Configuring a CSS as a Content Routing Agent

This chapter provides an overview of the CSS Content Routing Agent (CRA) feature and describes how to configure it for operation. Information in this chapter applies to all CSS models, except where noted.

This chapter provides the following sections:

Overview of the Content Routing Agent Feature

To improve a client's overall browser experience by decreasing the response times for content requests, configure a CSS as a Content Routing Agent (CRA). A Cisco Content Router 4430-B (Content Router) running software version 1.1 redirects a client to the closest (best) replicated-content site represented by a CRA, based on network delay using a software process called boomerang. For details on the Cisco Content Router software and boomerang, refer to the *Cisco Content Routing Software Configuration Guide and Command Reference*, Release 1.1.

Configure a CRA at each content site within each domain that you want to support. This configuration also requires a Content Router.

The Content Router intercepts DNS requests from a client, then routes them to a CRA. For example, to route www.foo.com, the address record (A-record) in the primary DNS server for www.foo.com is changed to a name server record (NS-record) pointing to the Content Router. The Content Router and its CRAs handle all requests for the IP address of www.foo.com. When the CRAs receive a DNS request from the Content Router, the CRAs respond to the client's local name server at the same time. The first response through the network is used and the local name server discards all other responses. The CRA with the winning response is the site to which the client connects.

Figure 3-1 shows an example of the boomerang process in direct mode. A CSS configured as a CRA also works with a Content Router operating in (WCCP) mode. For more information on Content Router modes, refer to the *Cisco Content Routing Software Configuration Guide and Command Reference*, Release 1.1.
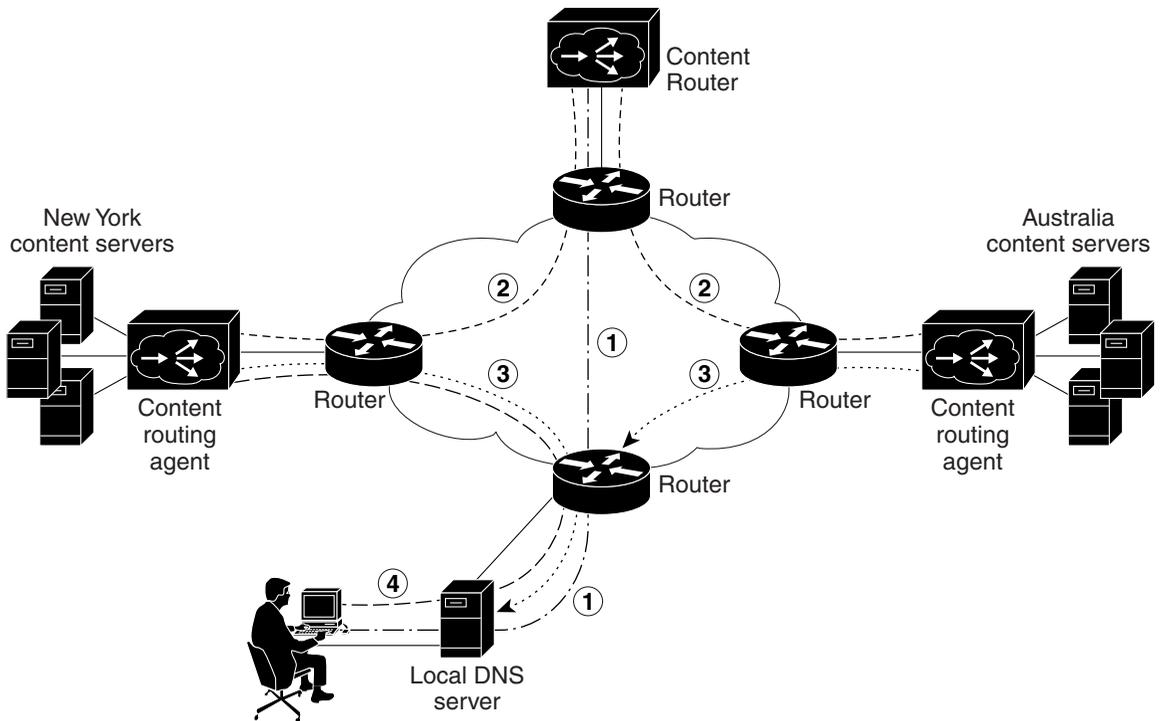
Note The Content Routing Agent feature is part of the CSS Standard feature set.

Figure 3-1   Example of Boomerang Content Routing Process - Direct Mode

1. DNS request is sent to Content Router.
2. Content Router forwards request to content routing agents.
3. Agents simultaneously send responses back to local DNS server.
   First response through the network contains the IP address of the best site.
4. User connects to best site.

46626

Content Routing Agent Quick Start

Table 3-1 provides a quick overview of the steps required to configure the Content Routing Agent feature on a CSS. Each step includes the CLI command required to complete the task. For a complete description of each feature and all the options associated with the CLI commands, refer to the following sections.

Table 3-1   Content Routing Agent Configuration Quick Start

Task and Command Example
1. Configure a Cisco Content Router 4430-B. Configure Content Routing Agents (CRAs) and the domains associated with them on the Content Router. For details, refer to the *Cisco Content Routing Software Configuration Guide and Command Reference*, Release 1.1.

2. On a CSS that you want to configure as a CRA, enter config mode.
 	
`# config`
`(config)#`

3. Enable the CRA feature on a CSS. `(config)# dns-boomerang client enable`
4. Create a domain record in the CRA for each domain with which you associated the CRA when you configured the Content Router. `(config)# dns-boomerang client domain www.sample.com 192.168.1.1`

5. Optionally, configure an alias for each configured domain to reduce administrative overhead.
 	
`(config)# dns-boomerang client domain www.sample.com alias`
`gif.www.sample.com`

6. Display CRA statistics. `(config)# show dns-boomerang client`

Configuring Content Routing Agent Parameters

The following sections describe the CLI commands and their options and variables that you use to configure the CSS as a CRA.

Enabling the Content Routing Agent

Use the **dns-boomerang client enable** command to enable the CRA functionality on the CSS. There are no options for this global configuration mode command.

For example:

```
(config)# dns-boomerang client enable
```

To disable the CRA, enter:

```
(config)# no dns-boomerang client enable
```

Configuring the CPU Load Threshold

Use the **dns-boomerang client cpu-threshold** command to set the CSS CPU load threshold for domains configured to use or return a local virtual IP address (VIP). If the CPU load exceeds the configured threshold value, then the CSS drops subsequent incoming DNS requests from the Content Router until the load is lower than the threshold.

The syntax for this global configuration mode command is:

dns-boomerang client cpu-threshold *threshold*

The variable for this command is *threshold*. Enter an integer from 1 to 99. The default is 99.

For example:

```
(config)# dns-boomerang client cpu-threshold 50
```

To reset the CSS CPU threshold to the default value, enter:

```
(config)# no dns-boomerang client cpu-threshold
```

Note   To display the CPU load, use the **show system-resources** command.

Configuring Content Routing Agent Domain Records

Use the **dns-boomerang client domain** command to create a domain record in the Content Routing Agent DNS server for each of the domains you associated the agent with when you configured domains on the Content Router. If the matching domain record keepalive messaging succeeds, the CSS uses this record for DNS resolutions. There is no Content Routing Agent configuration mode. Unlike other **dns-record** commands on the CSS, this command requires keywords for specifying options. (For details on configuring DNS domain records for other DNS applications, refer to Chapter 1, Configuring the CSS Domain Name Service, in the section "Configuring Domain Records".)

The syntax for this global configuration mode command is:

> **dns-boomerang client domain** *dns_name ip_or_host* {**"***uri***"**} {**key**
>   [**"***secret***"**|**des-encrypted** *encrypted_key*|**"***encrypt_key***"**]}
>   {**dns-ttl** *number1*} {**ip-ttl** *number2*} {**threshold** *number3*}]

The variables and options for this command are:

- *dns_name* - The domain name mapped to the client record. Enter the name as a case-sensitive, unquoted text string with no spaces and a maximum length of 72 characters. For example, www.sample.com.

- *ip_or_host* - The IP address or the host name of the content server or web cache bound to the domain name on the CSS. This IP address can be a local VIP. Enter the address in dotted-decimal notation (for example, 192.168.11.1).

- **"***uri***"** - The optional URI that the CSS uses for the keepalive probe to the Content Router for a domain. Enter a quoted text string with a maximum of 255 characters. If you do not prepend the URI with a slash (/) character, the CSS prepends it.

- **key** - The optional keyword that defines the clear-text shared RC4 secret or DES encryption key on the Content Router. See Table 3-2 for a comparison of how you configure a password on a CSS (configured as a CRA) and on a Content Router.

- "*secret*" - The optional clear-text Content Router secret for encrypting packets sent between a Content Router and a CRA. The secret you specify here must match the secret configured on the Content Router. Enter the secret as a case-sensitive quoted text string with no spaces and a maximum of 64 characters (not including the quotes). For example, if MySecret is the secret configured on the Content Router for this domain, then enter **"MySecret"**.

- **des-encrypted** - The optional keyword that specifies that a Data Encryption Standard (DES)-encrypted password follows.

- *encrypted_key* - The DES encryption key that the CSS had previously encrypted. The CSS does not re-encrypt this key and saves it in the running-config as you entered it. Enter an unquoted case-sensitive text string with no spaces and a maximum of 64 characters.

- "*encrypt_key*" - The DES encryption key that you want the CSS to encrypt. The CSS saves the encrypted key in the running-config as you entered it. Enter a quoted case-sensitive text string with no spaces and a maximum of 16 characters.

Table 3-2   Configuring a Password on a CSS (CRA) Versus a Content Router

CSS Password Command	Content Router Password Command
key "*secret*"	no equivalent
key des-encrypt "*password*"	**key** *word* or **key 0** *word*
key des-encrypt *password*	**key 7** *word*

Note   The DES encryption algorithm on the CSS is different from the Cisco Type 7 encryption algorithm on the Content Router. Therefore, encrypted passwords are displayed differently on the CSS and on the CR.

- **dns-ttl** *number* - The optional DNS time-to-live keyword and value in seconds returned in the CRA's DNS responses. This option determines the length of time a DNS server caches the returned information for reuse. Enter an integer from 1 to 2147483647 seconds. The default is the dns-ttl value configured on the Content Router.

- **ip-ttl** *number* - The optional IP routing time-to-live keyword and value in router hops returned in the CRA's DNS responses. This option determines how many router hops a response packet traverses enroute to the D-Proxy before it is discarded. This helps to eliminate the CRA from longer response routes. Enter an integer from 1 to 255. The default is the ip-ttl value configured on the Content Router.

- **threshold** *number* - The optional load threshold for testing the keepalive state of a local VIP. If the load on the dns-record associated with the content rule is greater than the threshold value, then the CSS drops subsequent Content Router requests for that record until the load is lower than the threshold. Enter an integer from 2 to 254. The default value is 254.

> **Note**   You must also configure the **add dns** command in the VIP's content rule to add domain names. Refer to the *Cisco Content Services Switch Basic Configuration Guide*, Chapter 3, Configuring Content Rules, in the section "Adding a Domain Name System to a Content Rule".

For example:

```
(config)# dns-boomerang client domain www.foo.com 192.168.11.1 key
"MySecret" dns-ttl 240 ip-ttl 5 threshold 175
```

To remove a CRA domain, enter:

```
(config)# no dns-boomerang client domain www.foo.com
```

Configuring an Alias for an Existing Client Domain

Use the **dns-boomerang client domain alias** command to create an alias for an existing client domain. The alias behaves exactly the same as the configured domain name. This command reduces administrative overhead by allowing you to use the shorter alias name instead of the domain name, IP address, and all the other options and variables for the configured record. The syntax for this global configuration mode command is:

dns-boomerang client domain *dns_name* **alias** *alias_name*

The variables and options are:

- *dns_name* - The domain name of a configured client record. Enter the name as a case-sensitive, unquoted text string with no spaces and a maximum of 72 characters.

- **alias** - The keyword required to create an alias name.

- *alias_name* - The domain name that the CSS treats exactly the same as the associated *dns_name*. Enter the name as a case-sensitive, unquoted text string with no spaces and a maximum of 72 characters.

For example:

```
(config)# dns-boomerang client domain www.sample.com alias
gif.www.sample.com
```

To remove the alias, enter:

```
(config)# no dns-boomerang client domain alias www.sample.com
```

Clearing Domain Statistics

Use the **dns-boomerang client zero** command to clear the statistics for one or all configured domains. If you do not specify a domain name, the CSS clears the statistics for all configured domains. This command is available in SuperUser and all configuration modes.

The syntax for this global configuration mode command is:

dns-boomerang client zero *dns-name*

The variable for this command is *dns_name*, the domain name mapped to the client record statistics that you want to clear. Enter the name as a case-sensitive, unquoted text string with no spaces and a maximum of 72 characters.

For example:

```
(config)# dns-boomerang client zero www.sample.com
```

Displaying Content Routing Agent Statistics

Use the **show dns-boomerang client** command to display information for all configured domains. This command is available in SuperUser and all configuration modes.

The syntax for this global configuration mode command is:

show dns-boomerang client {**all**|**global**|**domain** {*domain_name*}}

The options and variable for this global configuration mode command are:

- **all** - Displays all information (global and domain-related) for all domains mapped to a client record. Same as the **show dns-boomerang client command**.

- **global** - Displays global information only for all domains mapped to a client record.

- **domain** - Displays domain-related information for all domains mapped to a client record.

- *domain_name* - Displays domain-related information for the specified domain.

For example:

```
(config)# show dns-boomerang client global
```

Table 3-3 describes the fields in the **show dns-boomerang client** output.

Table 3-3   Field Descriptions for the show dns-boomerang client Command

Field	Description
Total DNS A-record requests	The total number of address record requests from the Content Server.
Total packets dropped	
Unknown domain	The number of DNS packets with domains not configured on this CSS (for Content Routing).
Invalid source address	The number of packets with invalid source addresses.

*Table 3-3   Field Descriptions for the show dns-boomerang
client Command (continued)*

Field	Description
Excess length	The number of packets that had lengths longer than what the CR could send.
CPU threshold exceeded	The number of packets dropped because the CPU threshold was exceeded.
Configured CPU threshold	The configured threshold value above which the CSS drops requests from the Content Router.
Rule load threshold exceeded	The number of requests from the Content Router that were dropped because the load on a local rule exceeded the configured threshold.
Keepalive state Down	The number of packets dropped because the keepalive failed.
Security failure	The number of requests for this domain that were dropped due to security errors (key/secret failure or mismatch).
Domain	The DNS name mapped to the client record.
Content server	The address of the content server bound to the domain.
Origin server	The address for the most recently used origin server that was passed from the Content Router.
Bad probes	The number of times (in percent) that the keepalive message failed to find the service Up.
DNS A-record requests	The number of DNS address record requests for this domain from the Content Router.
Dropped (server down)	The number of requests for this domain that were dropped because the server was down.
Dropped (CPU busy)	The number of requests for this domain that were dropped because the CPU threshold was exceeded.
Dropped (rule load exceeded)	The number of requests from the Content Router that were dropped because the load on a local rule exceeded the configured threshold.

Table 3-3   Field Descriptions for the show dns-boomerang
client Command (continued)

Field	Description
Configured threshold	The load threshold value you configured with the **dns-boomerang client domain** command to test the keepalive state of a local VIP.
Security failures	The number of requests for this domain that were dropped due to security errors (key/secret failure or mismatch).
Alias	The alias that maps to the configured domain name.
DNS A-record requests	The number of DNS address record requests for this alias from the Content Router.