the Commands button for the zone which you want to synchronize on the Edit Zone page.

**Step 3** Click the Command icon next to Synchronize HA Zone to synchronize the HA DNS zone.

Synchronizing the HA DNS zone will always sync the associated views and named ACLs for primary zones.

**Note** In the Expert mode, you have the option to choose the type of synchronization. The Use Server Algorithms option is checked by default. If you click the command icon next to the Synchronize HA Zone without choosing another option, server algorithms will be used to synchronize the zone. You can override this by checking either Push Full Zone From Main to Backup check box or Pull Full Zone From Backup to Main check box.
**CLI Commands**

Use `zone name ha-sync-all-rrs` to manually schedule HA zone synchronization for the zone, or to raise its priority, if the zone is already in the sync-pending state (see the `zone` command in the CLIGuide.html file in the /docs directory for syntax and attribute descriptions).

**Enable Logging of HA DNS Information**

The log settings, `ha-details` and `ha-messages`, enable logging of HA DNS-related information.

---

**Note**

The HA communications with versions earlier to 8.0 are not supported. So, you have to upgrade both the main and the backup servers in the same maintenance window.

---

**Viewing HA DNS Statistics**

You can view HA DNS statistics.

**Local Basic or Advanced Web UI**

Click the Statistics tab on the Manage DNS Authoritative Server page to open the DNS Server Statistics page. The statistics appear under the HA Statistics and Max Counter Statistics subcategories of both the Total Statistics and Sample Statistics categories.

**CLI Commands**

Use `dns getStats ha [total]` to view the HA DNS Total counters statistics, and `dns getStats ha sample` to view the Sampled counters statistics.
CHAPTER 8

Managing Zones

The Domain Name System (DNS) is a distributed database for objects in a computer network. By using a nameserver approach, the network consists of a hierarchy of autonomous domains and zones. The namespace is organized as a tree that often resembles the organizations that are responsible for the administration boundaries. For an introduction to the protocol, see Introduction to the Domain Name System, on page 1.

The basic function of DNS nameservers is to provide data about network objects by answering queries. You can configure the Cisco Prime Network Registrar DNS server and zones by accepting the system defaults or changing them.

DNS also supports creation of the Internationalized Domain Names (IDN). The full set of Unicode characters are supported to name DNS domains in the WebUI, web-services (REST), and Java SDK with limited sort and search capabilities. For more information, see the Cisco Prime Network Registrar 8.3 Release Notes.

Note
You must set the locale parameters on UNIX to en_US.UTF-8 when running Java tools that use Java SDK, such as cnr_rules. For more information, see "Running Data Consistency Rules" section in the Administration Guide.

This chapter describes the basics of configuring the Cisco Prime Network Registrar DNS servers, and their primary and secondary zones. Managing Resource Records, on page 101 describes how to manage DNS resource records (RRs) and hosts, and Managing Authoritative DNS Server, on page 43 describes how to set some of the more advanced zone and DNS server properties.

Each zone will have an explicit view id that defines its view. The list of views for any given zone distribution will be defined by the list of zones. Synchronizing the zone will always sync the associated views and named ACLs for both primary and secondary zones. Managing DNS Views, on page 97 describes how to manage DNS views.

• Managing Primary DNS Servers, on page 70
• Creating and Applying Zone Templates, on page 70
• Staged and Synchronous Modes, on page 72
• Configuring Primary Forward Zones, on page 73
• Configuring Primary Reverse Zones, on page 79
• Getting Zone Counts on the Server, on page 81
• Enabling DNS Updates, on page 81
• Managing Secondary Servers, on page 82
• Configuring Subzones, on page 84
Managing Primary DNS Servers

Adding a zone involves creating a domain name. You can also define an owner and use a zone template. If you do not use a template, you must also define the Start of Authority (SOA) and Name Server (NS) properties for the zone.

You do not need to create a loopback zone for the local host, because Cisco Prime Network Registrar automatically creates one. A loopback zone is a reverse zone that a host uses to resolve its loopback address, 127.0.0.1, to localhost so that it can direct network traffic to itself. The loopback zone is 127.in-addr.arpa, which appears on the list of reverse zones.

Related Topics

- Configuring Primary Forward Zones, on page 73
- Configuring Primary Reverse Zones, on page 79
- Getting Zone Counts on the Server, on page 81

Creating and Applying Zone Templates

A zone template is a convenient way to create a boilerplate for primary zones that share many of the same attributes. You can apply a zone template to any zone, and override the zone attributes with those of the template. You can create zone templates in the local and regional cluster web UIs and in the CLI.

Be careful applying a template to an existing zone. The template overwrites all explicitly set attributes for the zone (other than its name), possibly causing severe consequences if the zone is already configured in a network. To make a limited attribute change to multiple zones using a template, be sure to change only that attribute (or attributes), leaving the others unset, before you apply the template to the zones.

Local Basic or Advanced and Regional Web UI

Step 1
From the Design menu, choose Zone Templates under the Auth DNS submenu.

Step 2
You can add a zone template at the local and regional clusters, and you can also pull and push zone templates at the regional cluster in the web UI:

- To add a zone template at the local cluster or explicitly add one at the regional cluster, click the Add Zone Templates icon in the Zone Templates pane. This opens the Add Zone Template dialog box, enter the name and click Add Zone Template.

To make the zone template meaningful, you would enter the suggested serial number, nameserver, contact e-mail address, and list of nameservers, because they are required for the zone itself. You might also want to specify any zone owners or zone distributions. You do not necessarily need to add these values for the zone template, because you can do so for the zone once it is created from the template. However, the template name and zone default TTL are required. (For a description of the minimally required zone attributes, see Creating Primary Zones, on page 73.)
After you enter these values, click **Save** at the bottom of the page.

- At the regional cluster, to pull a zone template from one or more local clusters, click the **Pull Replica** icon in the Zone Templates pane. This opens the Select Replica Zone Template Data to Pull dialog box which shows a tree view of the regional server replica data for the local clusters’ zone templates. The tree has two levels, one for the local clusters and one for the templates in each cluster. You can pull individual templates from the clusters, or you can pull all of their templates:
  - To pull individual zone templates, expand the tree for the cluster, choose a pull criterion next to its name, then click **Pull Zone Template**.
  - To pull all the templates from a cluster, choose a pull criterion, then click **Pull All Zone Templates**.
  - To update all the replica data for a cluster, click the **Pull Replica** icon.

The pull selection criteria are:

- **Ensure**—Pulls each template, except if an existing template by that name already exists at the regional cluster, in which case it does not overwrite the regional cluster data.
- **Replace**—Pulls each template and overwrites the data for it if it already exists at the regional cluster, without affecting any additional templates at the regional cluster. This is the default and recommended setting.
- **Exact**—Pulls each template, overwrites the data for it if it already exists at the regional cluster, and removes any additional templates at the regional cluster.

- At the regional cluster, to push a zone template to one or more local clusters:
  - To push all the zone templates on the page List Zone Templates page—Click the **Push All** icon in the Zone Templates pane.
  - To push individual zone templates on the page List Zone Templates page—Click **Push**.

Both of these actions open a version of the Push Zone Template Data to Local Clusters page.

This page provides a choice of the synchronization mode and the destination clusters. Move the desired cluster or clusters from the Available field to the Selected field, then click one of the data synchronization mode radio buttons:

- **Ensure**—Pushes each template, except if an existing template by that name already exists at the local cluster, in which case it does not overwrite the local cluster data. This is the default and recommended setting.
- **Replace**—Pushes each template and overwrites the data for it if it already exists at the local cluster, without affecting any additional templates at the local cluster.
- **Exact**—Available for “push all” operations only, it pushes each template, overwrites the data for it if it already exists at the local cluster, and removes any additional templates at the local cluster.

After making these choices, click **Push Data to Clusters**. This opens the View Push Zone Template Data Report page, where you can view the intended results of the push operation. Click **OK** to implement the push operation.

**Step 3**

You can apply the template to a new or existing zone:

1. **New zone**—Select the template from the Template drop-down list when you create the zone, as described in Configuring Primary Forward Zones, on page 73.
2. **Existing zone**—After you create a zone (see Configuring Primary Forward Zones, on page 73, you can apply the template when you edit the zone on the Edit Zone page. Click the template name in the Template drop-down list, then click **Apply Template**.

---

After you enter these values, click **Save** at the bottom of the page.

- At the regional cluster, to pull a zone template from one or more local clusters, click the **Pull Replica** icon in the Zone Templates pane. This opens the Select Replica Zone Template Data to Pull dialog box which shows a tree view of the regional server replica data for the local clusters’ zone templates. The tree has two levels, one for the local clusters and one for the templates in each cluster. You can pull individual templates from the clusters, or you can pull all of their templates:
  - To pull individual zone templates, expand the tree for the cluster, choose a pull criterion next to its name, then click **Pull Zone Template**.
  - To pull all the templates from a cluster, choose a pull criterion, then click **Pull All Zone Templates**.
  - To update all the replica data for a cluster, click the **Pull Replica** icon.

The pull selection criteria are:

- **Ensure**—Pulls each template, except if an existing template by that name already exists at the regional cluster, in which case it does not overwrite the regional cluster data.
- **Replace**—Pulls each template and overwrites the data for it if it already exists at the regional cluster, without affecting any additional templates at the regional cluster. This is the default and recommended setting.
- **Exact**—Pulls each template, overwrites the data for it if it already exists at the regional cluster, and removes any additional templates at the regional cluster.

- At the regional cluster, to push a zone template to one or more local clusters:
  - To push all the zone templates on the page List Zone Templates page—Click the **Push All** icon in the Zone Templates pane.
  - To push individual zone templates on the page List Zone Templates page—Click **Push**.

Both of these actions open a version of the Push Zone Template Data to Local Clusters page.

This page provides a choice of the synchronization mode and the destination clusters. Move the desired cluster or clusters from the Available field to the Selected field, then click one of the data synchronization mode radio buttons:

- **Ensure**—Pushes each template, except if an existing template by that name already exists at the local cluster, in which case it does not overwrite the local cluster data. This is the default and recommended setting.
- **Replace**—Pushes each template and overwrites the data for it if it already exists at the local cluster, without affecting any additional templates at the local cluster.
- **Exact**—Available for “push all” operations only, it pushes each template, overwrites the data for it if it already exists at the local cluster, and removes any additional templates at the local cluster.

After making these choices, click **Push Data to Clusters**. This opens the View Push Zone Template Data Report page, where you can view the intended results of the push operation. Click **OK** to implement the push operation.

**Step 3**

You can apply the template to a new or existing zone:

1. **New zone**—Select the template from the Template drop-down list when you create the zone, as described in Configuring Primary Forward Zones, on page 73.
2. **Existing zone**—After you create a zone (see Configuring Primary Forward Zones, on page 73, you can apply the template when you edit the zone on the Edit Zone page. Click the template name in the Template drop-down list, then click **Apply Template**.
CLI Commands

Use `zone-template name create` to create the zone template. (See Configuring Primary Forward Zones, on page 73 for how to apply the template to a zone.) For example:

```
nrcmd> zone-template zone-template-1 create serial=1
```

To apply a template to a zone, use `zone-template name apply-to zone`. Note that the syntax permits one or more comma-separated zones and also the `all` keyword for all zones. You can also clone a template from an existing template by using `zone-template clone-name create clone=template`, and then make adjustments to the clone. For example:

```
nrcmd> zone-template zone-template-1 apply-to example.com,boston.example.com
nrcmd> zone-template cloned-template create clone=zone-template-1 owner=owner-1
```

Staged and Synchronous Modes

You can perform additions or edits to DNS zones, RRs, and hosts in one of two modes in the regional cluster—staged or synchronous:

- **Staged**— Changes to zones, their hosts and RRs are written to the CCM regional database. You must synchronize the zones to propagate pending changes to the local DNS servers. When adding or deleting zones, or when updating zone settings, you must also reload the local DNS servers following synchronization.

- **Synchronous**— After committing changes to the CCM regional database, they are immediately propagated to the local DNS servers. Changes to hosts and RRs will immediately be active, but similar to staged mode, changes to zones may also require a DNS server reload. If propagation cannot occur because the local servers are unreachable, you must manually synchronize the zones to propagate pending changes once the connection is restored.

The zone distribution determines which local DNS servers will publish the zone. Once assigned, synchronization can occur in synchronous edit mode, on a zone basis, or for all zones in the distribution.

Staged edit mode is the default value for regional servers. To choose the mode, select Session Settings from the `Username` menu in the Web UI. The username drop-down list is available at the top right of the window adjacent to the Log Out link.

On local clusters, edits are always performed in synchronous mode. When HA DNS is configured, zone changes are immediately propagated to the HA partner. If propagation cannot occur because the partner unreachable, host and RR changes will be synchronized automatically once the connection is restored, but you must manually synchronize the zones to propagate pending changes.

---

**Note**

In Cisco Network Registrar versions earlier than 7.1, the dns edit mode was called zone edit mode.

Local and Regional Web UI

Staged or synchronous zone modes are preset based on the Session Edit Modes setting in Session Settings on the Web UI main page `Username` menu:

- The regional web UI is preset to **staged**.
• The local web UI is preset to **synchronous**.

**CLI Commands**

Set the session `dns-edit-mode` attribute to staged or synchronous. For example:

```
nrcmd> session set dns-edit-mode=sync
```

**Configuring Primary Forward Zones**

This section explains how to configure a primary nameserver with a primary forward zone. When you are done with this procedure, follow the procedure in the Configuring Primary Reverse Zones, on page 79 to configure a reverse zone for each network that you use.

---

**Tip**

For an example of adding a forward zone, see the "Create the Zone Infrastructure" section in Cisco Prime Network Registrar 8.3 Administrator Guide.

---

**Creating Primary Zones**

Creating a primary zone requires, at a minimum, adding certain key Start of Authority (SOA) attributes and nameservers for the zone. The advantage of Basic mode in the web UI is that many of these settings are already done for you.

**Local Basic Web UI**

1. **Step 1** From the **Design** menu, choose **Forward Zones** under the **Auth DNS** submenu to open the List/Add Forward Zones page.
2. **Step 2** Click the **Add Forward Zone** icon in the Forward Zones pane, enter the zone name (in domain name format).
3. **Step 3** Enter the name of the nameserver host, such as **ns1**.
4. **Step 4** Enter the contact e-mail name, such as **hostmaster**.
5. **Step 5** Click **Add DNS Zone**. Basic mode creates the zone with preset values:
   - Zone default TTL—**24h**
   - Start of Authority (SOA) serial number—**1**
   - SOA secondary refresh time—**3h**
   - SOA secondary retry time—**60m**
   - SOA secondary expiration time—**1w**
   - SOA minimum TTL—**10m**
Local Advanced and Regional Web UI

Step 1  From the Design menu, choose Forward Zones under the Auth DNS submenu to open the List/Add Forward Zones page.

Step 2  Click the Add Forward Zone icon in the Forward Zones pane, enter the zone name (in domain name format).

Step 3  Enter the name of the nameserver host, such as ns1.

Step 4  Enter the contact e-mail name, such as hostmaster.

Step 5  Enter the serial number.

Step 6  Click Add Zone.

Step 7  Choose an owner or region, if necessary, from the drop-down list.

Step 8  Apply an existing zone template, if necessary (see Creating and Applying Zone Templates, on page 70). Click the name of the configured template in the drop-down list.

**Caution**  Be careful applying a template to a zone that is already live. Explicitly defined attributes on the template replace the existing ones defined for the zone.

Step 9  Modify the top attributes, if necessary:
   a)  Owner and region
   b)  Preconfigured zone distribution (see Managing Zone Distributions, on page 87)
   c)  Zone default TTL

Step 10  In the SOA attributes, enter a:
   a)  Serial number, such as 1.
      A primary DNS server uses a serial number to indicate when its database changes and uses any incrementing of this number to trigger a zone transfer to a secondary server. The serial number you can enter here is the suggested one only, and the DNS server does not always accept it. If you edit the serial number to be less than the actual serial number that the server maintains, the server logs a warning message and ignores the suggested serial number. The actual serial number always equals or is higher than the suggested one. You can get the actual serial number by using zone name get serial (if the DNS server is running; if the server is not running, or listing or showing the zone attributes, it always returns the suggested serial number), or by refreshing the DNS Server Value for the zone Serial Number attribute. You must explicitly enter this suggested serial number when creating a zone.

   b)  Nameserver host, such as ns1.
      Enter either just the hostname or its fully qualified name (such as ns1.example.com., but you must end it with a trailing dot). Use the fully qualified name if the primary nameserver is in a different zone. The primary DNS server becomes the ns value in the zone SOA record. You must also specify one or more authoritative nameservers for the zone—these become the Name Server (NS) records for the zone. In the CLI, the primary DNS server automatically becomes the first NS record and also appears as the first entry in the nameservers attribute list.

   c)  Contact e-mail name, such as hostmaster.
      The fully qualified contact e-mail name becomes a slightly altered version of the e-mail address in that dots (.) are substituted for the at symbol (@). If using the fully qualified value, end the address with a trailing dot (for example, enter hostmaster@example.com as hostmaster.example.com.). Precede any dot before the @ in the original address with a backslash (\) (for example, enter hostmaster.marketing@example.com as hostmaster\.marketing.example.com.).

Step 11  Enter an authoritative nameserver name under Nameservers further down the page, then click Add Nameserver.
Authoritative nameservers validate the data in their zones. Both primary and secondary servers can be authoritative. The crucial difference is where they get their zone data. A primary server obtains its data from an administrator, as stored in the server configuration database, and from DNS updates, typically from a DHCP server. A secondary server obtains the zone data from its designated master servers by way of a zone transfer.

You must add at least one nameserver for a zone—Cisco Prime Network Registrar does not consider the zone data complete unless you do so. The nameservers you list should be those that you want people outside your domain to query when trying to resolve names in your zone. You must add the authoritative nameservers in addition to the primary server for the zone. If the primary DNS server for the zone is in the zone, you must create a host address for it.

For every DNS internal-to-zone nameserver, you must create an Address (A) resource record (RR) to associate the server domain name with an IP address:

1. Click Host to open the List Zones page.
2. Click the zone name to open the List/Add Hosts for Zone page.
3. Enter the hostname of the authoritative server.
4. Enter its IP address.
5. Click Add Host. The server hostname and address appear in the list.
6. To edit the host, click its name to open the Edit Host page. Click Modify to implement the changes.

Step 12 Configure additional attributes as needed.
Step 13 Click Save.

CLI Commands

To create a primary zone, use zone name create primary nameserver contact. You must specify a primary DNS server; this server becomes the first authoritative DNS nameserver. For example:

```
nrcmd> zone example.com create primary ns1 hostmaster
```

The serial number defaults to 1. You can get the actual serial number by using zone name get serial (if the DNS server is running; if the server is not running, or listing or showing the zone attributes, it always returns the suggested serial number).

To add additional authoritative nameservers for the zone, enter a comma-separated list of fully qualified domain names using zone name set nameservers=list. Note that only the first server entered is confirmed by the command. Use zone name show to show all the server names.

Use zone name addRR hostname A address to add the authoritative server hostname and address. To list the host, use zone name listHosts. To remove the host, use zone name removeRR hostname A.

If you want to apply an existing template while creating a zone, use the template attribute. For example:

```
nrcmd> zone example.com create primary ns1 hostmastertemplate=zone-template-1
```

**Note**

In this example, even though you need to specify the nameserver and contact as part of the syntax, the template definition (if any) overwrites them.

To apply a template after creating the zone, use zone name applyTemplate template. For example:

```
nrcmd> zone example.com applyTemplate zone-template-1
```
Editing Primary Zones

You can edit a primary zone to modify its properties, apply a template to it, or use the zone definition to create a template from it.

Local Advanced and Regional Web UI

Step 1  From the Design menu, choose Forward Zones under the Auth DNS submenu to open the List/Add Forward Zones page.
Step 2  Select the zone in the Forward Zones pane to open the Edit Zone page.
Step 3  Make attribute changes as necessary.
Step 4  To apply a template to the zone, choose a template name from the drop-down list at the bottom of the page, then click Apply Template.

Caution  Be careful applying a template to a zone that is already live. Explicitly defined attributes on the template replace the existing ones defined for the zone.

Step 5  To use the zone definitions to create a template from them while modifying the zone, click Modify Zone and Save Template. On the Save New Zone Template page, give the template a name in the Value field, then click Save Zone Template. You return to the List/Add Zones page.

Confirming Zone Nameserver Configuration

Confirm your zone NS RR configuration by looking at the RRs that you created.

Local Advanced and Regional Web UI

Select the zone from the Forward Zones pane, and click the Resource Records tab. There should be an A record for each nameserver host in the zone. Edit these records or add more on this page.

See Adding Resource Record to Zone, on page 102.

CLI Commands

Use zone name listRR to check the RRs you added.

Synchronizing Zones

If a zone needs to be synchronized, in the regional server, click the Zone Sync tab for the Primary Forward/Reverse zone. Click the Sync Zone - Report button to open a Synchronize Zone page. Expert mode includes an additional Sync CCM Hosts from RR Data - Report button.

Manual zone synchronization should only be used when there is an inconsistency between the HA main and HA backup that is not being resolved automatically by the servers.

Zone Commands

The List/Add Zones (Forward/Reverse) page includes a Commands button. When clicked, this opens the Commands dialog box. These commands serve specific purposes:
- **Scavenge zone**—See the "Scavenging Dynamic Records" section in *Cisco Prime Network Registrar 8.3 DHCP User Guide*.

- **Get scaveng start time**—See the "Scavenging Dynamic Records" section in *Cisco Prime Network Registrar 8.3 DHCP User Guide*.

- **Synchronize HA Zone (Forward Zones)**—See Synchronizing HA DNS Zones, on page 67

---

**Note**

You can see the Synchronize HA Zone command only if the server is an HA main server. You cannot see this command if it is an HA backup server.

---

**Importing and Exporting Zone Data**

The easiest and quickest way to create a primary zone is to import an existing BIND format zone file, defined in RFC 1035. You can also export these same kinds of files to another server. BIND 4.x.x uses a boot file, called named.boot, to point the server to its database files. You can import your entire BIND 4.x.x configuration using the `import` command in the CLI. BIND 8 and BIND 9 use a configuration file, called named.conf, with a different syntax.

You can import and export zone data only by using the CLI.

When a BIND file contains an `$INCLUDE` directive, BIND searches for the include file relative to the directory that the directory directive in the named.boot file specifies. In contrast, the `nrcmd` program searches for the include file relative to the directory containing the zone file being processed.

To avoid this problem, ensure that the BIND configuration uses absolute paths whenever specifying an include file in a zone file. If your zone files contain relative paths when specifying include files, and the directory containing the zone file is not the same as the directory that the directory directive in the named.boot file specifies, your configuration cannot load properly. You need to convert the relative paths in your zone files to absolute paths so that you can import your BIND configuration into Cisco Prime Network Registrar. Here is an example of a configuration and how to fix paths in directory hierarchy, configuration files, and zone files:

- **Directory hierarchy:**

  ```
  /etc/named.conf
  /etc/named.boot
  /usr/local/domain/primary/db.example
  /usr/local/domain/primary/db.include
  /usr/local/domain/secondary
  ```

- **Configuration file (/etc/named.conf):**

  ```
  #BIND searches for zone files and include files relative to /usr/local/domain
  option directory /usr/local/domain
  #BIND finds zone file in /usr/local/domain/primary
  zone example.com {
  type master ;
  file primary/db.example ;
  #end of /etc/named.conf
  ```

- **Configuration file (/etc/named.boot):**

  ```
  ```
#BIND searches for zone files and include files relative to /usr/local/domain
directory /usr/local/domain
#BIND finds zone file in /usr/local/domain/primary
primary.example.com primary/db.example
#end of /etc/named.boot

• Incorrect zone file (/usr/local/domain/primary/db.example):

#BIND searches for include file relative to /usr/local/domain
$INCLUDE primary/db.include
#end of /usr/local/domain/primary/db.example

To make the configuration loadable, change the relative path ($INCLUDE primary/db.include) in the file
db.example to an absolute path ($INCLUDE /usr/local/domain/primary/db.include).

The following table describes the named.boot and named.conf file directives that BIND 4 and BIND 9 support,
and the corresponding Cisco Prime Network Registrar user interface location or syntax, if any.

### Table 6: BIND-to-CLI Command Mappings

<table>
<thead>
<tr>
<th>BIND 4 Command</th>
<th>BIND 9 Command</th>
<th>Mapping to User Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>—</td>
<td>acl name { addr-match-list ;}</td>
<td>Web UI: List/Add Access Control Lists page fields (see the &quot;Assigning ACLs on DNS Caching Servers or Zones&quot; section in Cisco Prime Network Registrar 8.3 DHCP User Guide). CLI: acl name create value match-list=addr-match-list</td>
</tr>
<tr>
<td>—</td>
<td>key id { algorithm string ; secret string ;}</td>
<td>Web UI: List/Add Encryption Keys page fields. CLI: key name create secret algorithm=alg</td>
</tr>
<tr>
<td>—</td>
<td>options { allow-query addr-match-list ;}</td>
<td>Web UI: Edit DNS Server page, enable restrict-query-acl CLI: dns set restrict-query-acl</td>
</tr>
<tr>
<td>options listen-on port</td>
<td>options { listen-on port {addr-match-list } ;}</td>
<td>Web UI: Edit DNS Server page, set Listening port. CLI: dns set local-port-number=port</td>
</tr>
<tr>
<td>options max-cache-ttl num</td>
<td>options { max-cache-ttl num ;}</td>
<td>Web UI: Edit DNS Server, set Max. RR caching TTL. CLI: dns set max-cache-ttl=num</td>
</tr>
<tr>
<td>options no-fetch-glue</td>
<td>options { fetch-glue no ;}</td>
<td>Web UI: Edit DNS Server page, enable Don’t fetch missing glue records. CLI: dns enable no-fetch-glue</td>
</tr>
<tr>
<td>options notify yes</td>
<td>options { notify yes ;}</td>
<td>Web UI: Edit DNS Server page, enable Send zone change notification (NOTIFY). CLI: dns enable notify</td>
</tr>
<tr>
<td>options rrset-order order order ...</td>
<td>options { rrset-order order ; order ; ... ;}</td>
<td>Web UI: Edit DNS Server page, enable Enable round-robin. CLI: dns enable round-robin</td>
</tr>
</tbody>
</table>
### Configuring Primary Reverse Zones

For a correct DNS configuration, you must create a reverse zone for each network that you use. A reverse zone is a primary zone that DNS clients use to convert IP addresses back to hostnames, and resides in a special in-addr.arpa domain. You can create a reverse zone manually or import it from BIND. You can also create reverse zones from subnets (see Adding Reverse Zones from Subnets, on page 81).

#### Related Topics

- Adding Reverse Zones as Zones, on page 79
- Adding Reverse Zones from Subnets, on page 81

### Adding Reverse Zones as Zones

You can manually add a reverse zone as a zone.

#### Local Basic or Advanced and Regional Web UI

From the Design menu, choose Reverse Zones under the Auth DNS submenu to open the List/Add Reverse Zones page. This page is almost identical to the List/Add Forward Zones page. Then, add a reverse zone the same way you would add a forward zone, as described in Configuring Primary Forward Zones, on page 73, except use the reverse of the forward zone network number added to the special in-addr.arpa domain as the zone name. Use the same template or SOA and nameserver values as you used for the related forward zone.

You can enter a DHCPv4 subnet or DHCPv6 prefix value in the Name field, which converts the subnet or prefix into an appropriate reverse zone name.

<table>
<thead>
<tr>
<th>BIND 4 Command</th>
<th>BIND 9 Command</th>
<th>Mapping to User Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>options support-ixfr yes</td>
<td>options { request-ixfr yes ; }</td>
<td>Web UI: Edit DNS Server page, enable Request incremental transfers (IXFR). CLI: dns enable ixfr-enable</td>
</tr>
<tr>
<td>options transfer-format</td>
<td>options { transfer-format many-answers ; }</td>
<td>Web UI: Edit DNS Server page, enable Use multi-rec format for zone transfers. CLI: dns enable axfr-multirec-default</td>
</tr>
<tr>
<td>many-answers</td>
<td></td>
<td></td>
</tr>
<tr>
<td>primary zonename file</td>
<td>zone &quot;name&quot; { type master; }</td>
<td>Web UI: Add Zone page fields. CLI: zone name create primary file=file</td>
</tr>
<tr>
<td>secondary zonename addr list</td>
<td>zone &quot;name&quot; { type slave; }</td>
<td>Web UI: Add Secondary Zone page fields. CLI: zone name create secondary ip-addr[ip-addr ...]</td>
</tr>
<tr>
<td>addr list [backupfile ]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>—</td>
<td>zone &quot;name&quot; { allow-query { addr ; ... } ; }</td>
<td>Web UI: Edit Zone page, set restrict-query-acl. CLI: zone name set restrict-query-acl=addr [addr ...]</td>
</tr>
<tr>
<td>tcplist addrlist xfernets addrlist</td>
<td>zone &quot;name&quot; { allow-transfer { addr ; ... } ; }</td>
<td>Web UI: Edit Zone page, enable restrict-xfer and set restrict-xfer-acl zone name set restrict-xfer-acl=addr [addr ...]</td>
</tr>
</tbody>
</table>
To create a reverse zone by using an IPv4 subnet or an IPv6 prefix, do the following:

### Local Basic or Advanced and Regional Web UI
To create a reverse zone by using the name of an IPv6 prefix, do the following:

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

**Step 2**
- In the List/Add Reverse Zones page, click the **Add Reverse Zone** icon in the Reverse Zones pane, enter values in the Name field, for example:
  - **209.165.201.1/24** — Creates a reverse zone by using an IPv4 subnet.
  - **2001:db8:ff80:ff80::/64** — Creates a reverse zone by using an IPv6 prefix.

**Step 3**
- Enter the required fields to create the reverse zone:
  - **Nameserver** — Enter `ns1.example.com` (include the trailing dot).
  - **Contact E-Mail** — Enter `hostmaster.example.com` (include the trailing dot).
  - **Serial Number** — Enter 1.

**Step 4**
- Click **Add Reverse Zone**. The List/Add Reverse Zones page appears.

---

### CLI Commands
Use `zone name create primary` and `zone name addRR PTR` to add the primary reverse zone and pointer records for the server. You can also apply a zone template.

To create a reverse zone by using:

- An IPv4 subnet

  For example, you can enter:

  ```
  nrcmd> zone 209.165.201.1/24 create primary ns1.example.com. hostmaster.example.com.
  ```

- An IPv6 prefix

  For example, you can enter:
Adding Reverse Zones from Subnets

An alternative to creating reverse zones manually is to create them from existing subnets. You can do this in the web UI only.

**Local Advanced and Regional Web UI**

1. From the Design menu, choose Subnets under the DHCPv4 submenu to open the List/Add Subnets page.
2. Create a subnet for the reverse zone, or use one of the existing subnets.
3. Click the Reverse Zone tab, and choose an existing zone template.
4. Click Report to show the changesets for the creation.
5. Click Revert to return to the List/Add Subnets page.
6. Confirm the creation by clicking Run, then Reverse Zones to see the newly created zone on the List/Add Reverse Zones page.

**Getting Zone Counts on the Server**

You can view the created zones associated with the DNS server, hence obtain a count, in the web UI.

Using the CLI, you can get an exact count of the total zones for the DNS server by using `dns getZoneCount [forward | reverse | primary | secondary | all]`. With no options specified, the command returns the total number of published zones only.

**Enabling DNS Updates**

DNS Update (RFC 2136) integrates DNS and DHCP so that they can work together. DNS update automatically records the association between the hosts and their DHCP-assigned addresses. Using DHCP and DNS update, you can configure a host automatically for network access whenever it attaches to the network. You can locate and access the host using its unique DNS hostname.

DNS update is described more fully in the "Managing DNS Update" chapter in Cisco Prime Network Registrar 8.3 DHCP User Guide. The chapter includes sections on the following:

- **Update policy (the Update Policies tab)**—Determines what kind of RRs you want updated when name-to-address associations change through DHCP. (See the "Configuring DNS Update Policies" section in Cisco Prime Network Registrar 8.3 DHCP User Guide.)
• **Update map (the Update Maps tab)**—Defines an update relationship between a DNS server or HA DNS pair and a DHCP failover pair, DHCP policies, client-class, or access control list. (See the "Creating DNS Update Maps" section in Cisco Prime Network Registrar 8.3 DHCP User Guide.)

## Managing Secondary Servers

When you configure a zone, choose at least one secondary server. If you have only one nameserver and it becomes unavailable, there is nothing that can look up names. A secondary server splits the load with the primary or handles the whole load if the primary is unavailable. When a secondary server starts up, it contacts the primary and pulls the zone data over. This is known as a zone transfer.

**Note**

Zone transfer in secure mode supports both HMAC-MD5 based TSIG and GSS-TSIG.

**Tip**

If the authoritative server for your secondary zones is also running Cisco Prime Network Registrar 6.0 or later, see Managing Zone Distributions, on page 87 for how to avoid entering these zones manually. If you have only one secondary server, remove it geographically from the primary. They should not be on the same network segment, switch, or router, but on a different cluster entirely.

You can configure a secondary DNS server to be responsible for a secondary zone, which makes the server a secondary for that zone. You also need to give the address of the master server from which to perform zone transfers. Cisco Prime Network Registrar must know about this master server.

## Adding Secondary Forward Zones

You can add a secondary forward zone at the local cluster.

### Local Basic or Advanced Web UI

**Step 1**

From Design menu, choose Secondary Zones under the Auth DNS submenu to open the List/Add Secondary Zones page.

**Step 2**

Click the Add Secondary Zone icon in the Secondary Zones pane to open the Add Secondary Zone dialog box.

A secondary zone requires a name and a list of one or more master servers. You can also enable restricting zone transfers to a set of hosts, then enter the access control list (ACL) of the restricted hosts in the restrict-xfer-acl field. Enter other attribute values as necessary.

**Step 3**

Click Add Secondary Zone.

Clicking the name of the secondary zone in the Secondary Zones pane opens the Edit Secondary Zone page where you can edit the secondary zone. Click Save on this page.

You can add the secondary reverse zone the same way you do a secondary forward zone, except that the address must be a reverse zone address.
CLI Commands

To create a secondary zone, use `zone name create secondary address`. You must specify the primary DNS server IP address to perform the zone transfer.

For example:

```
nrcmd> zone shark.zone. create secondary 172.18.123.177
```

If you are using HA DNS server pair, the IP addresses must be provided by separating the addresses with comma. The HA DNS backup server will be used when the primary server is unavailable.

For example:

```
nrcmd> zone shark.zone. create secondary 172.18.123.177,172.18.123.45
```

Enabling Zone Transfers

A secondary server periodically contacts its master server for changes, called a zone transfer. The interval is defined in the server SOA record as the secondary refresh time. You can restrict zone transfers by setting the `restrict-xfer` attribute to true (the preset value is false) on the master server. You have to set the `restrict-xfer-acl` setting accordingly.

Note: If you restrict zone transfers, the `nslookup` utility `ls` command may fail because it tries to do a full zone transfer, unless you include the IP address that `ls` runs from in the zone `restrict-xfer-acl` list.

Before you begin

Prereq

Local Advanced and Regional Web UI

Step 1
In the Forward Zones pane, click the name of the primary zone to open the Edit Zone page.

Step 2
In the zone attributes area, you can set the `restrict-xfer` attribute to false (the preset value). If you set the attribute to true, you can also specify a list of servers to which to restrict the zone transfers by using the `restrict-xfer-acl` attribute, separating the IP addresses with commas.

Secondary zones can also restrict zone transfers from other secondary zones, so that the `restrict-xfer` and `restrict-xfer-acl` attributes are also available for secondary zone configurations.

Step 3
Click Save.

Step 4
You can force zone transfers for the DNS server in two ways:

- On the Secondary Zones pane, click the Full Zone Transfer button.

- To force all zone transfers from the primary server, on the Manage DNS Authoritative Server page, click the Commands button to Force all zone transfers.
CLI Commands

In the CLI, zone transfers are enabled by default, unless you restrict them using `zone name enable restrict-xfer`. If you want to force a zone transfer, use `zone name forceXfer secondary`.

Configuring Subzones

As the zone grows, you might want to divide it into smaller pieces called subzones. You can delegate administrative authority for these subzones, and have them managed there or served by separate servers. This partitioning is called subzone delegation. Establish subzone delegation by performing these tasks:

1. Choose a subzone name.
2. Specify a nameserver name.
3. Specify a nameserver address.

Related Topics

Choosing Subzone Names and Servers, on page 84
Creating and Delegating Subzones, on page 85
Undelegating Subzones, on page 86
Editing Subzone Delegation, on page 86

Choosing Subzone Names and Servers

After you decide to divide the zone into subzones, you must create names for them. Involve the people responsible for the subzones in deciding their names, and try to maintain a consistent naming scheme.

These suggestions can help you avoid subzone naming problems:

- Consider not naming a subzone by its organizational name. In a changing business environment, organizations merge and are renamed. Naming a subzone after an organization could result in a name that is no longer meaningful over time.
- Consider not using geographical names that indicate the subzone location. Geographical names are meaningless to people outside your organization.
- Do not use cryptic names; make them obvious.
- Do not use existing or reserved top-level domain names as subzones. Using existing names can result in routing problems.

After you choose a subzone name, specify its nameservers, the ones the parent domain nameservers use when queried about the subzone. To ensure that the subzone is always reachable, you should specify two nameservers. They must be authoritative for this zone as either primary or secondary.

Whenever a subzone nameserver changes its name or address, the subzone administrator must inform its parent zone so that the parent zone administrator can change the subzone nameserver and glue records. A glue record is an A record with the address of a subzone authoritative nameserver. If the subzone administrator fails to inform its parent, the glue records are invalid. The common symptom is that a host cannot reach a host in another domain by its name, only by its address.
Creating and Delegating Subzones

You delegate a subzone by creating it in the parent zone. There should be one NS record for each nameserver to which the subzone is delegated. Each NS record requires a corresponding A record describing the address of the nameserver, unless the nameserver is outside the parent zone or subzone. This A record is called a glue record. Such a zone which creates the NS RR and corresponding A records (glue records) for point of delegation in the parent zone is called a parented zone. A zone that does not create the NS RR and corresponding A records (glue records) for point of delegation in the parent zone is called an unparented zone.

Consider a zone example.com with a parent zone .com and a subzone subdomain.example.com. If example.com is a parented zone, NS RR for the example.com appears in two places; within the example.com and within its parent zone .com. Within example.com are authoritative records for the nameservers for the zone, at the point of delegation for either a subdomain of the zone or in the parent zone. The parent zone .com will contain non-authoritative NS RR for example.com at its point of delegation and subdomain.example.com will have non-authoritative NS RR in example.com at its point of delegation.

See Choosing Subzone Names and Servers, on page 84

Local Basic or Advanced Web UI

Step 1 Create a zone as a subdomain of the parent domain on the List/Add Forward Zones page:
- If applying a zone template, go to Step 2.
- If not applying a zone template, on the List/Add Forward Zones page, click the Add Forward Zone icon and add the SOA records and the nameserver with its address.

Step 2 If Cisco Prime Network Registrar detects a parent zone based on the subzone name, the Create Subzone in Parent Zone page appears. Click Create as Subzone (or Create as Unparented Zone if you do not want it to be a subzone) on this page.
Creating as subzone will create the NS RR and corresponding A records (glue records) for point of delegation in the parent zone.

Step 3 If you configured a nameserver in the subzone, you need to create a glue Address (A) record for it. In the field provided, enter the IP address of the nameserver, then click Specify Glue Records. (If there are multiple subzone nameservers, there are multiple fields for the glue records.)

Step 4 Click Report to show the intended changesets for the added records.

Step 5 Click Return after viewing the actual changesets implemented.

Step 6 To confirm the added records for the subzone, click the View icon in the RR column for the subzone. The glue A record or records for the subzone nameserver should appear. Click Return to Zone List.

Step 7 To confirm the added records for the parent zone, click the View icon in the RR column for the parent zone. The subzone nameserver (NS) record or records plus the glue A record or records for them should appear. Click Return to Zone List.
CLI Commands

On the subzone primary nameserver machine, create the subdomain:

```
nrcmd> zone boston.example.com. create primary bostonDNSserv1 hostmaster
```

On the parent zone nameserver machine, add an NS record for the subzone nameserver, then Create a glue A record for the subzone nameserver:

```
nrcmd> zone example.com. addRR boston NS bostonDNSserv1.boston.example.com.
nrcmd> zone example.com. addRR bostonDNSserv1.boston.example.com. A 192.168.40.1
```

Editing Subzone Delegation

You can edit the subzone RRs.

Local Basic or Advanced and Regional Web UI

**Step 1**
On the corresponding Edit Zone page, click the Resource Records tab, edit the NS RR for the subzone by clicking the Edit icon next to the record to open the Edit RR in Zone page.

**Step 2**
Edit the NS record data.

**Step 3**
Click Modify Resource Record.

**Step 4**
Edit the glue A RR for the subzone server in the same way as in the previous steps.

CLI Commands

Use `zone name removeRR` to delete the NS and glue A records, then use `zone name addRR` to replace them.

Undelegating Subzones

If you undelegate a subzone, you need to remove any associated NS and glue A records from the parent zone.

**Note**
If you delete the subzone, Cisco Prime Network Registrar cleans up the delegation records automatically.

Local Basic or Advanced and Regional Web UI

On the corresponding Edit Zone page, click the Resource Records tab, delete the NS record for the subzone, then delete the glue A record for the subzone server host.

CLI Commands

Use `zone name removeRR NS` and `zone name removeRR A` to remove the subzone NS and glue A records.
Managing Zone Distributions

Creating a zone distribution simplifies creating multiple zones that share the same secondary zone attributes. It simplifies to a great extent the setup and management of multiple clusters sharing zone relationships such as primary to secondary or main to backup in the case of DNS HA.

The zone distribution requires adding one or more predefined secondary servers. Running a zone distribution synchronization adds secondary zones managed by secondary (slave) servers for each primary zone managed by a primary server. You can also use zone distributions to synchronize zone data from the CCM database to the local DNS server and regional and local cluster zone data. Synchronizing the zone data will always sync the associated views and named ACLs for both primary and secondary zones.

The distribution must be in a star topology, that is, one primary server and multiple secondary servers. The authoritative (master) server can only be the local primary server where the zone distribution default is defined. Starting with Cisco Prime Network Registrar 6.2, you can manage one zone distribution at the local cluster and multiple distributions at the regional clusters.

Related Topics

- Preparing the Zone Distribution Map, on page 87
- Creating a Zone Distribution, on page 89
- Pulling Zone Distributions from Replica Data, on page 91

Preparing the Zone Distribution Map

To prepare for creating a zone distribution, draw a zone distribution map diagram on paper.

### Step 1

Start by identifying the HA DNS pair that is primary (or the primary server if HA is not involved) for all the zones that you include in the map:

a) Create a box for each server in the HA DNS pair. For example, the server pair for the Chicago-cluster consists of the servers at 192.168.50.1 and 192.168.60.1.

b) Write the IP addresses of each server in each box.

c) Write a P (for Primary) inside each box (see the image below).
Step 2 Identify the role as master for each server by writing an M below the box. In the example, both primary servers are, by definition, also masters that will send copies of their zones to other servers over zone transfers. Even so, write the M below the box to make later steps easier.

Step 3 Identify all slave servers that will receive zone transfers directly from these masters. Below the master server boxes on the page, add a box for each slave, and write its IP address inside the box. For example, the slave servers at 192.168.70.1 and 192.168.80.1 get zone transfers from the Chicago-cluster masters.

Step 4 Write an S above each slave server box.

Step 5 Draw arrows from the M to each S representing the zone transfer flow (see the diagram). In this HA DNS example, the arrows go from each master to both slaves.

Step 6 As you can see from the diagram, you can extend the boxes further so that the original slaves can become masters to another set of servers (a.b.c.d and w.x.y.z).

Step 7 Enter the IP address in each box with an M below it in the Master Servers list when creating the zone distribution. In the CLI, set the master-servers attribute to the list of IP addresses; for example:

```
nrcmd> zone-dist dist-1 create Chicago-cluster master-servers=192.168.50.1,192.168.60.1
```

Step 8 From the Secondary Servers drop-down list on the Add or Edit Zone Distribution Secondary Server page, choose the cluster associated with the slave server IP addresses in the boxes that have an S above them.

In the CLI, use `zone-dist name addSecondary cluster`; for example:

```
nrcmd> zone-dist dist-1 addSecondary Boston-cluster
```
Creating a Zone Distribution

If you move a zone from one zone distribution to another, synchronize the first zone distribution, move the zone, then synchronize the second zone distribution.

Local Basic or Advanced and Regional Web UI

Step 1
From Deploy menu, choose Zone Distributions (for the regional cluster) or Zone Distribution (for the local cluster). The option is available if the server is configured with authoritative service. This opens the regional List/Add Zone Distributions page or the local View Zone Distribution page. Note that the default zone distribution is predefined at both clusters; however, the default cluster is the only one available at the local cluster.

Step 2
To add a new zone distribution, click the Add Zone Distribution icon to open the Add Zone Distribution dialog box. To edit an existing zone distribution, select its name to open the Edit Zone Distribution page.

Step 3
In the Primary Server field, enter the cluster (or configured HA DNS pair) that has the primary server. This primary server is authoritative for the zones that you will determine further down the page. This selection is subtractive: the next zone distribution you create will no longer have the cluster that you set here as one of the choices.

Step 4
In the Master Servers list, add the IP address (and optional key) for each master server. The master server is generally the primary server. However, you might want to set up a hierarchy of primaries and secondaries where you need to define the master servers for each of the secondary relationships. You might also want to determine the HA DNS server pairs from the master server list. You can also add an optional TSIG key or GSS-TSIG keys (see the "Transaction Security" or "GSS-TSIG " section in the Cisco Prime Network Registrar 8.3 DHCP User Guide) to the master server address by hyphenating the entry in the format address–key. For each entry, click Add IP Key.

Step 5
For a zone distribution, you need to add at least one secondary server. Click Add Secondary Server on the Edit Zone Distribution page to open the Add Zone Distribution Secondary Server page. Here, choose the cluster of the secondary server. Optionally, if the master servers are other than the primary servers indicated for the zone distribution, add the master server addresses, separating multiple addresses with commas. After clicking Add Server returns you to the Edit page, you can connect to the secondary server cluster, delete it, or edit it to change the master servers.

To manage the secondary servers in the zone distribution, click the View icon in the Manage Servers column to open the List Secondary Servers page. You can also edit the secondary server on an Edit Zone Distribution Secondary Server page.

Step 6
Choose the forward and reverse zones for the zone distribution. The default zone distribution includes all the created forward and reverse zones. For all other created zone distributions, you must move the zone or zones into the Selected column.

Step 7
Click Save.

Step 8
Synchronize the zone distribution with the local cluster DNS servers. A synchronization:

• Pushes staged zone, RR, or host edits to the primary server cluster or HA DNS pair for the regional cluster in Ensure, Replace, or Exact modes, or from the local cluster in Exact mode.

• Creates secondary zones for secondary servers, in Exact mode.

Step 9
Click the Synchronize Zone Distribution tab, and choose a synchronization mode:

• Update—Adds new zones, RR sets, and hosts; replaces existing hosts if there are conflicts; and creates new secondary zones.
• **Complete**—Like Ensure mode, except that it always replaces existing RR sets and hosts, and modifies the master server list on existing secondary zones.

• **Exact**—Like Complete mode, except that it deletes extra zones, RR sets, hosts, and secondary zones no longer on the primary.

**Step 10**
Click Report in the Synchronize Zone Distribution tab (or the same icon in the Synchronize All Zone Distributions area of the page at the regional cluster). This opens the Sync Zone Distribution page that shows a preview of the data synchronized.

### CLI Commands

To create the zone distribution, use `zone-dist name create primary-cluster`. (The primary cluster can also be the HA DNS pair.) For example:

```
nrcmd> zone-dist dist-2 create Chicago-cluster
```

To set the master server or servers, use `zone-dist name set master-servers=addresses`, separating the addresses with commas. For example:

```
nrcmd> zone-dist zone-dist-2 set master-servers=192.168.50.1,192.168.60.1
```

To add the secondary server, use `zone-dist name addSecondary secondary-cluster`. For example:

```
nrcmd> zone-dist zone-dist-2 AddSecondary Boston-cluster
```

You must associate the zone distribution directly with the zone or zone template. Use `zone name set dist-map=zone-dist-list` or `zone-template name set dist-map=zone-dist-list`, separating the zone distribution entries with commas. For example:

```
nrcmd> zone example.com set dist-map=zone-dist-2
nrcmd> zone-template zone-template-1 set dist-map=zone-dist-2
```

To synchronize the zone distributions, use `zone-dist name sync`. You can do a synchronization in update, complete, or exact mode, and you can exclude RRs and secondary zones:

- **At the local cluster,** this synchronizes staged edits to the DNS server and primary zones to secondaries. Regardless of the synchronization mode, this always synchronizes the exact list of authoritative zones.
- **At the regional cluster,** this synchronizes primary zones with the local clusters, and primaries to secondaries. This replaces primary zones at the local cluster in Update and Complete modes, and deletes extra primary zones at the local cluster in Exact mode.
- **For secondary zones,** the same synchronization logic occurs at the local and regional clusters. In Update mode, this ensures that corresponding secondary zones exist on the server. In Complete mode, existing zones are updated to use the master server list specified by the zone distribution map. In Exact mode, any zones not matching the distribution map are deleted.

For example:

```
nrcmd> zone-dist zone-dist-1 sync exact no-rrs no-secondaries
```
Pulling Zone Distributions from Replica Data

You can pull zone distributions from the local replica data instead of explicitly creating them.

Tip
For an example of pulling local zone data to create a zone distribution, see the "Pull Zone Data and Create a Zone Distribution" section in Cisco Prime Network Registrar 8.3 Administrator Guide.

Regional Web UI

Step 1 From Deploy menu, choose Zone Distribution. This opens the regional List/Add Zone Distribution page.
Step 2 On the List/Add Zone Distribution page, click the Synchronize Zone Distribution tab in the Zone Distributions pane.
Step 3 Choose the data synchronization mode (Update, Complete, or Exact). These modes are described in the table on that page.
Step 4 Click Report at the bottom of the dialog box.
Step 5 Click Run.

Managing DNS ENUM Domain

Creating separate ENUM domains simplifies the management of Naming Authority Pointer (NAPTR) Electronic Numbering (ENUM). It simplifies to a great extent the setup and management of E.164 numbers and how available services are connected to the E.164 numbers. When you create an ENUM zone and add the corresponding E.164 numbers, Cisco Prime Network Registrar automatically creates a forward zone and the respective NAPTR resource records.

Managing DNS ENUM Defaults

To configure the default ENUM settings, do the following:

Local Basic or Advanced Web UI

Step 1 From the Design menu, choose Defaults under the DNS ENUM submenu to open the Manage DNS ENUM Defaults page.
Step 2 Enter the Top-level Domain.
Step 3 Enter the Local Prefix such as +46.
Step 4 Enter the Default Services values: select a service type, enter a URI, and click Add Service.
Step 5 Select a Zone Template.
Step 6 Click Save.

CLI Commands

Using the CLI, you can set the default ENUM domain, default top-level domain and local prefix, service, and zone template by using:
Adding DNS ENUM Domains

Adding an ENUM domain involves creating a domain name. You can also define an owner and use a zone template.

When you create an ENUM zone, Cisco Prime Network Registrar automatically creates a forward zone. For example, if you create an ENUM domain for E.164 number prefix 100 and the default top-level domain is set to e164enum.net., a forward zone 0.0.1.e164enum.net. is automatically created and appears in the list of forward zones.

This section explains how to configure an ENUM domain.

**Local and Regional Web UI**

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

**Step 2**  
Click the Add Domains icon in the Domains pane to open the Add ENUM Domain dialog box.

**Step 3**  
Enter the E.164 number prefix for the domain, such as 897.

**Step 4**  
Enter the name of the nameserver host, such as ns1.

**Step 5**  
Enter the contact e-mail name, such as hostmaster.

**Step 6**  
Click Add ENUM Domain. The domain will be created with the default local prefix such as +4689. The Basic mode creates the zone with the following preset values:

- Zone default TTL-24h
- Start of Authority (SOA) serial number-1
- SOA secondary refresh time-3h
- SOA secondary retry time-60m
- SOA secondary expiration time-1w
- SOA minimum TTL-10m

**CLI Commands**

The ENUM domain commands are shown in the table below:

<table>
<thead>
<tr>
<th>Action</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create</td>
<td>dns-enum-domain prefix create [zone-template-name] [nameservers [person]]</td>
</tr>
</tbody>
</table>
Adding DNS ENUM Numbers

Cisco Prime Network Registrar supports NAPTR RRs. These records help with name resolution in a particular namespace and are processed to get to a resolution service.

In addition to the option of adding NAPTR resource records, you can now directly add the E.164 numbers and associate the corresponding services with the numbers. When you add a DNS ENUM number, you need to specify either the E.164 number prefix of the parent domain or the Zone templates, and a NAPTR resource record is created for the E.164 number. This approach uses a reversed E.164 number and treats every digit as a node on the DNS name hierarchy. For example, the E.164 address +4689761234 creates a NAPTR RR 4.3.2.1.6.7.9.8 for the +46 E.164 prefix domain.

For more information on NAPTR resource records, see the Name Resolution in a Namespace Using NAPTR Resource Records, on page 108.

Local and Regional Web UI

Step 1  From the Design menu, choose Numbers under the DNS ENUM submenu to open the List/Add DNS ENUM Numbers page.
Step 2  Click the Add Numbers icon in the Numbers pane to open the Add ENUM Number dialog box.
Step 3  Enter the E.164 number along with the E.164 number prefix, such as 1234.
Step 4  Select a service type, enter a URI, and click Add Service.
Step 5  Enter the E.164 number prefix for the parent domain.
Step 6  Select the Zone Template if you have not specified the E.164 prefix.
Step 7  Select a Ported option and enter the Ported Nameserver FQDN.
Step 8  Click Add ENUM Number. The number will be created and added under the domain +4689.

CLI Commands

Using the CLI, you can add ENUM number by using:

dns-enum-number <number> create <type> <subtype> <uri> [zone-template-name] [domain-prefix]

Pulling and Pushing ENUM Domains

You can push ENUM Domains to and pull ENUM Domains from local clusters on the List/Add DNS ENUM Domains page in the regional cluster web UI.

Pushing ENUM Domains to Local Clusters

To push ENUM domains to the local cluster, do the following:

Regional Basic and Advanced Web UI
Pulling ENUM Domains from the Replica Database

To pull ENUM domains from the replica database, do the following:

**Regional Basic and Advanced Web UI**

**Step 1** From the Design menu, choose Domains under the DNS ENUM submenu to view the List/Add DNS ENUM Domains page in the regional web UI.

**Step 2** Click the Pull Replica icon in the Domains pane.

**Step 3** Click the Replica icon in the Update Replica Data column for the cluster. (For the automatic replication interval, see the Replicating Local Cluster Data section in *Cisco Prime Network Registrar 8.3 Administrator Guide*.)

**Step 4** Choose a replication mode using one of the Mode radio buttons.

**Step 5** Leave the default Replace mode enabled, unless you want to preserve any existing ENUM domains data at the local cluster by choosing Ensure.

**Step 6** Click the Pull all ENUM Domains button to view the pull details, and then click Run.

Pulling and Pushing ENUM Numbers

You can push ENUM numbers to and pull ENUM numbers from local clusters on the List/Add DNS ENUM Numbers page in the regional cluster web UI.

**Pushing ENUM Numbers to Local Clusters**

To push ENUM numbers to the local cluster, do the following:

**Regional Basic and Advanced Web UI**

**Step 1** From the Design menu, choose Numbers under the DNS ENUM submenu to view the List/Add DNS ENUM Numbers page in the regional web UI.
Pulling ENUM Numbers from the Replica Database

To pull ENUM numbers from the replica database, do the following:

**Regional Basic and Advanced Web UI**

Step 1  From the Design menu, choose Numbers under the DNS ENUM submenu to view the List/Add DNS ENUM Number page in the regional web UI.

Step 2  Click the Pull Replica icon in the Numbers pane.

Step 3  Click the Replica icon in the Update Replica Data column for the cluster. (For the automatic replication interval, see the Replicating Local Cluster Data section in *Cisco Prime Network Registrar 8.3 Administrator Guide*.)

Step 4  Choose a replication mode using one of the Mode radio buttons.

Step 5  Leave the default Replace mode enabled, unless you want to preserve any existing ENUM number data at the local cluster by choosing Ensure.

Step 6  Click the Pull all ENUM Numbers button to view the pull details, and then click Run.
Pulling ENUM Numbers from the Replica Database
Managing DNS Views

DNS Views let you present alternate versions of zone data to different communities of clients using a single name server. For example, a DNS server for example.com can maintain two views of the zone, where the view of example.com that can be queried internally includes many hosts that do not exist in the external view. Each zone view is treated as an independent copy of the zone. The DNS server, when answering queries on the zone, uses the match criteria defined in each view to determine the matching zone for the client. The query is answered based on that zone contents. In some cases, the zone contents may only vary slightly between views.

- DNS Views Processing, on page 97
- Key Points to Remember When you Work on DNS Views, on page 97
- Managing DNS Views, on page 98
- Reorder DNS Views, on page 98
- Synchronizing DNS Views, on page 99
- Pushing and Pulling DNS Views, on page 99

DNS Views Processing

DNS Views allow a name server to segregate the data and provide a different view of the data based on the clients accessing it. When DNS receives a DNS request, the request is processed to automatically associate it with a view for Cisco Prime Network Registrar servers.

Note

The auto-view detection is only applicable for Cisco Prime Network Registrar servers.

Views for the DNS client servers such as Caching DNS, Secondary DNS, Primary for Notifies, DHCP and so on are easily defined with minimal configuration.

Key Points to Remember When you Work on DNS Views

Following are some of the key points or attributes you should know when you work on DNS Views:

- View ID—Defines a unique integer identifier for the view that is assigned by the CCM server or the user while creating DNS views.
• **View Priority**—Each DNS View will be assigned a unique priority to determines its order in the view list. The lowest non-zero priority value will have the highest priority and will be processed first. A zero priority is reserved for the default view, which will always be last. The web UI will provide an option to reorder views without explicitly setting the priority.

• **Default View**—The default view is created with view-id=0, priority=0, and client and destination ACLs set to any. Requests that do not match a named view will always fall into the default view. By default, zones will be created with a view-id=0, which will automatically place them in the default view. The default view cannot be modified or deleted.

• **acl-match-clients attribute**—Specifies the ACLs that maps clients to this view based on the source address (subnet or prefix) or TSIG key.

**Managing DNS Views**

You can create, edit, and delete DNS Views from local or regional cluster. You can also push or pull views and ACLs in Ensure, Replace, and Exact modes from or to the regional CCM server.

---

**Note**

You can create a maximum of 100 views.

---

**Local Basic or Advanced and Regional Web UI**

To create DNS Views:

**Step 1** From the **Design** menu, choose **Views** under the **Auth DNS** submenu.

**Step 2** On the **Views** pane, click the **Add View** icon.

**Step 3** Specify the name for the DNS views.

**Step 4** Specify the view id. If you do not specify, the application automatically assigns a view id to the view.

**Step 5** You can specify the view id. If you do not specify, the application automatically assigns a view id to the view.

**Step 6** Click the **ACL** that maps the client to this view in the **acl-match-clients** field.

**Step 7** Click the **Add DNS View** button.

To edit a DNS View, click its name in the **Views** pane on the left.

---

**Reorder DNS Views**

When you create a set of DNS Views, you can specify the priority order. To specify the priority order:

**Step 1** From the **Design** menu, choose **View** under the **Auth DNS** submenu to open the List/Add Zone Views page.

**Step 2** Click the **Reorder Views** icon in the **Views** pane to open the Reorder dialog box.

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

* Select the view and click the **Move up** or **Move down** icon to reorder the rules.
* Select the view and click the **Move to** button, and enter the row number to move the view.
Step 4  Click **Save** to save the reordered list.
If you delete a view, you get a choice to delete all zones.

---

**CLI Commands**

Use *dns-view name create* to add DNS Views (see the *dns-view* command in the CLIGuide.html file in the install-path/docs directory for syntax and attribute descriptions).

**Synchronizing DNS Views**

Zone distribution sync, single zone sync, and HA DNS zone sync will always sync associated views and named ACLs for both primary and secondary zones. The synchronization modes applied while running zone distribution or HA DNS sync vary. When you run:

- **Zone Distribution Sync**—views will be synchronized in Replace mode for all zone distribution sync types (Update, Complete, and Exact), while ACLs will use Ensure mode. If caching DNS servers are included in the zone distribution, the associated views and named ACLs will be synchronized to these servers and the masters list will be configured as exceptions for the unique set of domain names in the distribution. The user must exclude secondaries and/or caching servers.
- **HA DNS Sync**—views will be updated in Replace mode for both Update and Complete sync, while Exact sync will sync views in Exact mode.

**Pushing and Pulling DNS Views**

You can also push views and ACLs to and pull views and ACLs from the regional cluster in Ensure, Replace, and Exact modes.

**Pushing DNS Views to Local Clusters**

You can push the views you create from the regional cluster to any of the local clusters.

**Regional Web UI**

**Step 1**  From the **Design** menu, choose **Views** under the **Auth DNS** submenu.

**Step 2**  On the **Views** pane, click the **Push All** icon in the left pane, or select a **DNS View** and click **Push** at the top of the Edit Zone View page. This opens the Push Data to Local Clusters or Push Zone View page.

**Step 3**  Choose a push mode using one of the **Data Synchronization Mode** radio buttons.

- If you are pushing all the DNS Views, you can choose Ensure, Replace, or Exact.
- If you are pushing a DNS View, you can choose Ensure or Replace.

In both the above cases, Ensure is the default mode.
Choose Replace only if you want to replace the existing DNS View data at the local cluster. Choose Exact only if you want to create an exact copy of the DNS View at the local cluster, thereby deleting all DNS Views that are not defined at the regional cluster.

**Step 4** Choose one or more local clusters in the Available field of the Destination Clusters and move it or them to the Selected field.

**Step 5** Click **Push Data to Clusters**.

---

**Pulling DNS Views from Local Clusters**

Instead of explicitly creating views, you can pull them from the local clusters. In the regional web UI, you may first want to update the view replica data by clicking the Replica icon next to the cluster name.

**Regional Web UI**

**Step 1** From the **Design** menu, choose **Views** under the **Auth DNS** submenu.

**Step 2** On the **List/Add Zone Distribution** page, click the **Pull Replica** icon in the **Views** pane.

**Step 3** Choose the data synchronization mode (**Update**, **Complete**, or **Exact**). These modes are described in the table on that page.

**Step 4** Click **Report** at the bottom of the dialog box.

**Step 5** Click **Run**.
Managing Resource Records

This chapter explains how to configure some of the more advanced DNS zone and server parameters by using the Cisco Prime Network Registrar web UI and CLI. Before you proceed with the concepts in this chapter, read Managing Zones, on page 69 which explains how to set up the basic properties of a primary and secondary DNS server and its zones.

• Managing Resource Records for Zone, on page 101
• Adding Resource Record to Zone, on page 102
• Editing Resource Records, on page 103
• Removing Resource Records from Zone, on page 103
• Managing Resource Records for Host, on page 104
• Protecting Resource Record Sets, on page 104
• Searching Server-Wide for Records and Addresses, on page 105
• Filtering Resource Records, on page 107
• Advertising Services to Network Using Service Location (SRV) Records, on page 107
• Name Resolution in a Namespace Using NAPTR Resource Records, on page 108

Managing Resource Records for Zone

Resource records (RRs) comprise the data within a DNS zone. Although there is no fixed limit to the number of RRs a zone may own, in general, a zone may own one or more RRs of a given type (the zone always has a Start of Authority, or SOA, record). There are some exceptions depending on the types involved. All RRs have the entries described in the following table.

<table>
<thead>
<tr>
<th>RR Entry</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Owner of the record, such as a zone or hostname.</td>
</tr>
<tr>
<td>Class (not required for all formats)</td>
<td>Cisco Prime Network Registrar supports only the IN (Internet) class.</td>
</tr>
<tr>
<td>TTL (time to live)</td>
<td>Amount of time to store the record in a cache, in seconds. If you do not</td>
</tr>
<tr>
<td></td>
<td>include a TTL, Cisco Prime Network Registrar uses the zone default TTL,</td>
</tr>
<tr>
<td></td>
<td>defined as a zone attribute.</td>
</tr>
</tbody>
</table>
## Related Topics

- Adding Resource Record to Zone, on page 102
- Protecting Resource Record Sets, on page 104
- Editing Resource Records, on page 103
- Removing Resource Records from Zone, on page 103
- Searching Server-Wide for Records and Addresses, on page 105
- Filtering Resource Records, on page 107
- Advertising Services to Network Using Service Location (SRV) Records, on page 107
- Name Resolution in a Namespace Using NAPTR Resource Records, on page 108

## Adding Resource Record to Zone

Before adding or modifying RRs, keep in mind the two distinct dns edit modes that you can set and work in: staged and synchronous (see the "Staged and Synchronous Modes" section in Cisco Prime Network Registrar 8.3 DHCP User Guide).

Administrator roles required for RR management are the dns-admin role at the local cluster and the central-dns-admin role at the regional cluster. The host-admin role at the local cluster and the central-host-admin role at the regional cluster can view host records only.

### Local Basic or Advanced and Regional Web UI

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Choose Forward Zones from Design &gt; Auth DNS to open the List/Add Forward Zones page.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>In the Forward Zone pane, click the zone name to open the Edit Zone page. Note that resource record edits is managed jointly by CCM and DNS and a system lock is used to prevent DNS and CCM from accessing the resource record database at the same time.</td>
</tr>
<tr>
<td><strong>Tip</strong></td>
<td>Records are listed in the formats that their respective RFCs specify, with only the first record in a set labeled with its name, and in DNSSEC order. To reduce or increase the items in the table, change the page size value at the bottom of the page, then click Change Page Size.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Click the Resource Records tab.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Add the RR name, TTL (if not using the default TTL), type, and data as appropriate.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>By default, RRs are protected, which means that DNS Updates cannot overwrite them (see Protecting Resource Record Sets, on page 104). To unprotect the RRs, click the Locked icon to the left of the record name to change it to the Unlocked icon. Likewise, to protect the record, click the Unlocked icon to change it to the Locked icon.</td>
</tr>
</tbody>
</table>

### RR Entry

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Type of the record, such as A (AAAA for IPv6), NS, SOA, and MX. There are many types that various RFCs define, although fewer than ten are in common use.</td>
</tr>
<tr>
<td>Record data</td>
<td>Data types whose format and meaning varies with record type.</td>
</tr>
</tbody>
</table>
Step 6  Click Add Resource Record.

---

**CLI Commands**

Use `zone name addRR` to add a protected RR of a certain type. You can specify the name as a relative name, if the owner is in the same domain, an absolute name (by supplying the FQDN), or the same name as the zone name (by using the at [@] symbol).

For example:

```
nrcmd> zone example.com addRR -sync host101 A 192.168.50.101
```

Use `zone name addDNSRR type data` to add an unprotected RR.

---

**Editing Resource Records**

You can edit RRs as an individual record or as an RR set:

- **Individual RRs**—Click the Edit icon next to the record name to open the Edit RR in Zone page.
- **RR sets**—Click the name of the record to open the Edit RR Set in Zone page.

For a description of the fields to enter data, see *Adding Resource Record to Zone, on page 102.*

---

**Removing Resource Records from Zone**

You can remove RRs from a zone.

**Local Basic or Advanced and Regional Web UI**

On the local or regional the Resource Records tab for the Zone page:

- To remove an entire record name set, click the Delete icon next to the record set name in the list, then confirm the deletion.
- To remove individual records from the set, click the name of the record set to open the edit page, click the Delete icon next to the individual record in the list, then confirm the deletion.

**CLI Commands**

The CLI includes two removal commands, depending on the type of RR to remove:

- Use `zone name removeRR` to remove any RR. You must specify the owner. If you omit the data, Cisco Prime Network Registrar removes all records of the specified type for the specified owner. Similarly, if you omit the type, Cisco Prime Network Registrar removes all records for the specified owner.
- Use `zone name removeDNSRR` to remove unprotected RRs only.
Managing Resource Records for Host

You can manage the RRs for a host by configuring the host record rather than the individual RRs. When you define a host, the DNS server automatically creates an Address (A) RR for IPv4, or an AAAA RR for IPv6, for it. If the reverse zone for the host exists, the server can also create the associated Pointer (PTR) RR for it. See Managing Hosts, on page 111 for details.

Protecting Resource Record Sets

When an RR is protected, DNS Updates cannot modify the record. Most administratively created RRs are protected. However, RRs created by DNS Updates must be unprotected to allow the server to modify them. You can set this protection status for each RR set on the List/Add DNS Server RRs for Zone page.

Note that only the primary DNS server can recognize this protection status; secondary servers do not recognize the protection status of their RRs.

⚠️ Caution

Zone scavenging can remove RRs that are unprotected. See the "Scavenging Dynamic Records" section in Cisco Prime Network Registrar 8.3 DHCP User Guide for details.

Local Basic or Advanced and Regional Web UI

To protect an existing RR, do the following:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose Forward Zones from Design &gt; Auth DNS to open the List/Add Forward Zones page.</td>
</tr>
<tr>
<td>Step 2</td>
<td>In the Forward Zone pane, click the zone name to open the List/Add Forward Zones page.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click the Resource Records tab.</td>
</tr>
<tr>
<td>Step 4</td>
<td>On the Resource Records tab, click the Resource Record name in the list of Resource Records to edit the resource record.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Click Protect Set button to unprotected the selected RR set.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Click Save to save the resource record attribute modification.</td>
</tr>
</tbody>
</table>

Unprotecting Resource Record Sets

You can also unprotect an RR. To unprotect an RR while adding, click the Locked icon next to the Resource Record name field. The icon changes to the Unlocked icon.

Local Basic or Advanced and Regional Web UI

To unprotect an existing RR, do the following:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose Forward Zones from Design &gt; Auth DNS to open the List/Add Forward Zones page.</td>
</tr>
<tr>
<td>Step 2</td>
<td>In the Forward Zone pane, click the zone name to open the List/Add Forward Zones page.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click the Resource Records tab.</td>
</tr>
</tbody>
</table>
Step 4  On the Resource Records tab, click the Resource Record name in the list of Resource Records to edit the resource record.

Step 5  Click Unprotect Set button to unprotect the selected RR set.

Step 6  Click Save to save the resource record attribute modification.

Note  The icon to the left of the RR set name indicates the status of the Resource Record, whether it is protected or unprotected.

---

CLI Commands

To protect the RR sets, use `zone name protect-name rrset-name`; to unprotect the zone, use the `unprotect-name rrset-name` action instead. For example:

```
nrcmd> zone example.com protect-name boston
100 Ok
protected boston
nrcmd> zone example.com unprotect-name boston
100 Ok
unprotected boston
```

Searching Server-Wide for Records and Addresses

With Cisco Prime Network Registrar, you can search for RRs and IP addresses server-wide. The search is a filter mechanism whereby you can specify a combination of RR and address attributes to target one or more RRs or addresses configured for the network. The search function is available at the local cluster only.

You can search RRs by:

- IP address
- Protection state
- Name prefix
- Type
- Zone

Local Advanced Web UI

To search resource records by IP address, do the following:

Step 1  From the Operate menu, choose DNS > RR By IP Address from the Reports submenu to open the IP Address Search page.

Step 2  To search by IP address, enter an IP address, then click Search.

Note  In an IP address search, the DNS server does not search all forward zones for RRs that have the specified address in the data field. Instead, the server looks up the matching PTR record in the reverse zone and returns all the respective RRs in the forward zone.
Local Advanced Web UI

To search resource records, do the following:

**Step 1** From the Operate menu, choose DNS > Resource Records from Reports submenu to open the DNS Resource Record Search page.

**Step 2** Choose a filter attribute from the drop-down list.

**Step 3** Choose a filter type from the drop-down list depending on the filter attribute you chose:

- **RR Protection State**—RR Protection Status, either locked or unlocked.
- **RR Name Prefix**—RR Name Prefix.
- **RR Type**—RR Type.
- **Zone**—Zone List, Regular expression, or Zone Flags

**Step 4** Enter or select a Value, based on the Type selected. To clear the filter, click Clear Filter.

**Step 5** Click Add Element to add the search element to the filter elements list. The Filter Elements heading identifies the filter attribute and value used for the filter. If you add more than one element, the heading identifies the ANDed values of the elements. For example, if you add an element for a name prefix search for user, then add another element for an RR type search for A records, the filter element heading will identify the search as **RR Name Prefix = user AND RR Type = A**.

**Step 6** You can add as many elements as you like (remembering that the search results are an intersection of the filter elements). View the filter elements list by clicking the plus sign (+).

**Step 7** Click Search.

**Step 8** Check the table of resulting RRs from the search, which shows for each RR its zone, hostname, TTL, type, and associated data. If necessary, change the page size to see more entries at one time (you might still need to page forward and back). The RRs are sorted in DNSSEC order.

**Tip** If the search results are less than expected due to the ANDing of the filter elements, look at the filter list for any element that might be compromising the search, delete it by clicking the Delete icon next to it, then redo the search.

**CLI Commands**

Use `dns findRR` to find RRs across the zones. The command syntax is of two kinds:

```bash
nrcmd> dns findRR -name {fqdn | domainaddr}
nrcmd> dns findRR [-namePrefix nameprefix] [-rrTypes RRTypelist] [-protected] [-unprotected] [-zoneType {forward | reverse | primary | secondary | ALL}]
```

You can search by domain or its address, or enter the beginning characters of the RR name (the name prefix). If you search by RR name prefix, you can narrow the search by a list of RR types, protection status, or zone type. The output clearly indicates the zone for each found entry. For example:

```bash
nrcmd> dns findRR -namePrefix user -rrTypes A
```
Filtering Resource Records

You might want to filter records to display only one type of record, such as an A (or IPv6 AAAA) or PTR record. (See also Searching Server-Wide for Records and Addresses, on page 105.)

Local Basic or Advanced and Regional Web UI

You can filter RRs right from the Edit Zone page. Look for the Name and Type fields just below the Add Resource Record button.

By default, RRs are sorted alphabetically by name, starting with the top-of-zone records (marked with the @ symbol), and secondarily sorted by type, then data. You can also sort them by:

- **Protected state**—You can click All, Unprotected, or Protected.
- **Name prefix**—Starting characters in the name. Note that the * character is not a wildcard. For example, entering al returns alberta, allen.wrench, and allie, whereas entering al* returns al* and al*ert.
- **RR type**—Click one of the RR types in the drop-down list, such as A (or IPv6 AAAA) or TXT.

When the selection is complete, click Filter List. This returns just the filtered entries in the table below the fields. To return to the full, unfiltered list, click Clear Filter.

CLI Commands

Use zone zonename findRR to search on RR name prefixes, RR types, or protection status:

```
nrcmd> zone zonename findRR [-namePrefix nameprefix] [-rrTypes RRtypelist] [-protected -unprotected]
```

Advertising Services to Network Using Service Location (SRV) Records

The service location (SRV) RR is used to advertise services to the network. This RR is defined in the RFC 2782, “A DNS RR for specifying the location of services (DNS SRV).” The SRV can have an associated A or AAAA record. Windows domain controller is one service that uses the SRV records.

The RFC defines the format of the SRV record (DNS type code 33) as:

```
_service._protocol.name ttl class SRV priority weight port target
```

There should always be an A record associated with the SRV record target so that the client can resolve the service back to a host. In the Microsoft Windows implementation of SRV records, the records might look like this:

```
myserver.example.com A 201.165.201.1
_ldap._tcp.example.com SRV 0 0 389 myserver.example.com
_kdc._tcp.example.com SRV 0 0 88 myserver.example.com
_ldap._tcp.dc._msdcs.example.com SRV 0 0 88 myserver.example.com
```
An underscore (_) always precedes the service and protocol names. In the example, _kdc is the Key Distribution Center. The priority and weight help a client choose between target servers providing the same service (the weight differentiating those with equal priorities). If the priority and weight are all set to zero, the client orders the servers randomly.

Note

For a description of how Windows clients interoperate with DNS and DHCP servers, including scavenging dynamic RRs, see the "Configuring DNS Update for Windows Clients" section in Cisco Prime Network Registrar 8.3 DHCP User Guide.

Name Resolution in a Namespace Using NAPTR Resource Records

Cisco Prime Network Registrar supports Naming Authority Pointer (NAPTR) RRs. These records help with name resolution in a particular namespace and are processed to get to a resolution service. Because NAPTR records are a proposed standard, RFC 3403, Cisco Prime Network Registrar only validates their numeric record fields. However, the proposed standard requires a value for each field, even if it is null (""), and there are no preset values.

When using a NAPTR record to locate a Session Initiation Protocol (SIP) proxy, see the proposed standard, RFC 2916 or RFC 3263. In RFC 2916, the ENUM working group of the Internet Engineering Task Force specifies NAPTR records to map E.164 addresses to Universal Resource Identifiers (URIs). Using the NAPTR record resolves a name in the E.164 international public telecommunication namespace to a URI, instead of providing the name of a service to use as a resolver. The U flag was added to the NAPTR record for this purpose.

For example, to specify a SIP proxy for the phone number +4689761234, add a NAPTR record at the name 4.3.2.1.6.7.9.8.6.4.e164.arpa. with this content:

```
100 10 "u" "sip+E2U" "/^.*$/sip:info@example.com/" .
```

This sets these fields of the NAPTR record:

```
order = 100
preference = 10
flags = "u"
service = "sip+E2U"
regexp = "/^.*$/sip:info@example.com/"
replacement = .
```

After you configure these fields, the DNS client dealing with phone number +4689761234 can now find an SIP service URI by replacing the number with sip:info@tele2.se. The E.164 zone mostly uses the NAPTR record for wholesale replacement of the input telephone number. Section 3.2.3 of RFC 2916 includes an example of one transformation to a Lightweight Directory Access Protocol (LDAP) query that preserves some of the digits. The E.164 zone does not map to service location (SRV) records because it wants to obtain a SIP URL that is more humanly readable to the left of the at (@) symbol.
Local Basic or Advanced and Regional Web UI

**Step 1** On the Edit Zone page, click the Resource Records tab.

**Step 2** Enter the owner of the record in the Name field.

**Step 3** Enter the TTL (if necessary).

**Step 4** Click NAPTR in the Type drop-down list.

**Step 5** Enter the data as a string embedded in quotes and separated by spaces:
- a) Order
- b) Preference
- c) Flags
- d) Service
- e) Regular expression
- f) Replacement string

For example:

**Example:**

```
"100 10 u sip+E2U /\.*$/sip:info@tele2.se/."
```

**Step 6** Click Add Resource Record.

---

**CLI Commands**

Use `zone name addRR` to add a protected resource record to a zone.
Managing Hosts

This chapter explains how to configure hosts in DNS zones.

- Adding Hosts in Zones, on page 111
- Adding Additional RR for the Host, on page 112
- Editing Hosts, on page 112
- Removing Hosts, on page 113

Adding Hosts in Zones

You can manage the resource records (RRs) for a host by configuring the host rather than the individual RRs. When you define a host, the DNS server automatically creates an Address (A) RR in IPv4, or an AAAA RR in IPv6, for each address you specify. If you specify one or more aliases for the host, the server also creates a Canonical Name (CNAME) RR for each alias. You can also have the server create a Pointer (PTR) RR for the host in the reverse zone for the host, if the reverse zone exists.

Local Basic or Advanced Web UI

**Step 1**
From the **Design** menu, choose **Hosts** under the **Auth DNS** submenu.
This opens the List/Add Hosts for Zone page.

**Tip**
You can sort by hostname, IP address, IPv6 address (if appropriate), or alias by clicking the corresponding column heading on the List/Add Host for Zone page. However, for zones with a large number of hosts (more than 50,000), restrict the sort to the hostname. Sorting based on IP address or alias can take significantly longer, and could fail if you exceed the memory capacity of the CCM server.

**Step 2**
Enter the name of the host and its IPv4 or IPv6 address or comma-separated addresses.

**Step 3**
If the host has alias names, enter a comma-separated list.

**Step 4**
If you want to create a corresponding Pointer (PTR) RR for the host and you know that the reverse zone for the host exists, check the Create PTR Records? check box.

**Step 5**
Click **Add Host**.

**Step 6**
To confirm, from the **Design** menu, choose **Forward Zones under the Auth DNS submenu**. This opens the List/Add Forward Zones page.

**Step 7**
Click the **Resource Records** tab to view RR’s for the selected zone.
If you want to view the list of hosts for a particular zone, click the **Hosts** tab.

---

**CLI Commands**

To create A RR, alias RR, and PTR RR for existing reverse zones in a single operation, use `zone name addHost hostname address alias` for each host. To list the created zones, use `zone name listHosts`.

---

**Adding Additional RRs for the Host**

You add additional RRs for the host based on the dns edit mode you chose, either staged or synchronous. For details, see *Adding Resource Record to Zone*, on page 102.

Reload the DNS server if you want these RRs to become active server RRs.

---

**Local Basic or Advanced Web UI**

For example, to add additional CNAME RRs, add the alias hostname in the Name field under the Resource Records tab of the List/Add Forward Zones page, choose **CNAME** from the Type drop-down list, add the canonical name of the host in the Data field, then click **Add Resource Record**. Note that the DNS specification does not allow a CNAME RR with the same name as that of another RR.

For an MX RR, add the origin hostname in the Name field; choose **MX** from the Type drop-down list; add the integer preference value, a space, and the domain name of the mail exchanger for the origin host in the Data field; then click **Add Resource Record**. These entries should appear in the list at the bottom of the page.

---

**CLI Commands**

To create a CNAME record, use `zone name addRR alias CNAME canonical` for protected RRs or `zone name addDNSRR alias CNAME canonical` for unprotected RRs. To create an MX record, use `zone name addRR hostname MX preference mxname` for protected RRs or `zone name addDNSRR hostname MX preference mxname` for unprotected RRs.

---

**Editing Hosts**

Editing a host involves:

- Adding additional addresses or aliases
- Modifying its Resource Records (RR’s).

---

**Local Basic or Advanced Web UI**

**Step 1**

From the **Design** menu, choose **Hosts** under the **Auth DNS** submenu. This opens the List/Add Hosts for Zone page. If you have multiple zones configured, select the zone from the list of zones in the Hosts pane on the left.

**Step 2**

Click the hostname to add additional IP addresses or aliases, and click **Save**.
Step 3  
To modify the RRs, click the **Edit RRs** button to open the Edit View RR List page.

---

**CLI Commands**

To edit the host, you must remove and reenter its RRs by using `zone name removeRR name type data` or `zone name removeDNSRR name type data`, then `zone name addRR name ttl class type data` or `zone name addDNSRR name ttl type data`.

**Removing Hosts**

Removing a host removes all A, CNAME, and PTR RRs for that host.

**Local Basic or Advanced Web UI**

On the List/Add Hosts in Zone page (see Editing Hosts, on page 112 for the possible ways to get there), click the **Delete** icon next to the host you want to remove, then confirm the deletion.

**CLI Commands**

Remove the host by using `zone name removeHost`, then re-add it by using `zone name addHost`. 
CHAPTER 12

Authoritative DNS Metrics

These authoritative DNS metric elements are available in the dashboard:

- DNS Outbound Zone Transfers, on page 115
- DNS Inbound Zone Transfers, on page 116
- DNS Network Errors, on page 116
- DNS Related Servers Errors, on page 117
- DNS General Indicators, on page 117
- DNS Queries Per Second, on page 118

DNS Outbound Zone Transfers

The DNS Outbound Zone Transfers dashboard element rendered as a stacked area chart tracks the rate of change in full and incremental outbound zone transfer responses, and any associated errors. The chart is available if you choose DNS Metrics: DNS Outbound Zone Transfers in the Chart Selection list.

The resulting stacked area chart plots the following trends:

- Full Responses—Number of full outbound zone transfers (AXFRs out).
- Incremental Responses—Number of incremental outbound zone transfers (IXFRs out).
- Authorization Errors—Number of unauthorized (refused) zone transfer requests.
- Exceed Max Transfers Out—Number of failed outbound transfers that exceed the maximum limit.
- Other Errors—Number of other outbound transfer errors that are not authorization errors.

How to Interpret the Data

This chart is useful in gauging if outbound zone transfers to a secondary DNS server are occurring as predicted and if there are any authorizations or failed transfer attempts in the process. The most significant indicator is the trend in the number of outbound zone transfers denied for lack of permission or for not being authorized for the zone.

Troubleshooting Based on the Results

Check the primary and secondary server configurations if there are errors or exceeded limits in the outbound zone transfers.
DNS Inbound Zone Transfers

The DNS Inbound Zone Transfers dashboard element rendered as a stacked area chart tracks the rate of change in full and incremental inbound zone transfer responses, and any associated errors. The chart is available if you choose **DNS Metrics: DNS Inbound Zone Transfers** in the Chart Selection list.

The resulting stacked area chart plots the following trends:

- **Full Response**—Number of full inbound zone transfers (AXFRs in).
- **Incremental Responses**—Number of incremental inbound zone transfers (IXFRs in).
- **Authorization Errors**—Number of refused responses (xfer-in-auth-errors).
- **Failed Attempts**—Number of failures other than refusals (xfer-failed-attempts).
- **Exceed Max Transfers In**—Number of times that the concurrent inbound transfers reach the maximum limit.

**How to Interpret the Data**

This chart is useful in gauging if inbound zone transfers to a secondary DNS server are occurring as predicted and if there are any authentication or failed transfer attempts in the process. The most significant indicator is the trend in the number of inbound zonended transfers denied for lack of permission, for not being authorized for the zone, or for other reasons.

**Troubleshooting Based on the Results**

Check the primary and secondary server configurations if there are errors or exceeded limits in the inbound zone transfers.

DNS Network Errors

The DNS Network Errors dashboard element rendered as a line chart tracks the rate of change in DNS server network errors. The chart is available if you choose **DNS Metrics: DNS Network Errors** in the Chart Selection list.

The resulting line chart plots the following trends:

- **Query Error Packets/Query Responses**—Ratio of query error packets over responses. Responses consist of:
  - Authoritative
  - Authoritative no-such-name
  - Authoritative no-such-data
  - Nonauthoritative
  - Nonauthoritative no-such-data
  - Requests refused

- **Non Error Dropped Packets/Query Responses**—Ratio of nonerror dropped packets (queries dropped) over responses.

- **Update Errors/Updates**—Ratio of DNS Update errors over total updates.
How to Interpret the Data

This chart indicates query and response errors as an indication of the health of the server.

Troubleshooting Based on the Results

Check the DNS server network configuration if errors are increasing.

DNS Related Servers Errors

The DNS Related Servers Errors dashboard element rendered as a line chart tracks the rate of change in DNS related server errors. The chart is available if you choose DNS Metrics: DNS Related Servers Errors in the Chart Selection list.

The resulting line chart plots the following trends:

- **Referral Timeouts/Referrals**—Ratio of referral timeouts over referrals.
- **Failed Responses/Total Incoming Zone Transfer Requests**—Ratio of failed responses over incoming zone transfer requests.
- **TSIG Errors/TSIG Attempts**—Ratio of transaction signature (TSIG) errors (bad times, keys, or signatures) over total TSIG attempts (successfully received packets).

How to Interpret the Data

This chart indicates the health of connections and data transfers with related DNS servers. All three chart lines can have diagnostic significance.

Troubleshooting Based on the Results

Check the configurations and connectivity of the related servers in HA DNS relationships if errors are increasing.

DNS General Indicators

The DNS General Indicators dashboard element rendered as a table shows the server state, its last and startup reload time, the number of zones per server, and the total resource record (RR) count. The table is available if you choose DNS Metrics: DNS General Indicators in the Chart Selection list.

The resulting table shows:

- **Server State**—Up or Down (based on whether statistics are available), and how long the server has been in this state.
- **Last Reload**—How long since the last server reload.
- **Start Time**—Date and time of the last server process (Cisco Prime Network Registrar server agent) startup.
- **Total Zones**—Number of configured zones.
- **Total RRs**—Number of resource records.
How to Interpret the Data

The data in this chart shows general server health and operational duration. The objective is to make decisions about the server, such as whether it might be time for another reload, perhaps warranted by the number of configured zones.

Troubleshooting Based on the Results

If the server state is Down, all the DNS chart indicators show a red status box, so no data will be available. In the case of a server that is down, restart the server. The number of zones indicated might also require some evaluation and possible reconfiguration.

DNS Queries Per Second

The DNS Queries Per Second dashboard element, rendered as chart, displays queries per second for the Authoritative DNS server. This chart is available if you choose **DNS Metrics: DNS Queries Per Second** in the Chart Selection page 1.
Resource Records

Resource records comprise the data within a DNS zone. There is no fixed limit to the number of resource records a zone can own. In general, there can be zero, one, or more resource records of a given type. However, there are constraints on the number of certain types of records a zone can have.

All resource records have these required entries:

- **Name**—Name (host) that owns the record, such as example.com.
- **Class (not required for all formats)**—DNS supports only the IN (Internet) class of record.
- **TTL (time to live)**—Amount of time to store the record in cache, in seconds. If you do not include a TTL, Cisco Prime Network Registrar uses the zone default TTL, defined in the SOA resource record.
- **Type**—Type of the record, such as A, NS, SOA, and MX. There are many types that various RFCs define, although ten or fewer are in common use.
- **Record data**—Data types whose format and meaning varies with record type.

The following table lists all the resource record types Cisco Prime Network Registrar supports. It provides the field syntax and the field descriptions, as well as how the fields are represented in the Cisco Prime Network Registrar GUI.

**Table 8: Resource Records**

<table>
<thead>
<tr>
<th>Record</th>
<th>No.</th>
<th>Name</th>
<th>Syntax and Description</th>
<th>RFC</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>1</td>
<td>Host Address—Name-to-address mapping for the zone</td>
<td>name ttl class A address Web UI: Add or Edit Host for Zone page: Hostname, IP Address or Resource Records for Zone page: Name, TTL, Type, Data</td>
<td>1035</td>
</tr>
<tr>
<td>Record</td>
<td>No.</td>
<td>Name</td>
<td>Syntax and Description</td>
<td>RFC</td>
</tr>
<tr>
<td>--------</td>
<td>-----</td>
<td>-------------------------------</td>
<td>-------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>A6</td>
<td>38</td>
<td>IPv6 Address—name ttl class</td>
<td>In the data, the suffix address is an IPv6 address encoded</td>
<td>6563</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(Obsolete; use AAAA records</td>
<td>in network order (high-order octet first). There must be</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>instead)</td>
<td>exactly enough octets in this field to contain a number of</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>bits equal to 128 minus prefix length, with 0 to 7 leading</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>pad bits to make this field an integral number of octets.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Pad bits, if present, must be set to zero when loading a</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>zone file and ignored on reception. For example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2001:0:734c:c0::</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Web UI: Resource Records for</td>
<td>Data in the form:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Zone page: Name, TTL, Type=A6,</td>
<td>ncmd&gt; zone example.com addRR host456 A6 0</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Data=prefixlength suffixaddr</td>
<td>1345:c1:ca11:1:1234:5678:9abc:def0</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>prefixname , with data in the</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AAAA</td>
<td>28</td>
<td>IPv6 Address—name ttl class</td>
<td>Data is the IPv6 address format of eight sets of four</td>
<td>3596</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AAAA address</td>
<td>hexadecimal digits, separated by colons. The first set of</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>four digits is the high-order 16 bits of the address. You</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>can omit leading zeros in sets and omit a value in a set if</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>the value of the set is zero.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Web UI: Resource Records for</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Zone page: Name, TTL, Type=AAAA,</td>
<td>ncmd&gt; zone example.com addRR host456 AAAA 0</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Data=address</td>
<td>1345:c1:ca11:1:1234:5678:9abc:def0</td>
<td></td>
</tr>
<tr>
<td>AFSDB</td>
<td>18</td>
<td>Andrew File System (AFS)</td>
<td>name ttl class AFSDB subtype hostname</td>
<td>1183</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Data Base—</td>
<td>Subtype is either 1—AFS cell database server, or 2—DCE</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>authentication name server. Hostname is the domain name of</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>host that has a server for the cell named by the owner.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Web UI: Resource Records for</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Zone page: Name, TTL, Type=AFSDB,</td>
<td>ncmd&gt; zone example.com addRR host456 AFSDB 0</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Data=subtype hostname</td>
<td>1345:c1:ca11:1:1234:5678:9abc:def0</td>
<td></td>
</tr>
<tr>
<td>CNAME</td>
<td>5</td>
<td>Canonical Name—Aliases or</td>
<td>alias ttl class CNAME canonicalname</td>
<td>1035</td>
</tr>
<tr>
<td></td>
<td></td>
<td>nicknames</td>
<td>You cannot have any other resource records associated with</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>a CNAME. Aliases are useful when you want the outside</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>world to know a single, easily remembered name. You can</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>also use aliases when a host changes its name. In that case,</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ensure that you have a CNAME pointer so that when people</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>use the original name, it can be resolved to the newer one.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Web UI: Resource Records for</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Zone page: Name=alias , TTL,</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Type=CNAME, Type, Data=canonicalname</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Record</td>
<td>No.</td>
<td>Name</td>
<td>Syntax and Description</td>
<td>RFC</td>
</tr>
<tr>
<td>--------</td>
<td>-----</td>
<td>------</td>
<td>------------------------</td>
<td>-----</td>
</tr>
<tr>
<td>DHCID</td>
<td>49</td>
<td>Dynamic Host Configuration Identifier— (RFC 4701)</td>
<td>name ttl class DHCID data The DNS server uses this RR to allow DHCP clients and servers to update DNS automatically. This RR is not user-configurable. The data is the result of a one-way hash computation of the client message and the domain name. Sample RR output for an IPv6 address:</td>
<td>4701</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>chi6.example.com IN DHCID (AAIBY2/AuCcgoJbaxcQc9TUappF6910jxfNuVAA2kJEA= )</td>
<td></td>
</tr>
<tr>
<td>HINFO</td>
<td>13</td>
<td>Host Info— Hardware and software information for the host</td>
<td>name ttl class HINFO cpu os Data is the hardware (CPU) and operating system.</td>
<td>1035</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Web UI: Resource Records for Zone page: Name, TTL, Type=HINFO, Data=cpu os</td>
<td></td>
</tr>
<tr>
<td>ISDN</td>
<td>20</td>
<td>Integrated Services Digital Network (ISDN) Address—</td>
<td>name ttl class ISDN ISDNnumber [subaddr ] Data is the ISDN number of the owner and Direct Dial In, if any, and an optional ISDN subaddress string</td>
<td>1183</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Web UI: Resource Records for Zone page: Name, TTL, Type=ISDN, Data=ISDNnumber [subaddr ]</td>
<td></td>
</tr>
<tr>
<td>MB</td>
<td>7</td>
<td>Mailbox Domain Name—</td>
<td>name ttl class MB mbox Data is the domain name of the host with the specified mailbox.</td>
<td>1035</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Web UI: Resource Records for Zone page: Name, TTL, Type=MB, Data=mbox</td>
<td></td>
</tr>
<tr>
<td>MG</td>
<td>8</td>
<td>Mail Group Member—</td>
<td>name ttl class MG mgroup Data is the domain name of the mailbox group (mailing list).</td>
<td>1035</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Web UI: Resource Records for Zone page: Name, TTL, Type=MG, Data=mgroup</td>
<td></td>
</tr>
<tr>
<td>MINFO</td>
<td>14</td>
<td>Mailbox Info—</td>
<td>name ttl class MINFO respmbx errormbox Data is the mailbox responsible for the mailing list, and the mailbox to receive error messages.</td>
<td>1035</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Web UI: Resource Records for Zone page: Name, TTL, Type=MINFO, Data=respmbx errormbox</td>
<td></td>
</tr>
<tr>
<td>MR</td>
<td>9</td>
<td>Mail Rename—</td>
<td>name ttl class MR newmbox Data is the mailbox name to rename the owner mailbox.</td>
<td>1035</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Web UI: Resource Records for Zone page: Name, TTL, Type=MR, Data=newmbox</td>
<td></td>
</tr>
<tr>
<td>Record</td>
<td>No.</td>
<td>Name</td>
<td>Syntax and Description</td>
<td>RFC</td>
</tr>
<tr>
<td>--------</td>
<td>-----</td>
<td>------</td>
<td>------------------------</td>
<td>-----</td>
</tr>
<tr>
<td>MX</td>
<td>15</td>
<td>Mail Exchanger—Where to deliver the mail for a domain name</td>
<td><code>name ttl class MX pref mxname</code> Data is the preference value (16-bit integer for the preference for the record, with lower values having preference), and the domain name of the mail exchanger for the owner.</td>
<td>1035</td>
</tr>
</tbody>
</table>
| NAPTR | 35  | Naming Authority Pointer—Produces a new domain label or Universal Resource Identifier (URI). You can then use DNS to look up services for many resource names that are not in domain name syntax. | `name ttl class NAPTR order pref flags serv regexp replace`  
- `order` — 16-bit integer for the order in which to process the NAPTR records to ensure the correct ordering of rules, with low numbers processed before high numbers.  
- `pref` — 16-bit unsigned integer for the order in which to process NAPTR records with equal `order` values, with low numbers processed before high numbers.  
- `flags` — Character-string containing flags to control aspects of rewriting and interpreting fields, single characters from the set [A-Z0-9] (not case-sensitive); the S, A and U flags denote a terminal lookup, the P flag says that the remainder of the application-side algorithm should be carried out protocol-specific.  
- `serv` — Valid protocols or services.  
- `regexp` — String containing a substitution expression applied to the original string held by the client to construct the next domain name to look up. (For common regex usage, see the Common Regex Values table in *Cisco Prime Network Registrar 8.3 Administrator Guide*).  
- `replace` — Next FQDN to query for NAPTR, SRV, or address records, depending on the value of the `flags` field. | 2915 |
<p>| NS     | 2   | Name Server—Authoritative server for the zone | <code>name ttl class NS nameserver</code> Machines that provide name service must not reside in the owner domain. For each domain, you must have at least one NS record. NS records for a domain must exist in both the zone that delegates the domain and in the domain itself. NS record names must have an equivalent A record (they cannot point to an alias). | 1035 |</p>
<table>
<thead>
<tr>
<th>Record</th>
<th>No.</th>
<th>Name</th>
<th>Syntax and Description</th>
<th>RFC</th>
</tr>
</thead>
</table>
| NSAP   | 22  | Network Service Access Point (NSAP) Address— | *name ttl class NSAP NSAPaddr*  
Data is the *NSAPaddr* —Octet values assigned by the assigning authority, a character string of the type used in TXT and HINFO records (see RFC 1706).  
**Web UI:** Resource Records for Zone page: Name, TTL, Type=NSAP, Data=NSAPaddr | 1706 |
| PTR    | 12  | Pointer—Reverse mapping       | *name ttl class PTR dname*  
Data is the domain name of host having the reverse record indicated by the owner. PTR records are used for reverse mapping, specifically in the in-addr.arpa zones for translation of addresses to names. PTRs use official names, not aliases. The name in a PTR record is the local IP address portion of the reverse name.  
**Web UI:** Resource Records for Zone page: Name, State, TTL, Type=PTR, Data=dname | 1035 |
| RP     | 17  | Responsible Person—          | *name ttl class RP mbox txhost*  
Data is the domain name of the mailbox for the responsible person, and the domain name of host where TXT records exist.  
**Web UI:** Resource Records for Zone page: Name, TTL, Type=RP, Data=mbox txhost | 1183 |
| RT     | 21  | Route Through—               | *name ttl class RT pref intermediatehost*  
Data is the *pref* —16-bit integer for preference to give to this record among others of the same owner, and *intermediatehost* —domain name of the host serving as intermediate to reach the owner.  
**Web UI:** Resource Records for Zone page: Name, TTL, Type=RT, Data=pref intermediatehost | 1183 |
| SOA    | 6   | Start of Authority—Every zone must have a single SOA record | *name ttl class SOA primeserver hostmaster (serial refresh retry expire minimum)*  
**Web UI:** Add or Edit Zone page SOA Attributes: Serial Number, SOA TTL, Nameserver, Contact E-Mail, Secondary Refresh, Secondary Retry, Secondary Expire, Minimum TTL | 1035 |
<table>
<thead>
<tr>
<th>Record</th>
<th>No.</th>
<th>Name</th>
<th>Syntax and Description</th>
<th>RFC</th>
</tr>
</thead>
<tbody>
<tr>
<td>SRV</td>
<td>33</td>
<td>Service Location—</td>
<td>name ttl class SRV priority weight port target  &lt;br&gt;  • priority — 16-bit priority to give the record among the owner SRV records.  &lt;br&gt;  • weight — 16-bit load to give the record at the same priority level.  &lt;br&gt;  • port — 16-bit port on which to run the service.  &lt;br&gt;  • target — Domain name of host running on the specified port.  &lt;br&gt; Administrators can use several servers for a single domain, move services between hosts with little difficulty, and designate some hosts as primary servers for a service and others as backups. Clients ask for a specific service or protocol for a domain and receive the names of any available servers. See the &quot;Managing DNS Update&quot; chapter in Cisco Prime Network Registrar 8.3 DHCP User Guide for how this record affects Windows servers.  &lt;br&gt; <strong>Web UI</strong>: Resource Records for Zone page: Name, TTL, Type=SRV, Data=priority weight port target</td>
<td>2782</td>
</tr>
<tr>
<td>TXT</td>
<td>16</td>
<td>Text—</td>
<td>name ttl class TXT textstring  &lt;br&gt; Data is one or more text character strings that can contain any type of information.  &lt;br&gt; <strong>Web UI</strong>: Resource Records for Zone page: Name, TTL, Type=TXT, Data=textstring</td>
<td>1035</td>
</tr>
<tr>
<td>WKS</td>
<td>11</td>
<td>Well Known Services—</td>
<td>name ttl class WKS addr protocol servicelist  &lt;br&gt;  • addr — 32-bit IP address.  &lt;br&gt;  • protocol — 8-bit IP protocol number, which can be TCP or UDP.  &lt;br&gt;  • servicelist — Variable-length bit map in 8-bit multiples of services, which can be TIME, TELNET, FTP, or SMTP.  &lt;br&gt; <strong>Web UI</strong>: Resource Records for Zone page: Name, TTL, Type=WKS, Data=addr protocol servicelist</td>
<td>1035</td>
</tr>
<tr>
<td>X25</td>
<td>19</td>
<td>X.25 Address—</td>
<td>name ttl class X25 PSDNaddr  &lt;br&gt; Data is the character string of the Public Switch Data Network (PSDN) address in the X.121 numbering plan associated with the owner.  &lt;br&gt; <strong>Web UI</strong>: Resource Records for Zone page: Name, TTL, Type=X25, Data=PSDNaddr</td>
<td>1183</td>
</tr>
</tbody>
</table>