Running the Setup Web UI

The Cisco Prime IP Express setup interview in the web UI takes you through a series of consecutive pages to set up a basic configuration. For an introduction and details on the basic navigation for the pages, see Introducing the Setup Web UI.

This chapter contains the following sections:

Setting Up Services for Regional

The Set up this Server page opens when you click the **Setup** icon on the main menu in the regional Basic user mode. On this page, decide if you want to enable or disable:

- **Dynamic Host Configuration Protocol (DHCP)—**DHCP provides the mechanism for dynamic address assignment that is an essential part of Cisco Prime IP Express. DHCP configuration will takes through a series of pages for DHCP setup or based on the user selection DHCP setup is bypassed. See the Setting Up DHCP Services, on page 2.
- **Bring Your Own Device (BYOD)—**BYOD provides the mechanism for authorizing and registering the devices to get access to IP network resources. Configuring BYOD takes through a series of pages for BYOD setup or based on user selection the BYOD setup bypassed. See the Setting Up BYOD Service, on page 4.
- **Security—** Security provides option to select the authentication type and configure the external authentication servers. See the Security, on page 5.

Note Selections made in Setup this Server page are not persisted.

Click **Next** to go to the next page depending on your selections, or click **Finish** to end the setup and go to the Setup Interview Report page.

Setting Up DHCP Services

The DHCP server can be configured to serve only IPv4 address or IPv6 address or both. On this page you can choose either one or all the options such as Failover, DHCPv4, and DHCPv6 to configure the DHCP service(s).

DHCP Failover

Failover is a protocol designed to allow a backup DHCP server to take over for a main server if the main server becomes unavailable for any reason. On this page, you can configure the DHCP cluster name for main and backup servers which are going to be in failover relationship. You can also view, modify, and delete the failover pairs.

You need to perform " Synchronize Failover Pair " for newly added Failover Pair. You can choose the Direction of Synchronization. For initial failover configurations, use the Exact or Complete operation.

- Click **Report** to view the change set details.
- Click **Run** <mode> to apply the changes.

DHCPv4

DHCP configuration process takes through a series of configuration pages required for issuing IPv4 address. Below pages are related to configuration pages required for issuing IPv4 address.

DHCP - Scope Templates Page

You need to create a scope template to use it in subsequent pages for creating scopes in local cluster from regional. A scope consists of one or more ranges of dynamic addresses in a subnet that a DHCP server manages. You must define one or more scopes before the DHCP server can provide leases to clients.

You can specify expressions in a scope template to dynamically create scope names, IP address ranges, and embedded options when creating a scope. Usage of scope templates will ease the job of configuring multiple scopes.

Steps to create a scope Template:

Step 1 Click **Add Scope Templates** icon in the Scope Templates pane.

Step 2 Enter the scope template name in the Name box, and then click **Add DHCP Scope Template** button.

Step 3 Click **Save** to save the scope template, and the click Next to move to the next page.

Step 4 Enter "(concat "byod-" subnet)" in the **Scope Name Expression** text box.

Step 5 Enter "(create-range first-addr last-addr)" in the **Range Expression** text box and the click Save to save the page. Click **Next.**

Step 6 Click **Add Subnet** to create subnet.

Step 7 Enter subnet IP in the **Address** text box, for example 10.76.206.0, and then click **Add Subnet** button.

Step 8 Click the **Push** icon to push the subnet to the local cluster.

Step 9 Select the local cluster host name to which you want to push the subnet, from the **Cluster or Failover** drop-down list.

Step 10 Select the scope template from the **Scope Template** drop-down list.

Step 11 Click **Push Subnet** button and click next for **BYOD Setup** page.

DHCP - Subnets Page

On this Page, you can create, modify and delete subnets and push to local cluster or failover pair. Click on the push icon to select the local cluster host name or failover pair name to which you want to push the subnet.

Step 1 Enter subnet IP in the Address text box, for example 10.76.206.0, and then click **Add Subnet** button.

Step 2 Click the **Push** icon to push the subnet to the local cluster.

Step 3 Select the local cluster host name to which you want to push the subnet, from the **Cluster or Failover** drop-down list.

Step 4 Select the scope template from the **Scope Template** drop-down list.

Step 5 Click **Push Subnet** button for **BYOD Setup** page.

DHCPv6

DHCPv6 configuration process takes through a series of configuration pages required for issuing IPv6 address. Below pages are related to configuration required for providing IPv6 leases by DHCP Server.

DHCPv6 Prefix Templates

You can either configure DHCPv6 prefixes directly, or create prefix templates for creating prefixes.

During Prefix creation, you can specify expressions in a prefix template to dynamically create prefix names, IP address ranges, and embedded options.

DHCPv6 Prefixes

You can create, modify, delete DHCPv6 Prefixes and push selected DHCPv6 prefix to local cluster or failover pair. While pushing the prefix, prefix template is not mandatory.

Setting Up BYOD Service

You need to specify CDNS Server IP and the lifetime of lease to be provided for unregistered devices and click save. Based on this input, policy configuration for unregistered device (BYOD_Unregistered) is created automatically in the regional server . In addition, client classes (BYOD_Unregistered and BYOD_Registered) required for BYOD setup will be created automatically in the regional server . In the subsequent pages, you are allowed to edit the auto created policy and client classes, but don't delete the auto created policy and client classes unless if you want to do BYOD setup manually.

Choose the configuration values you want, based on information in the following subsections, then click **Next** to activate your settings.

CDNS Server

Choose a relevant CDNS server top act as spoof DNS to redirect to a BYOD web server. Set a lease time for the BYOD unregistered device to be connected.

Policies and Client Classes

After configuring the CDNS server and lease time the Policies (BYOD_Unregistered) and Client Classes (BYOD_Registered and BYOD_Unregistered) will be created automatically.

BYOD - Scope / Prefix creation for unregistered device

This page will help you in creating pool of IPv4 and IPv6 address for unregistered device.

DHCPv4 tab

User will have two options - split a scope or assign a tag to existing scope. This page will list scopes those are not yet BYOD enabled for each cluster / failover pair. Split Scope icon will split the existing scope<scope name> into two scopes, one for registered devices and another for unregistered devices. If split is successful, user can see that two scopes with same subnet having different range of IP address have been created in the corresponding local cluster or failover pair. The newer scope name will be BYOD_Unregistered_<scope name> and have a selection tag BYOD_Unregistered. Only the range will be modified in the existing scope.

The unregistered scope range of IP address is determined based on the percentage provided by the user. For example, 10.0.0.0/24 subnet will have maximum of 254 hosts and 10% of 254 will be 25 hosts. But we carve up number of hosts as powers of 2 to find the subnet so it would be 16 hosts. The subnet 10.0.0.0/28 will be used in ACL to restrict the network access. As top/first 'n' addresses is used, leaving out the subnet ID and first IP address for router maximum of 14 BYOD devices can be used in this subnet.

Assigning a Tag icon will help in assigning a dedicated subnet for BYOD devices. The entire required DHCP/CDNS Server configuration is done automatically by setup Interview. The auto created policies and client classes in regional server for BYOD are automatically pushed to local cluster or failover pair on performing split or assign options for the first time. The "default" client is also created in local client databases. All the unregistered devices will be mapped to this "default" client configuration.

In CDNS, domain redirect functionality is used to redirect the http request from unregistered device to BYOD Webserver. Single CDNS server can be used as Spoof DNS as well as actual DNS server. Domain Redirect rule named 'BYODRule' and ACL named 'BYOD' in CDNS server are auto-created by setup Interview the first time split/assign operation is performed . "Match List" in ACL is updated with subnets on each split or assigns operation.

Note On deleting auto-created BYOD policy / client class, splitting or assigning the tag for the scope / prefix will not happen.

DHCPv6 tab

Similar to DHCPv4 User will have two options - split a prefix or assign a tag to existing prefix. This page will list prefixes that are not yet BYOD enabled for each cluster / failover pair. Split Prefix icon shall split existing prefix<prefix name> address range 50-50% into two prefix, one for registered devices and another for unregistered devices. If split is successful, user can see that two prefix with same prefix address having different range of IP address have been created in the corresponding local cluster or failover pair. The newer prefix name will be BYOD_Unregistered_<prefix name> and have a selection tag BYOD_Unregistered. Only the range will be modified in the existing prefix. Assign a Tag icon will help in assigning a dedicated prefix for BYOD devices.
To create an unregistered scope:

Step 1 In the Scope Creation page, select a cluster/failover pair in the left Clusters pane.

Step 2 Select a scope from the scope tree and enter a percentage value. In case of prefix, the split will be 50-50 percentage.

Step 3 Click the **Split Scope** icon to split the scopes for the BYOD unregistered scope or click the **Assign Tag** icon to allocate the complete scope for the BYOD unregistered scope.

BYOD Https Configuration

Key store file is not mandatory for BYOD; Device Registration page can be loaded in http if no key store file is uploaded. If the key store file is uploaded, then http request will be automatically redirected to https before loading Device Registration page.

Reload Servers

The changes made in CDNS and DHCP servers for BYOD will get impacted by choosing the corresponding servers and clicking the **Reload Servers** button in the Reload Servers page.

Security

Choose an authentication type from the drop-down list (Local/Radius/Active Directory).

If authentication type is local, local CCM database is used to authenticate the username/password credentials used while login using Cisco Prime IP Express WebUI/CLI/SDK.

Active Directory Server configuration is mandatory for BYOD. On Device Registration Page, the credentials provided are validated against Active Directory using GSSAPI mechanism (default).

If authentication type is Radius/Active Directory, follow the steps below:

Step 1 For Radius/Active Directory, click **Next** to configure the corresponding server.

Step 2 For Radius, click the **Add Radius** icon. Enter the name and address, and click the **Add External Authentication Server** button.

Step 3 For Active Directory, click the **Add Active Directory Server** icon. Enter the name, address, and domain, and click the **Add External Authentication Server** button.

Setup Interview Summary Report

The Setup Interview Summary Report page summarizes the actions you took on the setup pages and gives you the scopes/prefixes utilization report for BYOD.

Setting Up Services Local

The Set up this Server page opens when you click the Setup icon on the main menu in the local Basic user mode.

On this page, decide if you want to enable or disable:

- **Changing the administrator password—**For security purposes, you might want to change the administrator password from the value you set during the installation of Cisco Prime IP Express or during your first login to Cisco Prime IP Express web UI. See Changing the Administrator Password, on page 7 for details.

- **Dynamic Host Configuration Protocol (DHCP) server—**DHCP provides the mechanism for dynamic address assignment that is an essential part of Cisco Prime IP Express. Enabling DHCP goes to a series of pages for DHCP setup; disabling it bypasses the DHCP setup. See Setting Up DHCP Service, on page 7 for details.

- **Caching Domain Name System (CDNS) server—**CDNS provides your domain name structure. Enabling CDNS goes to a series of pages for CDNS setup; disabling it bypasses the CDNS setup. See Setting Up CDNS Service, on page 12 for details.

- **Authoritative Domain Name System (DNS) server—**DNS provides your domain name structure. Enabling DNS goes to a series of pages for DNS setup; disabling it bypasses the DNS setup. See Setting Up DNS Service, on page 13 for details.

- **DNS Update—**DNS Update combines the benefits of dynamic addressing using DHCP with permanent and unique hostnames in DNS. You can thereby configure DNS hosts automatically for network access. The DHCP server notifies the DNS server so that the DNS server can keep its resource records (RRs) up to date. Enabling DNS Update opens a series of pages for DNS Update setup; disabling it bypasses the DNS Update setup. See Setting Up DNS Update, on page 16 for details.

Note Selections you make are retained across login sessions.

Click **Next** to go to the next page depending on your selections, or click **Finish** to end the setup and go to the Setup Interview Report page.

Changing the Administrator Password

The Change Password for User page opens if you set the Change Password value to yes on the Set up this Server page in the setup interview.

After you change the password, the subsequent administrator-logins will use the new password.

If you do not want to change the password, check the **no** check box. To change the password, enter the new password, then enter it again in the Verify field to confirm it. Clicking **Next** or **Finish** submits your change, if any, for the next login session.

Setting Up DHCP Service

The Set up DHCP page opens in the proper sequence if you set the Enable DHCP Server value to **yes** on the Set up this Server page in the setup interview. It also opens if you click **DHCP** on the navigation bar.

To set up the DHCP server, be sure that the Enable DHCP Server value is set to **yes** on this page. If you already configured a main DHCP server in Cisco Prime IP Express and synchronized to it, then the setup process advises you that the current host is already a backup server, requiring no further DHCP configuration.

Choose the configuration values you want, based on the following subsections, then click **Next**. The setup process activates your settings, and the page that follows is for managing scopes (address pools).

Enable DHCP Failover

A DHCP Failover configuration provides a backup DHCP server that can take over if the main server is off the network for any reason. The servers act as redundant pairs and communicate with each other to prevent duplicate address assignments.

To provide failover service, set the Configure DHCP Failover value to **yes**. If the setup process detects an existing complex failover configuration, it notifies you that you are not allowed to configure failover from the setup interview. You are prevented from DHCP failover configuration if it was already configured in Advanced mode and one of the following conditions is true:

- More than one failover pair is configured.
- A single failover pair exists, and a main-server and backup-server was set.

For the follow-up failover configuration, see Setting Up DHCP Failover, on page 8.

Enable DHCP Classes of Service

Classes of service provide differentiated services to DHCP clients, the most common ones being:

- Address leases
- IP address ranges
- Addresses of the DNS servers serving the client
- Hostname assignments
- Denial of service through access controls

A class of service defined in the setup pages ultimately defines a:

- DHCP client-class with the same name as the class of service.
- DHCP policy with the same name as the class of service.
- DHCP scope assignment if the selection tag is defined as the class of service.

For the follow-up class of service configuration, see Setting Up DHCP Classes of Service, on page 9.

Server Logging Mode

The DHCP server provides log messages for which you can set the mode for the message output. The Server Logging Mode option has four possible values that translate into specific logging settings:

- **normal-operations (the preset value)—**Normal logging occurs.
- **high-performance—**High-performance logging occurs.
- **debugging—**Debug logging occurs.
- **customized—**Prompts to configure specific log settings, then logs only those settings.

Enable DHCP Traps

Setting SNMP traps for the DHCP server provides a way of reporting whether the server is up or down, the status of its partner communication, and whether it has a certain number of low or high free addresses available. DHCP traps are not enabled by default, so you have to set this value to **yes** to enable it. See Setting Up DHCP Traps, on page 11 for details.

Setting Up DHCP Failover

The Set up DHCP Failover page opens in the proper sequence if you set the Configure DHCP Failover value to **yes** on the Set up DHCP page in the setup interview.

The preset value for Configure DHCP Failover is **yes** and the DHCP Failover Role is preset to **main**. If you change the role of the current machine to **backup**, you cannot perform further failover configuration on this machine. (A message advises you to perform the failover configuration on the main server machine and do a failover synchronization from it.)

The Failover Partner value determines the address and access criteria for the remote backup server. If a cluster already exists for the server, you can choose the cluster from the Select existing cluster drop-down list. If there is no existing cluster, you can set one up for the backup server:

1. Enter the hostname or IP address of the backup DHCP server.
2. Enter the access criteria for the backup server: its administrator name and password, and SCP port number (preset to **1234**).
3. Click **Add Cluster** to add the cluster.

Decide if you want the failover pair to be in a load balancing relationship where lease assignments between the partner servers is 50% of the address pool for each server. If you want this load balancing to be in effect, set the Load Balancing value to **yes** (the preset value is **no**).

Choose or enter the configuration values you want, then click **Next** to activate your settings so that you can do further DHCP configuration.

Setting Up DHCP Classes of Service

The Set up DHCP Classes of Service page opens in the proper sequence if you set the Enable DHCP Classes of Service value to **yes** on the Set up DHCP page in the setup interview.

The preset value for the Enable DHCP Classes of Service is **yes**. Class of Service Usage sets whether you want the incoming DHCP packet to determine the class of service based on the incoming packet or register the clients individually on this page. If you choose to have the incoming packet assign the class of service, you need to do some configuration in Advanced mode, which involves setting an expression for the *client-class-lookup-id* DHCP server attribute. (See Assigning Classes of Service Based on Incoming Packets, on page 9.)

The DHCP Classes of Service values are for setting each class of service name and, optionally, the DNS forward zone to which you want to assign the class of service. For each class of service you add, click **Add Class of Service**.

Choose or enter the configuration values you want, then click **Next** to activate your settings so that you can do further DHCP configuration. If you chose under Class of Service Usage:

- **Assign class of service based on incoming packet?—**A special help link appears on the page (see Assigning Classes of Service Based on Incoming Packets, on page 9).
- **Register clients individually?** (the preset value)—List/Add DHCP Clients page opens (see Registering Clients Individually, on page 9).

Registering Clients Individually

The List/Add DHCP Clients page opens in the proper sequence if you enable the **Register clients individually?** Class of Service Usage setting on the Set up DHCP Classes of Service page. (See the *Configuring Clients* section of the *Cisco Prime IP Express 9.0 DHCP User Guide* for an example of the List/Add DHCP Clients page.)

On this page, enter the name of the DHCP client, and alternatively choose a preconfigured client-class from the drop-down list:

- If you also choose a client-class, the client is added to the list below without further configuration.
- If you omit the client-class, the Add DHCP Client page opens.
- For details on how to enter values on this page, see the *Configuring Clients* section of the *Cisco Prime IP Express 9.0 DHCP User Guide*. If you click the name of a client on the Add DHCP Client page, the Basic mode version of the Edit DHCP Client page opens (see the *Editing Clients and Their Embedded Policies* section of the *Cisco Prime IP Express 9.0 DHCP User Guide* for details).

Assigning Classes of Service Based on Incoming Packets

The Set up DHCP Classes of Service page changes to an informational page if you enable the **Assign class of service based on incoming packet?** Class of Service Usage setting on the Set up DHCP Classes of Service page.

Assigning classes of service based on incoming packets is less frequently used in Setup mode than registering clients individually and it requires Advanced mode configuration. Click **Next** on this page to go to the next setup task for DHCP. Then proceed as follows:

Step 1 Complete the setup pages to the end and exit Setup mode.

Step 2 Enter Advanced mode by clicking **Advanced**.

Step 3 Click **Deploy**, then **DHCP Server**.

Step 4 On the Manage DHCP Server page, click the Local DHCP Server link.

Step 5 On the Edit DHCP Server page, you need to enter an expression value (or include a reference to a file containing the expression) for the *client-class-lookup-id* attribute under the Client-Class category. Here are some examples of where you might want to set this attribute to differentiate clients:

- **Put Cisco IP phones in a voip client-class—**Search the incoming packet for the byte value 150 or 122 in the dhcp-parameter-request-list option (55). If found, assign the client the **voip** client-class:

```
(or
(if (search (byte 150) (request get-blob option 55)) "voip")
(if (search (byte 122) (request get-blob option 55)) "voip")
"<none>")
```

- **Put clients who share the first three bytes of their MAC addresses in a client-class—**Search the incoming packet for a MAC address starting with 01:02:03 and assign it the **red** client-class, and assign a MAC address starting with 04:05:06 the **blue** client-class:

```
(or
(if (starts-with (request get-blob chaddr) 01:02:03) "red")
(if (starts-with (request get-blob chaddr) 04:05:06) "blue")
"<none>")
```

- **Put Microsoft clients in an msftclass client-class—**Search the incoming packet for a *dhcp-class-identifier* option (60) value starting with MSFT and assign the client the **msftclass** client-class:

```
(or
(if (starts-with (request get-blob option 60) (as-blob "MSFT"))
"msftclass")
"<none>")
```

Step 6 Click **Save**.

Step 7 Click the **Restart Server** button in the Manage DHCP Server page to reload the server.

Managing DHCPv4 Subnet

The Scope Templates and Subnets page opens if you enable the DHCPv4 service and complete the configuration for DHCP failover in the setup interview. These subnets and scope templates are necessary to push the settings to local DHCP server.

You can define the scope template by entering its name in the Name field, then its expression in the Scope Name Expression field.

Click **Add Scope Templates** to add the scope template, then click **Next** to go to the Subnets page. Click the **Add Subnet** icon and enter the subnet address. Then push it by selecting the failover pair/cluster and scope template.

Managing DHCPv6 Prefix

The Prefix Template page opens if you enable the DHCPv6 service and complete the configuration for DHCP failover in the setup interview. These prefix and prefix templates are necessary to push the settings to local DHCP server.

You can define the prefix template by entering its name in the Name field, then its expression in the Prefix Name Expression field.

Click **Add Prefix Templates** to add the prefix template, then click **Next** to go to the Prefix page. Click the **Add Prefix** icon and enter the prefix address. Then push it by selecting the failover/cluster and prefix template.

Setting Up DHCP Traps

The Set up DHCP Traps page opens in the proper sequence if you set the Enable DHCP Traps value to **no** on the Set up DHCP page in the setup interview.

The preset value for Enable DHCP Traps is **no**. You need to determine which traps to set and how to set them. The Select DHCP Traps value determines the kind of traps to set. You can set all the traps or you can set selective ones that report:

- Server starts and stops (server-start and server-stop).
- When free addresses are detected (free-address-low and free-address-high).
- Size of the DNS queue (dns-queue-size).
- Whether partner servers are down or back up (other-server-down and other-server-up).
- Detected duplicate addresses (duplicate-address), address conflicts (address-conflict), or failover configuration errors (failover-config-error).

If you set the free address detection traps, you must also set their configurations:

- Name of the free address configuration (display-only value: **global**)
- How to determine the free addresses: by **scope**, **network**, or **scope-selection tags** (preset value: **scope**)
- Percentage of free addresses detected for which to generate a low-threshold trap and reenable the high threshold (preset value: **20%**)
- Percentage of free addresses detected for which to generate a high-threshold trap and reenable the low threshold (preset value: **25%**)

Choose or enter the configuration values you want, then click **Next** to activate your settings so that you can configure scopes for the DHCP addresses.

Managing DHCP Scopes

The Manage Scopes page opens if you enable the DHCP service and complete the last of the configuration pages for DHCP failover, classes of service, or traps in the setup interview. Scopes are address pools for which you want to set common lease configurations. These scopes are necessary for DHCP.

You can define the scope by entering its name in the Name field, then its subnet address (such as 192.168.50/24) in the Subnet field. If you configured a class of service in Setting Up DHCP Classes of Service, on page 9, you can also associate a class of service with the scope from the Class of Service drop-down list.

Click **Add Scope** to add the scope, then click **Next** to activate your settings and continue to the next configuration step. For example, if you chose to configure DHCP traps, you can configure the trap recipients next (see Setting Up Trap Recipients, on page 17), or you go to the DNS server configuration pages if you enabled the DNS server (see Setting Up DNS Service, on page 13).

Setting Up CDNS Service

The Set up CDNS page opens in the proper sequence if you set the Enable CDNS Server value to **yes,** and if the DNS Server role is set to **primary** on the Set up this Server page in the setup interview. It also opens if you click **CDNS** on the navigation bar.

Choose the configuration values you want, based on information in the following subsections, then click **Next** to activate your settings. The setup pages that follow are for configuring access controls and traps.

CDNS Server Role

A DNS server can be a caching server:

- **Caching—**Not authoritative for a zone and does not maintain a database of zone information, but answers queries through its cache and by querying authoritative name servers.

Server Logging Mode

The Caching DNS server provides log messages and you can set the mode for the message output. The Server Logging Mode option has four possible values that translate into specific logging settings:

- **normal-operations—**Normal logging occurs.
- **high-performance—**High-performance logging occurs.
- **debugging—**Debug logging occurs.
- **customized—**Prompts to configure specific log settings, then logs only those settings.

Enable CDNS Traps

Setting SNMP traps for the CDNS server provides a way of reporting whether the server is up or down. CDNS traps are not enabled by default, so you have to set this value to **yes** to enable it. See Setting Up CDNS Traps, on page 13 for details.

Setting Up CDNS Access Control

The Set up CDNS Access Control page opens in the proper sequence if you configured your CDNS server on the Set up CDNS page in the setup interview.

On this page, you can restrict queries and zone transfers based on an access control list (ACL):

- **dns-restrict-query-acl—**Provides a global ACL used to limit device queries that the DNS server honors. You can restrict query clients based on host IP address, network address, and other ACLs. The preset value is to allow **any** client to perform a query. Separate multiple ACL values with commas.
- **CDNS Forwarders—**If you want to set forwarders for a caching DNS server, specify the name and IP addresses and click **Add Forwarder**.

- **CDNS Resolution Exceptions—**If you do not want the CDNS server to use the usual method of querying root nameservers for certain names outside the domain, use resolution exception to bypass the root nameservers and target a specific server to handle name resolution. Enter any nameserver names and their comma-separated addresses, then click **Add Exception**.

Click **Next** to activate your settings and continue (or complete) the CDNS server configuration.

Setting Up CDNS Traps

The Set up CDNS Traps page opens in the proper sequence if you set the Enable CDNS Traps value to **yes** on the Set up CDNS page in the setup interview.

The preset value for Enable CDNS Traps is **yes**. You need to determine which traps to set and how to set them. The Select CDNS Traps value determines the kind of traps to set. The preset value for Select CDNS Traps is none. You can also set all the traps or selective ones that report i.e, Server starts and stops (server-start and server-stop).

Choose the configuration values you want, then click **Next** to activate your settings and complete the CDNS configuration.

Setting Up DNS Service

The Set up DNS page opens in the proper sequence if you set the Enable DNS Server value to **yes** on the Set up this Server page in the setup interview. It also opens if you click **DNS** on the navigation bar.

To set up the DNS server, be sure that the Enable DNS Server value is set to **yes**. If you already configured a primary DNS server elsewhere and synchronized to it, then the setup process advises you that the current Cisco Prime IP Express host is already configured as a secondary or caching server, and no further DNS configuration is necessary.

Choose the configuration values you want, based on information in the following subsections, then click **Next** to activate your settings. The setup pages that follow are for configuring forward and reverse DNS zones (including for High-Availability DNS servers), zone distributions, and access controls.

DNS Server Role

A DNS server can be a primary or secondary server:

- **Primary** (the preset value)—Authoritative for a zone and maintains this zone information in its database.
- **Secondary—**Loads a copy of the primary server zone information. The primary notifies the secondary about changes to its zone information and does a zone transfer to the secondary.
- **Caching—**Caches the query results.

If the server is a primary, you can also determine if you want it to be part of a High-Availability (HA) DNS server configuration (see Enable High-Availability DNS, on page 13 section). If the server is a secondary, you can set the access controls for the server only.

Enable High-Availability DNS

High-Availability (HA) DNS servers provide failover in case a server goes down. In this relationship, a second primary server can become a hot standby that shadows the main primary server.

To provide HA DNS service, set the Enable High-Availability DNS value to **yes**. If the setup process detects an existing complex HA DNS configuration, it notifies you that you are not allowed to configure HA DNS from the setup interview. You are prevented from HA DNS configuration in the setup pages if HA DNS was already configured in Advanced mode and one of the following conditions is true:

- More than one HA DNS server pair is configured.
- A single HA DNS pair exists, and a main-server or backup-server value was set.

For the follow-up HA DNS configuration, see Setting Up High-Availability DNS, on page 14.

Server Logging Mode

The DNS server provides log messages and you can set the mode for the message output. The Server Logging Mode option has four possible values that translate into specific logging settings:

- **normal-operations—**Normal logging occurs.
- **high-performance—**High-performance logging occurs.
- **debugging—**Debug logging occurs.
- **customized—**Prompts to configure specific log settings, then logs only those settings.

Enable DNS Traps

Setting SNMP traps for the DNS server provides a way of reporting whether the server is up or down, the status of its partner communication, partner configuration, master communication and secondary zone status. DNS traps are not enabled by default, so you have to set this value to **yes** to enable it. See Setting Up DNS Traps, on page 16 for details.

Setting Up High-Availability DNS

The Set up High-Availability DNS page opens in the proper sequence if you set the Enable High-Availability DNS value to **yes**, and if the DNS Server Role is set to '**primary**' on the Set up DNS Server page in the setup interview.

The preset value for Enable High-Availability DNS is **yes** and the preset value for HA DNS Role is **main**. The DNS Role is the role that you want this particular machine to perform. If you change the role of the current machine to **backup**, you cannot perform further failover configuration on this machine. (A message advises you to perform the failover configuration on the main server machine and to do an HA DNS synchronization from it.) Likewise, if Cisco Prime IP Express detects a complex HA DNS configuration, it warns you and you need to step past the HA DNS configuration setup.

The HA Partner value determines the address and access criteria for the remote backup server. If a cluster already exists for the server, you can choose the cluster from the Select existing cluster drop-down list. If there is no existing cluster, you can set one up for the backup server:

1. Enter the hostname or IP address of the backup DNS server.
2. Enter the access criteria for the backup server: its administrator name and password, and SCP port number (preset value: **1234**).
3. Click **Add Cluster** to add the cluster.

Choose or enter the configuration values you want, then click **Next** to activate your settings so that you can configure a DNS zone distribution.

Setting Up DNS Zone Distribution

The Set up DNS Zone Distribution page opens in the proper sequence if you configured your DNS server as a primary on the Set up DNS page in the setup interview.

The DNS Secondary Server(s) value determines which servers are the backup secondaries for the current DNS primary. You can choose the existing clusters where the secondary servers reside from the drop-down list, or you can add a new cluster. To create a new cluster:

1. Enter the hostname or IP address of the backup DNS server.
2. Enter the access criteria for the backup server: its administrator name and password, and SCP port number (preset value: **1234**).
3. Click **Add Cluster** to add the cluster.

Choose or enter the configuration values you want, then click **Next** to activate your settings so that you can configure zones for the DNS server.

Managing Forward Zones

The Manage Forward Zones page opens in the proper sequence if you configured your DNS server as a primary on the Set up DNS page in the setup interview.

You define the forward zone by entering its name in the Name field, its nameserver domain name in the Nameserver field (such as ns1.example.com.), and its hostmaster name in the Contact E-Mail field (such as hostmaster.example.com.).

Add the forward zone data, then click **Add Zone** in the Manage Forward Zones page to add the forward zone (see the *Configuring Primary Forward Zones* section of *Cisco Prime IP Express 9.0 Caching and Authoritative DNS User Guide*). Click **Next** to activate your settings so that you can add reverse zones for the DNS server.

Managing Reverse Zones

The Manage Reverse Zones page opens in the proper sequence if you configured your DNS server as a primary on the Set up DNS page and you configured a forward zone in the setup interview.

Cisco Prime IP Express creates the loopback reverse zone (127.in-addr.arpa.) automatically. You define additional reverse zones by entering the names in the Name field, the nameserver domain names in the Nameserver field (such as ns1.example.com.), and the hostmaster names in the Contact E-Mail field (such as hostmaster.example.com.). (Be sure to use fully qualified domain names by including the final dot in the name.)

Add the reverse zone data, then click **Add Zone** in the Manage Reverse Zones page to add the reverse zone (see the *Adding Reverse Zones as Zones* section of *Cisco Prime IP Express 9.0 Caching and Authoritative DNS User Guide*). Click **Next** to activate your settings so that you can add access controls for the DNS server.

Setting Up DNS Access Control

The Set up DNS Access Control page opens in the proper sequence if you configured your DNS server as primary or secondary on the Set up DNS page in the setup interview.

On this page, you can restrict queries and zone transfers based on an access control list (ACL):

- **dns-restrict-xfer-acl—**The default ACL that designates who is allowed to receive zone transfers. Setting the *restrict-xfer-acl* attribute on a zone overrides this setting. This setting does not apply to caching servers. The preset value is **none**. Separate multiple ACL values with commas.

Click **Next** to activate your settings and continue (or complete) the DNS server configuration.

Setting Up DNS Traps

The Set up DNS Traps page opens in the proper sequence if you set the Enable DNS Traps value to **yes** on the Set up DNS page in the setup interview.

The preset value for Enable DNS Traps is **yes**. You need to determine which traps to set and how to set them. The Select DNS Traps value determines the kind of traps to set. The preset value for Select DNS Traps value is **none**. You can also set all the traps or selective ones that report:

- Server starts and stops (server-start and server-stop).
- HA DNS partner up and down states (ha-dns-partner-up and ha-dns-partner-down) and configuration errors (ha-dns-config-error).
- Whether master servers are responding (masters-responding) or not responding (masters-not-responding).
- Whether secondary zones have expired (secondary-zone-expired).

Choose the configuration values you want, then click **Next** to activate your settings and complete the DNS configuration.

Setting Up DNS Update

The Set up DNS Update page opens in the proper sequence if you set the Enable DHCP Server value to **yes** and the Enable DHCP Update value to **yes** on the Set up this Server page in the setup interview. You must also have the Enable DNS Server set to **yes** if you want to use the local server for updates. The page also opens if you click **DNS Update** on the navigation bar, as long as the previous criteria are met.

On this page, you need to set the relationship among the DNS or DHCP servers for DNS Update to be effective:

- **DNS Server or HA Pair—**You can configure either a single DNS server or an HA DNS server pair for DNS Update. If a single server, the value is preset to **localhost**. If there is an HA DNS pair defined, you can choose its configuration name from the drop-down list. To define a new cluster, you can enter the Host name, IP address, Admin value, Password, and SCP Port value (preset value: 1234) in the respective fields, then click **Add Cluster**.
- **DHCP Server or Failover Pair—**You can configure either a single DHCP server or a DHCP failover server pair for DNS Update. If a single server, the value is preset to **localhost**. If there is a failover partnership defined, you can choose its configuration name from the drop-down list. To define a new cluster, you can enter the Host name, IP address, Admin value, Password, and SCP Port value (preset value: 1234) in the respective fields, then click **Add Cluster**.
- **Forward Zone Name—**You must define the forward zone that should receive DNS updates. The zone must already be defined for the DNS server or HA DNS pair. Enter the name of the zone in this field. You can also enter a comma-separated list of multiple forward zones if you want to differentiate them for classes of service. Otherwise you can select **example.com** (the preset value) or **none** from the Forward Zone Name drop-down list. If a reverse zone is already defined for the forward zone, completing this page also writes pointer (PTR) records to the appropriate reverse zone.

- **Secure DNS Updates?—**Set this value to **yes** if you want to use Transaction Signatures (TSIG) to secure DNS updates (the preset value is **no**). If enabled, the DNS server uses the TSIG key specified in its *dns-update-server-key* attribute, or the one defined in the following Server Key field.
- **Server Key—**If you enable Secure DNS Updates and a TSIG key exists, you can select it from the drop-down list. If the key does not exist, you can create one. Enter the key name in the Name field, then click **Generate Key** (this action uses the Cisco Prime IP Express **cnr-keygen** tool). Once you generate the key, its name appears in the Select existing key drop-down list.

Choose or enter the configuration values you want, then click **Next** to activate your settings and complete the DNS Update configuration.

Setting Up Trap Recipients

The Set up Trap Recipients page opens in the proper sequence if you enabled the DHCP or DNS server on the Set up this Server page and you also enabled traps on the setup pages for the DHCP or DNS server in the setup interview. The page also opens if you click **Traps** on the navigation bar, as long as the previous criteria are met.

For traps to be effective, you must specify the trap recipients (the hosts that should get trap notifications). Enter an identifying name for the host recipient, enter its IP address, then click **Add Trap Recipient**. Click **Next** to activate your settings and go to the Setup Interview Tasks page.

Setup Interview Tasks

The Setup Interview Tasks page opens if there is a task to perform based on the configurations in the setup interview. For example, creating a scope might require you to reload the DHCP server. The page identifies the task name, its ID, and the last time it ran. The Action column has a check box to select the task. To run one or more of the tasks, click **Run Selected Tasks**, which opens a confirmation page. On this page, click **Report and Exit** to go to the Setup Interview Report page.

Setup Interview Report

The Setup Interview Report page is the last page to open in the setup interview. The page summarizes the actions you took on the interview pages and gives you the session times and completion status.

Click **Exit Setup** to return to the Main Menu page.