Configuring the Content Routing Software

This chapter describes the basic steps for configuring the Content Router software.

Performing a Basic Startup Configuration

After you physically install the Content Router hardware, configure the Content Routing software by performing these tasks in the following order:

1. Collecting the Information Required for Initial Configuration

2. Initializing the Content Router Software

3. Configuring Direct or WCCP Mode

4. Creating Agent (Client) Lists

5. Configuring Domains on the Content Router

6. Configuring the Content Routing Agents

7. Verifying the Content Router Configuration

Note   See Appendix C, "Cisco Content Routing Software, Release 1.1 Commands," for detailed information about many of the commands mentioned in this chapter.

Collecting the Information Required for Initial Configuration

Step 1   Have the following information available for the Content Router. When you power on the Content Router for the first time, you are prompted to provide this information:

- Host name
- Domain name
- Administrator password
- Host IP address
- IP network mask
- Gateway IP address
- Domain Name System (DNS) name server IP address

Step 2   Gather the following information for each domain you want the Content Router to support:

- Domain name
- Origin server
- IP address of each machine you intend to use as a content routing agent

Step 3   Open a window for the Content Router console using your terminal emulation program and power on the Content Router.

When the Content Router begins booting, it sends messages to the console window. After the operating system boots, you are ready to initialize the basic software configuration.

Step 4   Proceed to the next section, "Initializing the Content Router Software."

Initializing the Content Router Software

To initialize the Content Router basic software configuration after the operating system has booted:

Step 1   Enter values for the following parameters as you are prompted:

- Host name for the Content Router
- Domain name for the Content Router
- Admin password for the Content Router

  This is the password you want to use for the **admin** user account, which is predefined on the Content Router. The password is case sensitive and can be up to 20 characters, including spaces and any printable characters. You cannot set the passwords globally. Verify the password for the **admin** user account (or press **Enter** without entering a password to keep the existing password).

  ✎
  Note   The Content Router does not display ***** (asterisks) while you are verifying your admin password.

- IP address for the Content Router, for example, 10.1.1.1

- IP network mask for the Content Router, for example, 255.255.255.0

  A network mask specifies which part of the IP address refers to the network; you can accept the default value by pressing **Enter**, or enter a different value.

- Gateway IP address for the Content Router, for example, 10.1.1.2

  This is the IP address of the router that allows the Content Router to connect to the network.

- DNS name server IP address for the Content Router

A sample of a basic configuration follows.

```
---- System Configuration Dialog ----
You may use Ctrl-D to abort Configuration Dialog at any prompt.
Would you like to enter the initial configuration? [yes]: yes
host name: boomerang
domain name: cisco.com
admin password: test
host IP address: 10.1.58.5
IP network mask: 255.255.255.0
gateway IP address: 10.1.58.1
DNS server: 172.16.2.132
```

Step 2   If the basic configuration is acceptable, enter **yes**. The Content Router indicates whether the configuration is accepted. At this point, the basic configuration is finished.

```
Use this configuration? [yes]: yes
>> Building configuration...
>> . . START - phase complete
```

Step 3   Proceed to the next section, "Configuring Direct or WCCP Mode."

Configuring Direct or WCCP Mode

The Content Router can operate in either direct mode or Web Cache Communication Protocol (WCCP) mode. To operate in direct mode, direct mode must be enabled on the Content Router. In direct mode, the Content Router acts as the authoritative DNS server for all domains configured on the Content Router. DNS Address requests are sent directly from a local DNS server to the Content Router. To operate in WCCP mode, WCCP must be enabled on the Content Router as well as on a router in the path to the Content Router and the primary DNS server. This router must also be configured to send DNS Address requests to the Content Router.

In performing the configuration tasks that follow, it may be useful to refer to the "Direct Mode" section on page 1-1 for a description and diagram of a boomerang-configured network in direct mode, and the "WCCP Mode" section on page 1-2 for a description and diagram of a boomerang-configured network in WCCP mode.

Configuring Direct Mode

Step 1   To establish the Content Router as the authoritative DNS server for a domain, configure the domain's primary DNS server.

For example, to make a Content Router with IP address 10.10.10.1 the DNS server for www.domain.com, you would add these DNS resource records:

```
www.domain.com  IN  NS  boomerang
boomerang       IN  A   10.10.10.1
```

Step 2   Use the **boomerang dns enable** command on the Content Router to specify direct mode.

```
Console (config)# boomerang dns enable direct-mode
```

Step 3   Proceed to the .

Configuring WCCP Mode

In order to configure WCCP on a router, you must already be familiar with basic router configuration. If you are not familiar with basic router configuration, consult the Cisco IOS documentation supplied with the router. Detailed information for the router commands mentioned here is in the Cisco IOS documentation. Refer to Appendix A, "Web Cache Communication Protocol Version 2," for more information.

To configure a router to redirect DNS address requests to the Content Router:

Step 1   Ensure that the router is running a release of the Cisco IOS software that includes WCCP Version 2. If it does not have this support, upgrade the Cisco IOS software before continuing.

Step 2   In global configuration mode, use the **ip wccp** command to enable WCCP support. The boomerang service is represented by service number 50, so enter:

```
Router(config)# ip wccp 50
```

Step 3   In interface configuration mode, use the **ip wccp 50 redirect out** command to have the interface redirect requests to the Content Router. Enter this command for each interface that is an outgoing interface connecting to subnets containing authoritative DNS servers.

You can confirm your settings using the following **show** commands on the router:

- **show ip wccp** shows the number of Content Routers and total number of packets redirected.
- **show ip wccp 50 detail** shows detailed information about each Content Router connected to the router.
- **show ip interface** shows detailed information about an interface, including whether WCCP redirection is enabled.

Step 4   Use the **boomerang dns enable** command on the Content Router to establish WCCP mode and configure the Content Router to accept redirected DNS address requests.

```
Console (config)# boomerang dns enable wccp-mode
```

Step 5   Enable WCCP and associate the Content Router with downstream routers. For example, if the router IP address is 172.46.67.1, enter these commands:

```
Console (config)# wccp router-list 1 172.46.67.1
Console (config)# wccp boomerang router-list-num 1
Console (config)# wccp version 2
```

Step 6   Proceed to the "Creating Agent (Client) Lists" section on page 2-5.

Note   In WCCP mode, to disable the boomerang process temporarily, disable WCCP on the router instead of disabling the individual Content Routers. Do so by using the **no ip wccp** command on the router.

Creating Agent (Client) Lists

Before configuring each domain, create the lists of content routing agents (also called clients) that you want to use with the domains. The agent list feature allows you reuse lists so that you do not have to re-create them each time you configure a domain. Release 1.1 allows the Content Router to support up to 200 content routing agents.

For each list of agents you want to create, do the following:

Step 1   Use the **boomerang client-list** global configuration command to enter client list configuration mode and create a list. For example, to create a list named List_A, enter the following commands:

```
Console (config)# boomerang client-list List_A
Console (config-client-lis)#
```

Step 2   Use the **client** command to assign agents to the list. For example:

```
Console (config-client-lis)# client 10.2.3.4
Console (config-client-lis)# client 10.2.5.7
Console (config-client-lis)# client 10.2.6.8
Console (config-client-lis)# client 10.2.7.9
```

Step 3   Proceed to the "Configuring Domains on the Content Router" section on page 2-6.

If you need to edit a list, use the **boomerang client-list** global configuration command to enter client list configuration mode for that list. To remove a client from a list, use the **no client** command in client list configuration mode. For example:

```
Console (config-client-lis)# no client 10.2.3.4
```

Configuring Domains on the Content Router

On the Content Router, configure each domain you want the Content Router to support.

For each domain, do the following:

Step 1   In global configuration mode, enter the **boomerang dns domain** *domain-name* command. For example, to establish support for www.foo.com, enter:

```
Console (config)# boomerang dns domain www.foo.com
```

After entering this command you are in domain configuration mode, where you will configure the specified domain.

Step 2   Use the **key** *keyword* command to establish a keyword that will be used to encrypt data sent between the Content Router and each content routing agent. For example, if you wanted to use MySecret as the keyword, enter:

```
Console (config-domain)# key MySecret
```

Note   You need to use the **key** command to enter this same keyword on each agent when you configure the agents for this domain. See the next section, "Configuring the Content Routing Agents." You can use a unique keyword for each domain.

Step 3   Use the **origin-server** *ip-address hostname* command to specify the "last chance" response server for the domain. For example, if the origin server host name is www.servername.com and located at IP address 10.10.10.5, enter:

```
Console (config-domain)# origin-server 10.10.10.5 www.servername.com
```

Note   You must use the **origin-server** command when you configure the Content Router in direct mode. In WCCP mode, if all content is supplied through push technology from the origin server to the content server, then it is not necessary to use the **origin-server** command. However, the **origin-server** command is necessary in WCCP mode if the content servers will pull the content from the origin server.

Step 4   Use the **client-group** *list-name* command to assign a list of agents to the domain. For example, to use client-list List_A:

```
Console (config-domain)# client-group List_A
```

Note   Additional command options are available for some of these commands. See the "Domain Configuration Commands" section on page B-10 of Appendix B for complete command syntax listings.

Step 5   Proceed to the next section, "Configuring the Content Routing Agents."

Configuring the Content Routing Agents

The next step is to set up each content routing agent for each domain you want the content routing agent to support. Systems, such as Content Engines, can be configured as content routing agents that interact with the Content Router. For details on how to configure a system as a content routing agent, refer to the documentation associated with that system's software. For example, to configure a Content Engine as a content routing agent, refer to the latest version of the *Cisco Cache Software Configuration Guide*.

Verifying the Content Router Configuration

Once you have configured the Content Router and the content routing agents, check to ensure that the Content Router is working properly.

Step 1   From the command-line interface (CLI) of the Content Router, enter the **show boomerang** *domain* command.

The one-way delay to the agents is shown in milliseconds. If an agent is repeatedly unreachable, the word "unknown" is displayed instead of a number.

Step 2   From a machine on a network near an agent, start a web browser and open various web pages within the configured domain. Access some pages more than once to ensure that some pages are in the cache. If the agent is a Cache Engine or Content Engine, use the **show boomerang** *domain* command on the agent. There should be a nonzero value for "Total bytes served." For example:

```
Console# show boomerang www.exampledomain.com
DNS packets with unknown domain0
HTTP hostname requests dropped0

Domain www.exampledomain.com
    Content server172.29.249.234
    Origin server172.29.249.205
    DNS A record requests4
    Dropped (server down)0
    Dropped (CPU busy)0
    Security failures0
    Cache hit bytes4713
    Cache miss bytes1571
    Total bytes served6284
```