Quick Start Guide for Cisco Network Registrar

Software Release 7.1
August 2009

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-16001-01

CONTENTS

Preface

This guide describes configuring Cisco Network Registrar by using the web-based user interface (web UI) and command line interface (CLI). The guide describes how to become familiar with Network Registrar features so that you can use them to administer network addresses.

Who Should Read This Guide

This guide is designed for network managers who are responsible for maintaining the network Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), Trivial File Transfer Protocol (TFTP), and Simple Network Management Protocol (SMTP) servers. The network manager should be familiar with the following topics:

- Basic concepts and terminology used in internetworking
- Network topology and protocols

How This Guide Is Organized

The two chapters in this guide are:

Document Conventions

This guide uses the documentation conventions described in the following sections.

Formatting

This guide uses the following formatting conventions:

- User input and controls are indicated in **bold**; for example, “enter **1234**” and “click **Modify Scope**.”
- Object attributes are indicated in *italics*; for example, “the *failover-safe-period* attribute.”

- Cross-references to chapters or sections of chapters are indicated in blue type; for example, "see the "Document Conventions" section on page v."

Navigation and Screens

This guide uses the following navigation and screen display conventions:

- Windows systems use a two-button mouse. To drag and drop an object, click and hold the left mouse button on the object, drag the object to the target location, then release the button.
- Solaris systems use a three-button mouse. To drag and drop an object, click and hold the middle mouse button on the object, drag the object to the target location, then release the button.
- Screen displays can differ slightly from those included in this guide, depending on the system or browser you use.

Callouts

Callouts in the text have the following meaning:

Caution *Be careful*. The description alerts you to potential data damage or loss.

Note *Take note*. The description is particularly noteworthy.

Timesaver *Save time*. The description can present a timesaver.

Tip *Consider this helpful hint*. The description can present an optimum action to take.

Product Documentation

Note We sometimes update the electronic documentation after original publication. Therefore, you should also review the documentation on Cisco.com for any updates.

Table 1 describes the product documentation that is available. You can view the marketing and user documents for Network Registrar at: http://www.cisco.com/en/US/products/sw/netmgtsw/ps1982/index.html.

Table 1 Product Documentation

Document Title	Available Formats
Quick Start Guide for Cisco Network Registrar 7.1 (This guide)	• PDF on the product CD-ROM • On Cisco.com: http://www.cisco.com/en/US/products/sw/netmgtsw/ps1982/prod_installation_guides_list.html
Documentation Guide for Cisco Network Registrar 7.1	• PDF on the product CD-ROM • On Cisco.com: http://www.cisco.com/en/US/products/sw/netmgtsw/ps1982/tsd_products_support_general_information.html
User Guide for Cisco Network Registrar 7.1	• PDF on the product CD-ROM • On Cisco.com: http://www.cisco.com/en/US/products/sw/netmgtsw/ps1982/products_user_guide_list.html
Installation Guide for Cisco Network Registrar 7.1	• PDF on the product CD-ROM • On Cisco.com: http://www.cisco.com/en/US/products/sw/netmgtsw/ps1982/prod_installation_guides_list.html
CLI Reference Guide for Cisco Network Registrar 7.1	• As an HTML document that you can view in your web browser when you install the software. The document is available at Programs > Network Registrar > Registrar CLI Reference Guide. • On Cisco.com: http://www.cisco.com/en/US/products/sw/netmgtsw/ps1982/prod_command_reference_list.html
Release Notes for Cisco Network Registrar 7.1	On Cisco.com: http://www.cisco.com/en/US/products/sw/netmgtsw/ps1982/prod_release_notes_list.html
Online Help	Choose Help > Help Contents in the main menu to view the entire help contents

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

CHAPTER 1

Introducing the Setup Web UI

The local cluster Network Registrar web UI, provides a setup environment in Basic user mode. The setup is in the form of a series of interview pages, very much like a wizard, based only on the selections you make.

Setup Functions

The setup pages provide these functions:

- User password change
- Dynamic host configuration:
  - Enable the Dynamic Host Configuration (DHCP) service
  - Set up DHCP failover between two servers
  - Set up classes of service
  - Enable Simple Network Management Protocol (SNMP) traps
- Domain names and hosts:
  - Enable the Domain Name System (DNS) service
  - Set up High-Availability (HA) DNS servers
  - Set up zone distributions to coordinate primary and secondary servers
  - Manage forward and reverse zones
  - Configure access controls
  - Enable SNMP traps
- DNS Update for dynamic hosts
- Simple Network Management Protocol (SNMP) trap recipients
- Trivial File Transport Protocol (TFTP) server

Setup Features and Navigation

The setup pages:

- Take you out of Basic and Advanced user modes and into special Setup mode. Basic and Advanced modes are for more specialized configuration after you set up the environment using the setup interview. These modes (and the server concepts) are described in detail in the *User Guide for Cisco Network Registrar*.
- Have an initial Set Up This Server page where you can enable and disable functions and which is the point of departure for all enabled function pages.
- Include **<<Back**, **Next>>**, and **Finish** buttons on pages so that you can step through sequentially, except that the **<<Back** is not on the Set Up This Server page and the **Next>>** button is not on the Setup Interview Report page. The **Finish** button jumps directly to the Setup Interview Report page.

  Note Do not use the browser's **Back** and **Forward** buttons to navigate through the setup process.

- Include the **Next>>** button that opens further pages depending on the criteria you set. For example, if the DNS server is enabled, but the server is not indicated as primary, the setup pages bypass the High-Availability (HA) DNS server, zone distribution, and forward and backward zone configuration pages.
- Provide a menu bar (**Services**, **DHCP**, **DNS**, **DNS Update**, **Traps**, and **Report**) so that you can access functions despite their enabled/disabled status on the Set Up This Server page. However, if a function is disabled on the Set Up This Server page, the function appears disabled on its setup page. You can change the status on the particular setup page, which resets the status on the Set Up This Server page.
- Are sometimes transactional and sometimes not. In some cases (such as with creating clusters and keys), writes to the database occur immediately when you enter a value. In other cases, writes to the database occur only when you click **Next>>** or **Finish**.
- Keep track of database writes and summarizes them on a report page when you click **Finish**.
- Provide initial selection defaults, and persist changes to the next setup. (For subsequent setups, the previously configured values become the new defaults.)

Configuration Options

The sample configuration shown in this guide is based on the typical use cases described in the following sections.

Mixed DHCP and DNS Scenarios

You can set up Network Registrar for a mixed DHCP and DNS configuration with different numbers of machines.

One-Machine Mixed Configuration

Configure both DHCP and DNS servers on a single machine, initially enabling the servers as primaries, and enabling the TFTP server and SNMP traps. Then configure at least one forward zone and corresponding reverse zone, at least one scope, and DNS Update.

Two-Machine Mixed Configuration

A mixed DHCP configuration on two machines offers a few alternatives:

- Configure one machine as primary DHCP and DNS servers, and the second machine as a secondary DNS server. Then configure a zone distribution and DNS access controls on the first machine and optionally access controls on the second machine.
- Configure one machine as DHCP and DNS main servers and the second machine as DHCP and DNS backup servers. Perform minimal configuration on the backup machine (changing the password, enabling DHCP and DNS, and selecting partner backup roles). On the main machine, build the configuration, creating server pairs and scheduling synchronization tasks with the backup machine.
- Configure one machine as a DHCP server and the second machine as a DNS primary, then configure either machine with DNS Update and push the configuration to the other machine.

Three-Machine Mixed Configuration

A mixed configuration on three machines offers a few additional alternatives:

- Configure one machine as a DHCP server, the second machine as a DNS primary, and the third machine as a DNS secondary. Optionally revisit the machines to make the DHCP main the DNS backup, and make the DNS main the DHCP backup.
- Configure one machine as DHCP failover and DNS High-Availability (HA) main servers, the second machine as DHCP failover and DNS HA backup servers, and the third machine as a DNS secondary server.

Four-Machine Mixed Configuration

A mixed configuration on four machines can include:

- DHCP and DNS main and backup pairs, with the first machine as a DHCP main, the second machine as a DHCP backup, the third machine as a DNS main configured with DNS Update, and the fourth machine as a DNS backup.
- An add-on to the three-machine scenario, with the first machine as a DHCP main, the second machine as a DNS main, the third machine as DHCP and DNS backups, and the fourth machine as a DNS secondary.

DHCP-Only Scenarios

A DHCP-only configuration can be on a single machine or two machines.

One-Machine DHCP Configuration

Initially configure just DHCP, skip the class-of-service and failover options, and revisit the setup to enable class-of-service and policy options.

Two-Machine DHCP Configuration

Configure the first machine as a DHCP main and the second machine as a backup, with minimal backup configuration (changing password, enabling DHCP, and selecting the backup role), and set up the first machine with failover load balancing, optionally scheduling failover synchronization tasks.

DNS-Only Scenarios

A DNS-only configuration can be on one, two, or three machines.

One-Machine DNS Configuration

Initially configure just DNS as a primary, secondary, or caching server.

Two-Machine DNS Configuration

Configure the first machine as a DNS primary and the second machine as a secondary, or the first machine as a main primary and the second machine as a backup primary.

Three-Machine DNS Configuration

Configure the first machine as a DNS main primary, the second machine as a backup primary, and the third machine as a secondary server.

CHAPTER 2

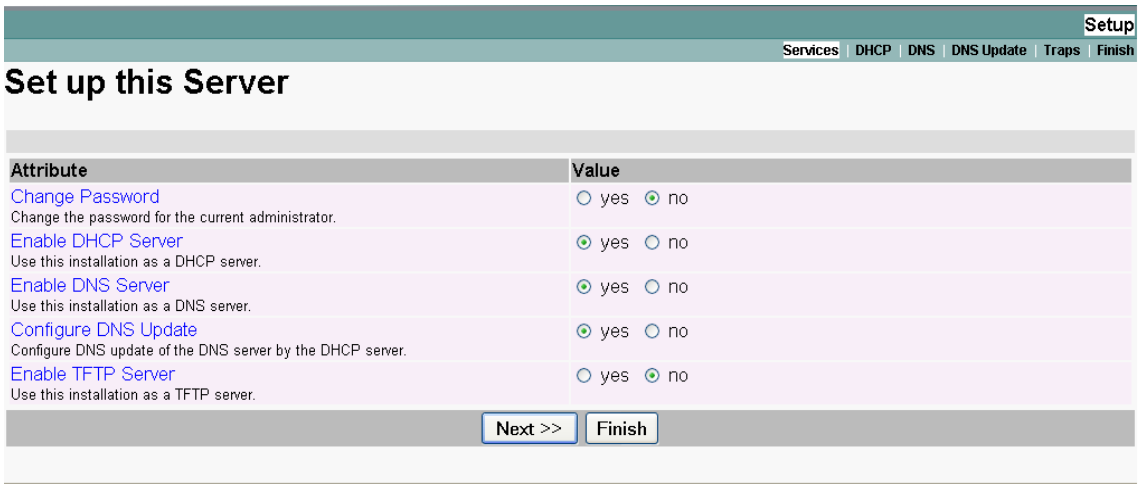
Running the Setup Web UI

The Cisco Network Registrar setup interview in the web user interface (UI) takes you through a series of consecutive pages to set up a basic configuration. For an introduction, configuration scenarios, and details on the basic navigation for the pages, see Chapter 1, "Introducing the Setup Web UI."

Setting Up Services

The Set Up This Server page opens when you click **Setup** on the navigation bar (or the Set up this Network Registrar Server link on the Main Menu page) in local Basic user mode. You immediately go into Setup mode and the Basic and Advanced tabs disappear (see Figure 2-1 on page 2-1).

Figure 2-1 Set Up This Server Page (Setup)



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 shipped preset value. See the "Changing the Administrator Password" section on page 2-2 for details.
- **Dynamic Host Configuration Protocol (DHCP) server**—DHCP provides the mechanism for dynamic address assignment that is an essential part of Network Registrar. Enabling DHCP goes to a series of pages for DHCP setup; disabling it bypasses the DHCP setup. See the "Setting Up DHCP Service" section on page 2-3 for details.

- **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 the "Setting Up DNS Service" section on page 2-10 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 the "Setting Up DNS Update" section on page 2-17 for details.
- **Trivial File Transfer Protocol (TFTP) server**—You might need to enable the TFTP server so that you can transfer files for provisioning addresses to cable modems. Enabling TFTP does not require further configuration in the setup pages (see the "Setup Interview Report" section on page 2-19).

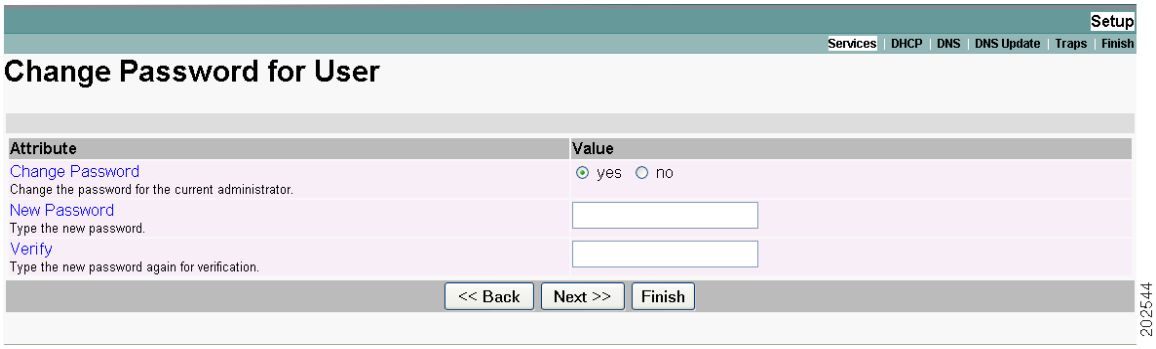
Note Selections you make are retained across login sessions.

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 (see Figure 2-2 on page 2-2) opens if you set the Change Password value to **yes** on the Set Up This Server page in the setup interview.

Figure 2-2 Change Password for User Page (Setup)



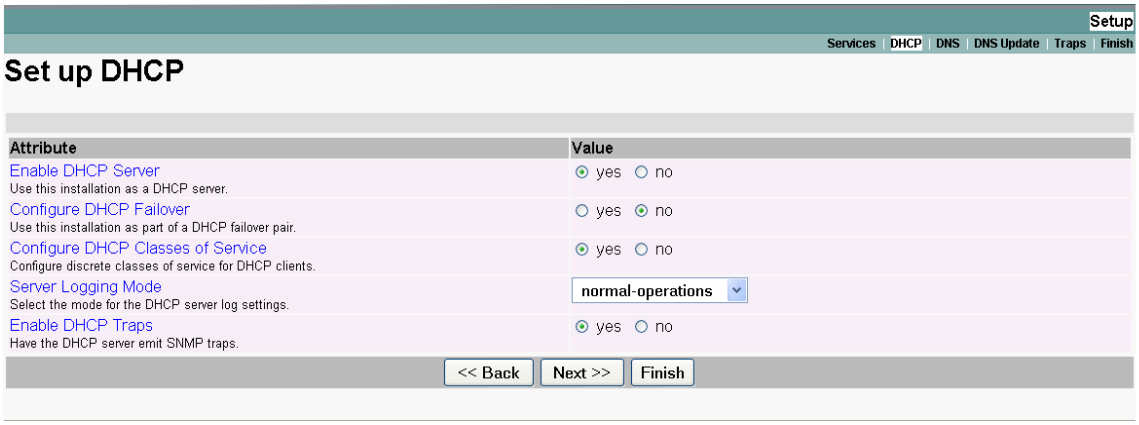
Changing the password ensures that subsequent administrator logins no longer use the preset password supplied at product shipment, but instead use the one you specify. This change is usually advisable to reduce security breaches.

To make the change, enter the new password, then enter it again to verify it; otherwise, click **no** for Change Password. Clicking **Next>>** or **Finish** submits your change, if any, for the next login session.

Setting Up DHCP Service

The Set Up DHCP page (see Figure 2-3 on page 2-3) 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.

Figure 2-3 Set Up DHCP Page (Setup)



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 Network Registrar 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 configuring 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 Enable 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, backup-server, or network-match-list value was set.

For the follow-up failover configuration, see the "Setting Up DHCP Failover" section on page 2-5.

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 the "Setting Up DHCP Classes of Service" section on page 2-6.

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.

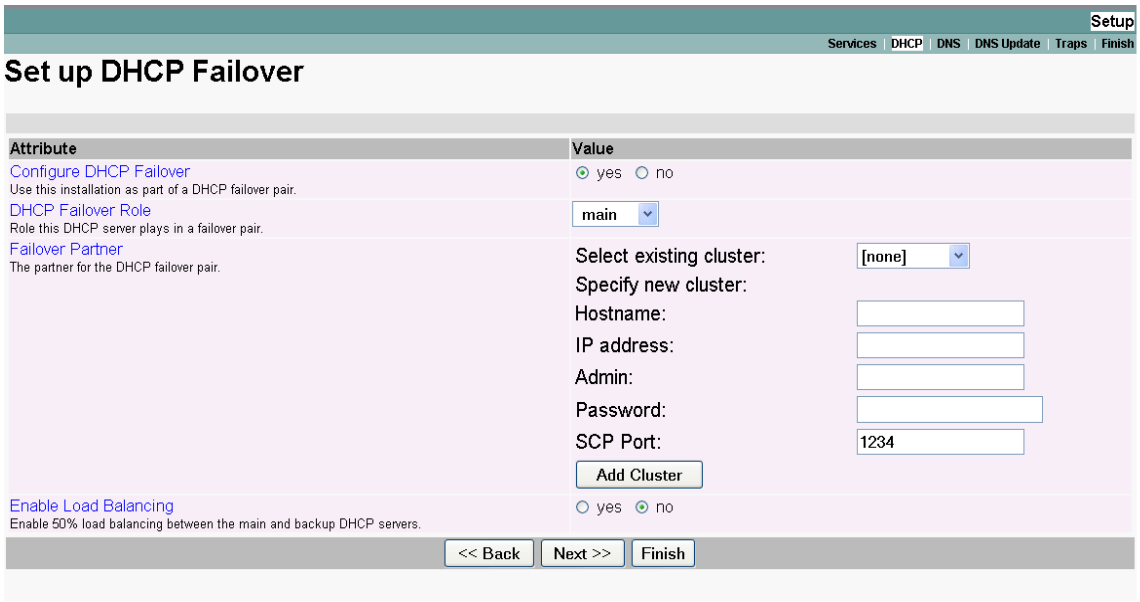
Enable DHCP Traps

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 the "Setting Up DHCP Traps" section on page 2-8 for details.

Setting Up DHCP Failover

The Set Up DHCP Failover page (see Figure 2-4 on page 2-5) opens in the proper sequence if you set the Enable DHCP Failover value to **yes** on the Set Up DHCP page in the setup interview.

Figure 2-4 Set Up DHCP Failover Page (Setup)



The preset value for Enable 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.) Likewise, if Network Registrar detects a complex failover configuration, it warns you and you need to step past the failover configuration setup.

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.

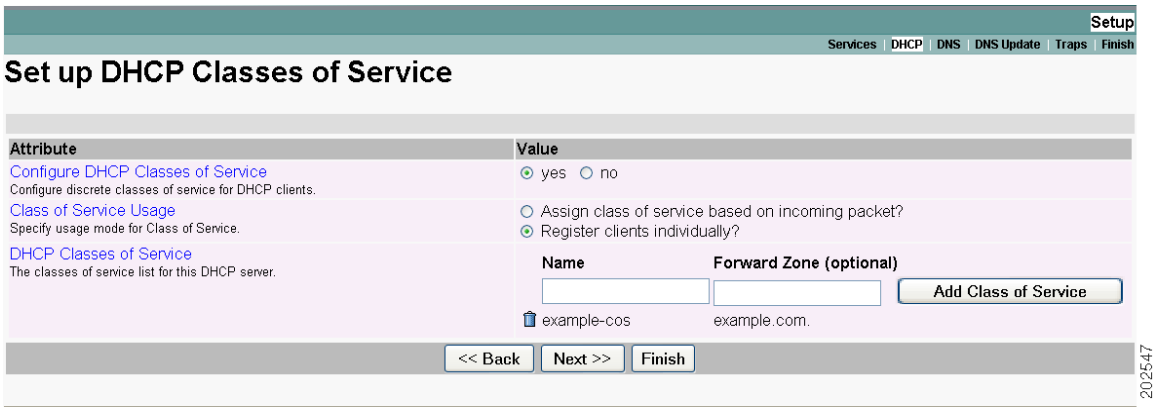
Decide if you want the failover pair to be in a load balancing relationship where lease assignments between the partner servers is 50% of the address pool for each server. If you want this load balancing to be in effect, set the Load Balancing value to **yes** (the preset value is **no**).

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 (see Figure 2-5 on page 2-6) 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.

Figure 2-5 Set Up DHCP Classes of Service Page (Setup)



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 the "Assigning Classes of Service Based on Incoming Packets" section on page 2-7.)

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 the "Assigning Classes of Service Based on Incoming Packets" section on page 2-7).
- **Register clients individually?** (the preset value), the List/Add DHCP Clients page opens (see the "Registering Clients Individually" section).

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 *User Guide for Cisco Network Registrar* 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 *User Guide for Cisco Network Registrar*. If you click the name of a client on the Add DHCP Client page, you open the Basic mode version of the Edit DHCP Client page (see the *Editing Clients and Their Embedded Policies* section of the *User Guide for Cisco Network Registrar* 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 in the setup interview.

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 **DHCP**, 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>")
```

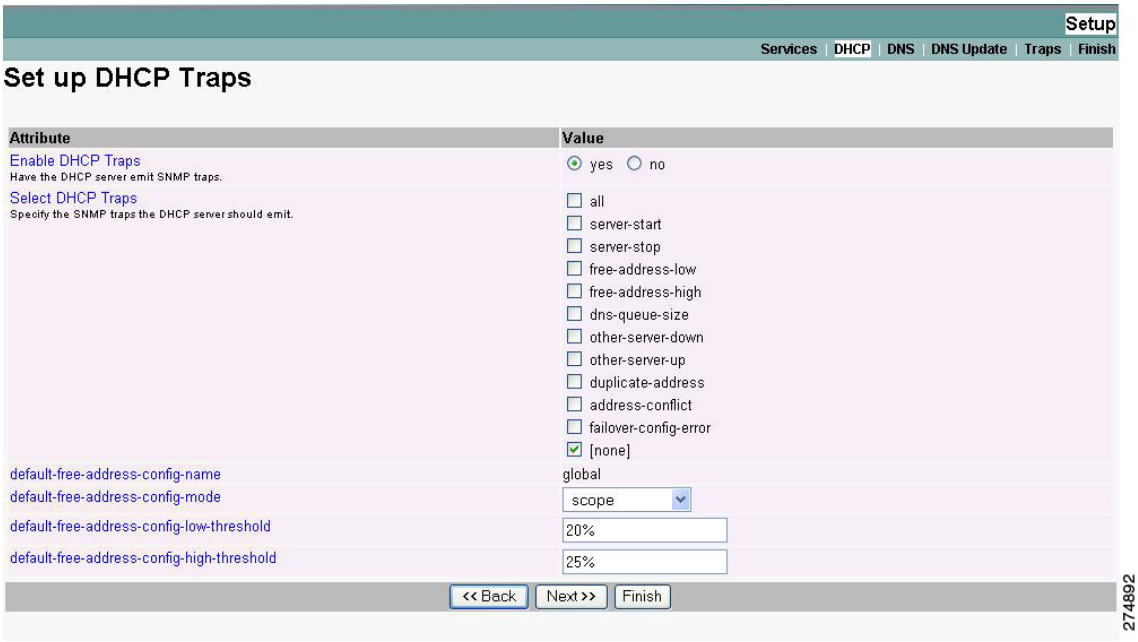
Step 6 Click **Modify Server**.

Step 7 Reload the DHCP server.

Setting Up DHCP Traps

The Set Up DHCP Traps page (see Figure 2-6 on page 2-8) opens in the proper sequence if you set the Enable DHCP Traps value to **yes** on the Set Up DHCP page in the setup interview.

Figure 2-6 Set Up DHCP Traps Page (Setup)



The preset value for Enable DHCP Traps is **yes**. 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:

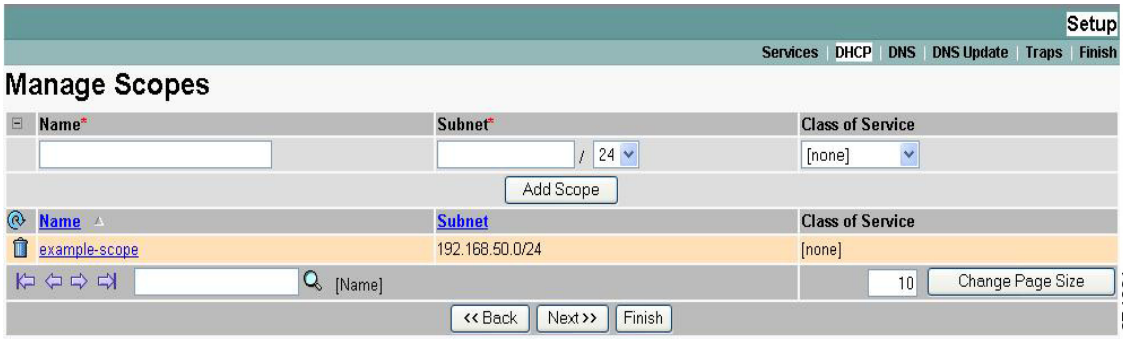
- Name of the free address configuration (display-only value: **global**)
- How to determine the free addresses: by **scope**, **network**, or **scope-selection tags** (preset value: **scope**)
- Percentage of free addresses detected for which to generate a low-threshold trap and reenable the high threshold (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 (see Figure 2-7 on page 2-9) 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.

Figure 2-7 Manage Scopes Page (Setup)



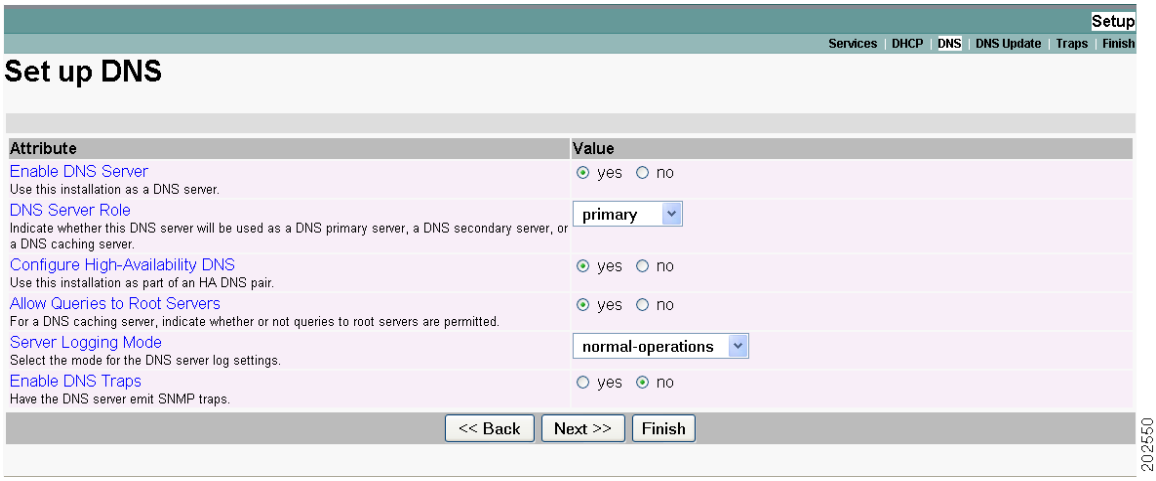
In Figure 2-7, an example-scope was already defined. You define the scope by entering its name in the Name field, then its subnet address (such as 192.168.50/24) in the Subnet field. If you configured a class of service in the "Setting Up DHCP Classes of Service" section on page 2-6, you can also associate 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 the "Setting Up Trap Recipients" section on page 2-18), or you go to the DNS server configuration pages if you enabled the DNS server (see the "Setting Up DNS Service" section).

Setting Up DNS Service

The Set Up DNS page (see Figure 2-8 on page 2-10) 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.

Figure 2-8 Set Up DNS Page (Setup)



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 Network Registrar 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, secondary, or caching 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**—Not authoritative for a zone and does not maintain a database of zone information, but answers queries through its cache.

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 the "Enable High-Availability DNS" section). If the server is a secondary, you can set the access controls for the server only. If the server is caching, you can decide if you want it to allow queries to internal root servers (see the "Allow Queries to Root Servers" section on page 2-11), and then set the access controls for the caching server.

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 the "Setting Up High-Availability DNS" section.

Allow Queries to Root Servers

If you set up the current DNS server as a nonauthoritative caching server, you can opt to allow clients to query internal root servers for zone information. To provide this service, set the Allow Queries to Root Servers value to **yes**.

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** (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.

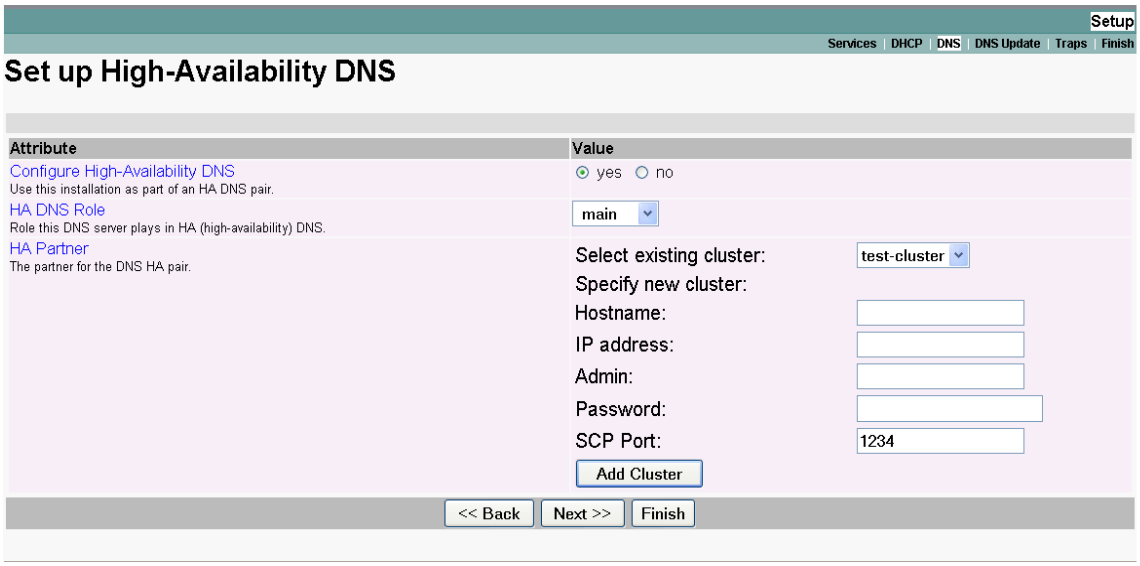
Enable DNS Traps

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, and whether it has a certain number of low or high free addresses available. DNS traps are not enabled by default, so you have to set this value to **yes** to enable it. See the "Setting Up DHCP Traps" section on page 2-8 for details.

Setting Up High-Availability DNS

The Set Up High-Availability DNS page (see Figure 2-9 on page 2-12) opens in the proper sequence if you set the Enable High-Availability DNS value to **yes** on the Set Up DNS Server page in the setup interview.

Figure 2-9 Set Up High-Availability DNS Page (Setup)



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 Network Registrar 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:

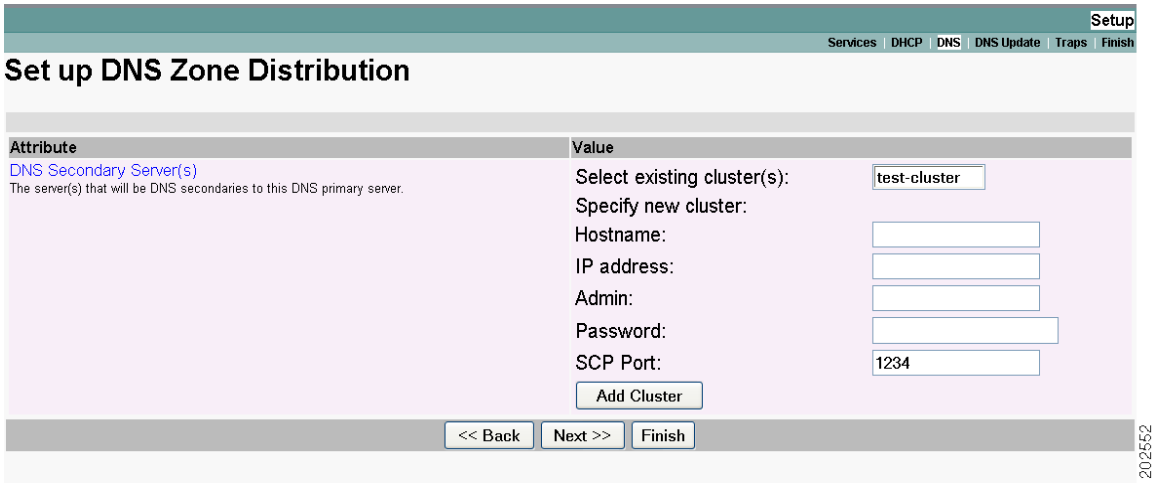
1. Enter the hostname or IP address of the backup DNS server.
2. Enter the access criteria for the backup server: its administrator name and password, and SCP port number (preset value: **1234**).
3. Click **Add Cluster** to add the cluster.

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 (see Figure 2-10 on page 2-13) opens in the proper sequence if you configured your DNS server as a primary on the Set Up DNS page in the setup interview.

Figure 2-10 Set Up DNS Zone Distribution Page (Setup)



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:

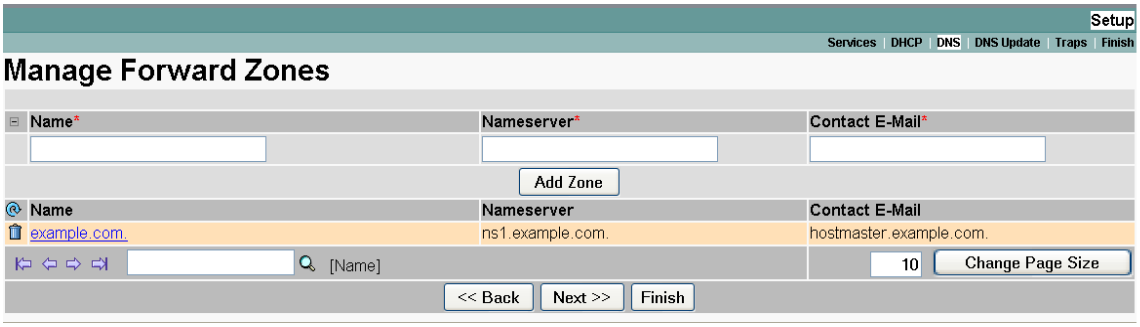
1. Enter the hostname or IP address of the backup DNS server.
2. Enter the access criteria for the backup server: its administrator name and password, and SCP port number (preset value: **1234**).
3. Click **Add Cluster** to add the cluster.

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 (see Figure 2-11 on page 2-14) opens in the proper sequence if you configured your DNS server as a primary on the Set Up DNS page in the setup interview.

Figure 2-11 Manage Forward Zones Page (Setup)



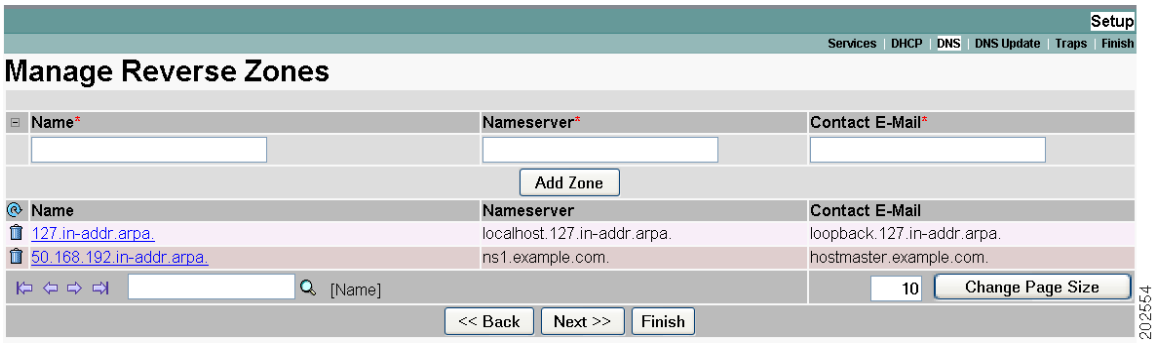
In Figure 2-11, an example.com zone was already defined. You define the forward zone by entering its name in the Name field, its nameserver domain name in the Nameserver field (such as ns1.example.com.), and its hostmaster name in the Contact E-Mail field (such as hostmaster.example.com.).

Click **Add Zone** to open the Add DNS Forward Zone page (see the *Configuring Primary Forward Zones* section of the *User Guide for Cisco Network Registrar*). Add the forward zone data, then click **Add Zone** to return to the Manage Forward Zones page. 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 (see Figure 2-12 on page 2-14) opens in the proper sequence if you configured your DNS server as a primary on the Set Up DNS page (see Figure 2-8 on page 2-10) and you configured a forward zone in the setup interview.

Figure 2-12 Manage Reverse Zones Page (Setup)



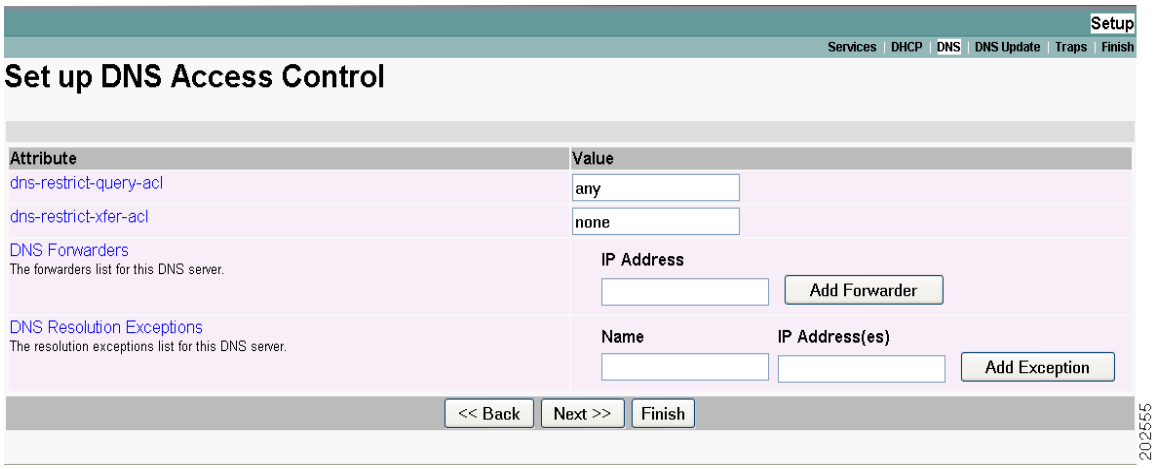
In Figure 2-12, a reverse zone was already defined. Network Registrar creates the loopback reverse zone (127.in-addr.arpa) automatically. You define additional reverse zones by entering the names in the Name field, the nameserver domain names in the Nameserver field (such as ns1.example.com.), and the 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.)

Click **Add Zone** to open the Add DNS Reverse Zone page (see the *Adding Primary Reverse Zones* section of the *User Guide for Cisco Network Registrar*). Add the reverse zone data, then click **Add Zone** to return to the Manage Reverse Zones page. 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 (see Figure 2-13 on page 2-15) opens in the proper sequence if you configured your DNS server as primary, secondary, or caching on the Set Up DNS page in the setup interview.

Figure 2-13 Set Up DNS Access Control Page (Setup)



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

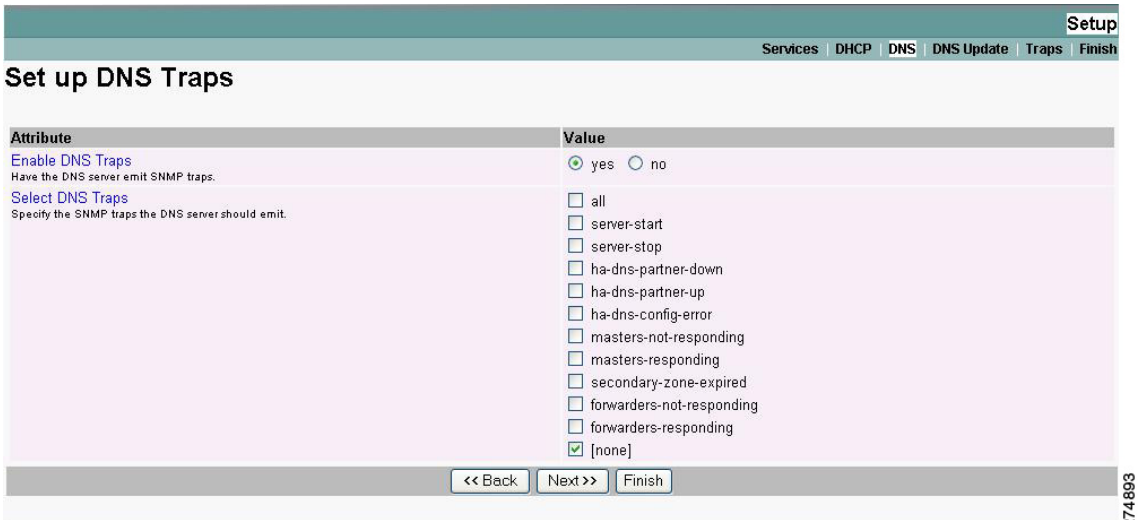
- **dns-restrict-query-acl**—Provides a global ACL used to limit device queries that the DNS server honors. You can restrict query clients based on host IP address, network address, TSIG keys, and other ACLs. The preset value is to allow **any** client to perform a query. Zones inherit this ACL if they are missing their *dns-restrict-query-acl* attribute value. This ACL also serves to filter queries for nonauthoritative zones. Separate multiple ACL values with commas.
- **dns-restrict-xfer-acl**—The default ACL that designates who is allowed to receive zone transfers. Setting the *restrict-xfer-acl* 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.
- **DNS Forwarders**—If you want to set forwarders for a caching DNS server, if you did not allow queries to root servers (see the "Allow Queries to Root Servers" section on page 2-11), you can enter the comma-separated IP addresses of the forwarding server in the IP Address field, then click **Add Forwarder**.
- **DNS Resolution Exceptions**—If you do not want the DNS 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 DNS server configuration.

Setting Up DNS Traps

The Set Up DNS Traps page (see Figure 2-14 on page 2-16) 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.

Figure 2-14 Set Up DNS Traps Page (Setup)



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:

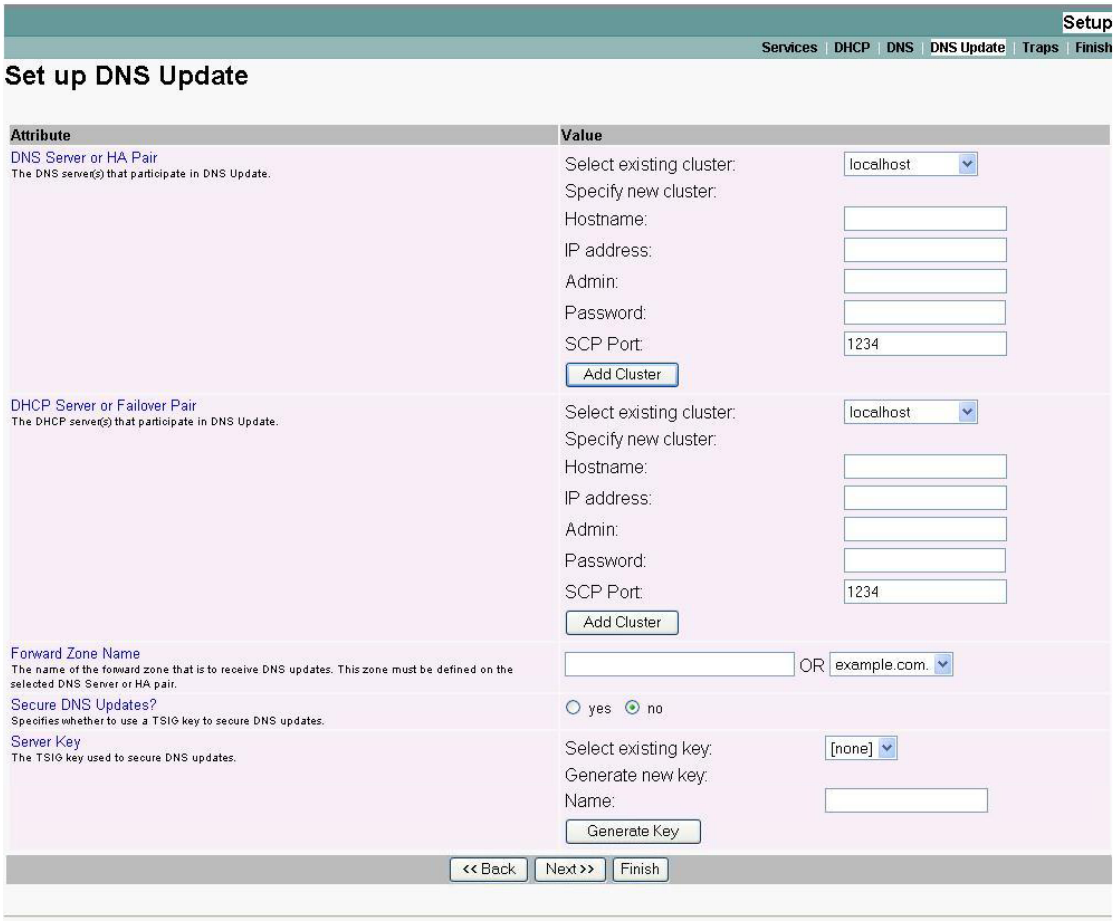
- Server starts and stops (server-start and server-stop).
- HA DNS partner up and down states (ha-dns-partner-up and ha-dns-partner-down) and configuration errors (ha-dns-config-error).
- Whether master and forwarding servers are responding (masters-responding) or not responding (masters-not-responding).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

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 (see Figure 2-15 on page 2-17) 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.

Figure 2-15 Set Up DNS Update Page (Setup)



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**.

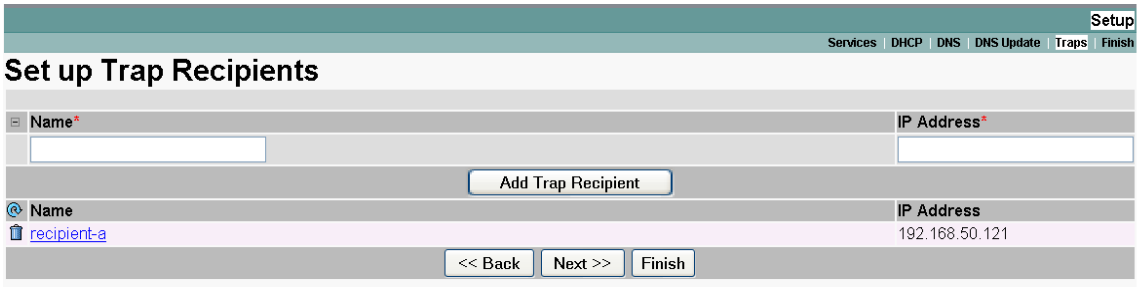
- **Forward Zone Name**—You must define the forward zone that should receive DNS updates. The zone must already be defined for the DNS server or HA DNS pair. Enter the name of the zone in this field. You can also enter a comma-separated list of multiple forward zones if you want to differentiate them 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 if 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 Network Registrar **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 (see Figure 2-16 on page 2-18) 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.

Figure 2-16 Set Up Trap Recipients Page (Setup)

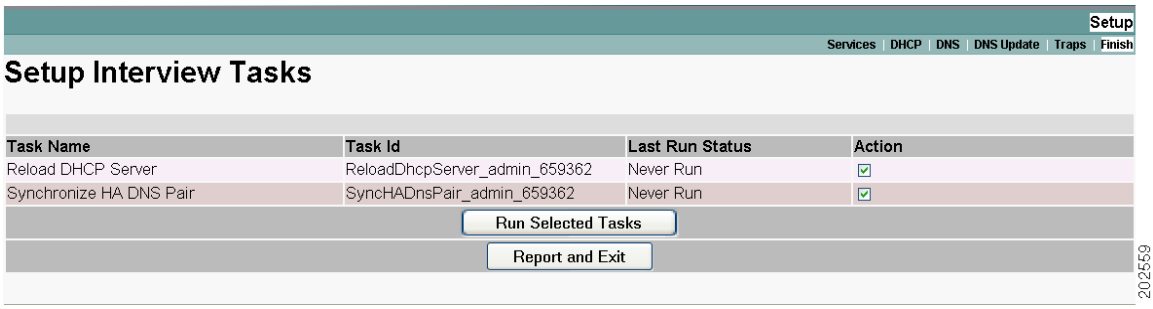


For traps to be effective, you must specify the trap recipients (the hosts that should get trap notifications). Enter an identifying name for the host recipient, enter its IP address, then click **Add Trap Recipient**. Click **Next>>** to activate your settings and go to the Setup Interview Tasks page.

Setup Interview Tasks

The Setup Interview Tasks page opens if there is a task to perform based on the configurations in the setup interview (see Figure 2-17 on page 2-19). 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.

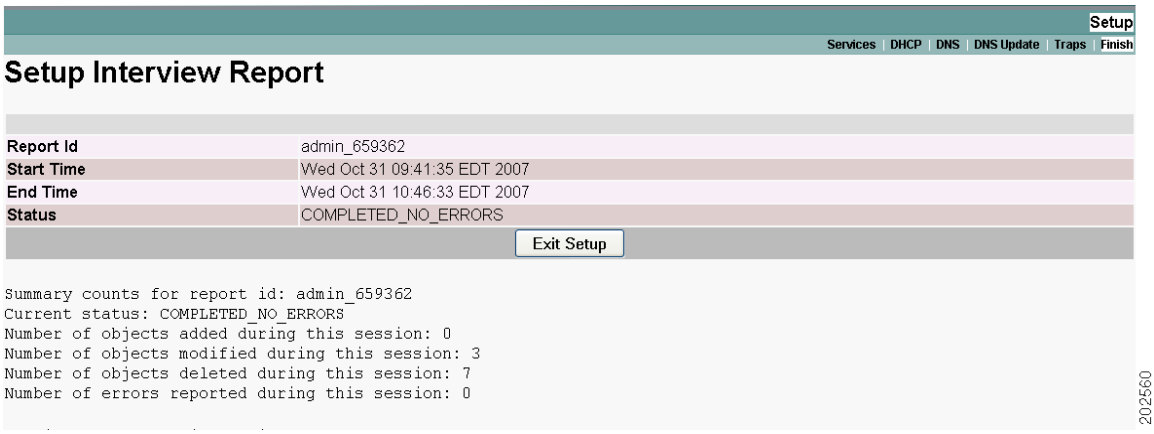
Figure 2-17 Setup Interview Tasks Page (Setup)



Setup Interview Report

The Setup Interview Report page (see Figure 2-18 on page 2-19 for an example) 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.

Figure 2-18 Setup Interview Report Page (Setup)



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

INDEX

R

S

T

U

Z