Configuring WCCP

The following sections describe the Web Cache Communication Protocol (WCCP) feature for Cisco Enterprise Content Delivery System (ECDS):

- Configuring WCCP General Settings, page 7-1
- Configuring WCCP Services, page 7-3
- Managing WCCP Router Lists, page 7-12
- Managing WCCP Port Lists, page 7-15
- Configuring WCCP Transparent Routing Bypass Settings, page 7-18
- Creating WCCP Bypass List Entries, page 7-19
- Configuring HTTP IP Spoofing with WCCP, page 7-19
- WCCP Interception for Live Streaming, page 7-21
- Basic WCCP CLI Configuration Examples, page 7-31
- Where to Go Next, page 7-40

Configuring WCCP General Settings

To use WCCP, the Service Engine must be properly configured. To use a WCCP-enabled router, an IP address must be configured on the router interface that is connected to the Internet, and this interface must be visible to the Service Engine on the network.

To configure WCCP general settings:

Step 1 Log into the ECDS administration GUI.
Step 2 Choose Devices > Devices. A list of devices is displayed.
Step 3 Click the Edit icon next to the Service Engine for which you want to configure WCCP service settings. The Device Home for Service Engine window displays.
Step 4 Choose Request Routing > WCCP > General Settings. The WCCP Configuration Settings window displays (Figure 7-1). Table 7-1 describes the fields and provides CLI information.
Step 5 Enable WCCP Version 2 by choosing 2 from the WCCP Version menu. Only WCCP Version 2 is supported with Cisco ECDS.
Step 6 To keep the TCP flow intact, and to avoid overwhelming Service Engines when they come up or are reassigned new traffic, check the Enable Flow Redirection check box. This feature also has a slow start mechanism which enables a Service Engine to manage an amount of data that is appropriate for its capacity (see Step 7).

Use the `wccp flow-redirect enable` command.

Step 7 To enable the slow start capability on the Service Engine, check the Slow Start check box. For more information about the WCCP Slow Start feature, see the “Slow Start” section on page 2-33.

Use the `wccp slow-start enable` command.
Configuring WCCP Services

See the following sections:
- Configuring WCCP Service Settings, page 7-3
- Managing WCCP Service Masks, page 7-9
- Managing WCCP Router Lists, page 7-12
- Managing WCCP Port Lists, page 7-15

Configuring WCCP Service Settings

To configure WCCP service settings for the Service Engine:

Step 1  Choose Request Routing > WCCP > Services. The WCCP Service Settings for Service Engine window appears (Figure 7-2).

Note  The Service Engine settings or its associated device group settings will be applied to this window depending on the choice that you have made in the WCCP General Settings window.

Figure 7-2  WCCP Service Settings
Step 2  To edit an existing service, click a service icon in the Service section. The Modifying page for that service is displayed. Figure 7-3 shows an example of the Custom WebCache service page.

Figure 7-3  Modifying WCCP Service Window

Step 3  Manage the following services from the WCCP Service Settings for Service Engine page:

- Creating New WCCP Service, page 7-4
- Configuring WCCP Services, page 7-5
- Configuring Dynamic Service Settings, page 7-6
- Configuring Load Balancing Hash, page 7-6
- Configuring Other Settings, page 7-7
- See also Enabling WCCP on the Router.

Creating New WCCP Service

To create new WCCP service:

Step 1  Click the Create New WCCP Service Setting icon in the taskbar. The Creating New WCCP Service window appears.

Step 2  Configure a maximum of seventeen services. If seventeen services have already been defined, the Create New WCCP Service Settings icon is not visible in the taskbar.

Note  Settings for a particular WCCP service can be configured only after the WCCP service has been associated with a router list. See the “Creating WCCP Router Lists” section on page 7-12.

Step 3  Proceed to Configuring WCCP Services.
Configuring WCCP Services

In the WCCP Service section:

**Step 1** Choose the type of WCCP service from the Service Type drop-down list. (See Table 7-2 for a description of the service types.)

**Table 7-2  WCCP Service Types**

<table>
<thead>
<tr>
<th>Service Type</th>
<th>Service Group Number</th>
<th>Description of Services</th>
<th>CLI Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>WebCache</td>
<td>0</td>
<td>Enables web cache service with WCCP Version 2. With web cache service, the router balances the traffic load within a Service Engine cluster based on the destination IP address (for example, web server IP address).</td>
<td>wccp web-cache</td>
</tr>
<tr>
<td>HTTPS</td>
<td>70</td>
<td>Enables WCCP flow redirection to a Service Engine configured as an HTTPS server.</td>
<td>wccp https</td>
</tr>
<tr>
<td>RTSP</td>
<td>80</td>
<td>Configures WCCP Version 2 Real-Time Streaming Protocol (RTSP) transparent interception.</td>
<td>wccp rtsp</td>
</tr>
<tr>
<td>Windows Media</td>
<td>81-82</td>
<td>Enables WCCP Version 2 Windows Media caching service.</td>
<td>wccp wmt</td>
</tr>
<tr>
<td>Windows Media RTSP</td>
<td>83</td>
<td>Enables Windows Media RTSP (port 5005) transparent interception.</td>
<td>wccp wmt-rtsp</td>
</tr>
<tr>
<td>RTMP</td>
<td>84</td>
<td>Managed domains.</td>
<td>wccp rtmp</td>
</tr>
<tr>
<td>Custom WebCache</td>
<td>98</td>
<td>Enables the Service Engine to accept redirected HTTP traffic on a port other than 80.</td>
<td>wccp custom-web-cache</td>
</tr>
<tr>
<td>Dynamic Service Number</td>
<td>90-97</td>
<td>Enables up to eight dynamic WCCP redirection services on the Service Engine.</td>
<td>wccp service-number</td>
</tr>
</tbody>
</table>

**Note** Direct video playback of wmv and flv files from HTTPS server using WCCP HTTPS is not supported. The content has to be downloaded to the local hard disk from the HTTPS Server and then to be played using video applications such as Windows Media Player and Flash Media Streaming player, respectively.

**Step 2** Associate a router list with the WCCP service by choosing one from the Router List drop-down list.

**Tip** Only configured router lists are displayed in the drop-down list.

See the following sections for more information about router lists:
- Creating WCCP Router Lists, page 7-12
- Modifying WCCP Router Lists, page 7-13
- Viewing WCCP Router Lists, page 7-14

**Step 3** Proceed to Configuring Dynamic Service Settings, page 7-6
Configuring Dynamic Service Settings

In the Dynamic Service Settings section:

**Step 1** To associate ports with specific WCCP Version 2 dynamic services, choose the port list number from the Port List drop-down menu. Figure 7-4 shows the Dynamic Service Settings section of the Creating New WCCP Service page.

*Figure 7-4 Dynamic Service Settings*

<table>
<thead>
<tr>
<th>Dynamic Service Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port List:</td>
</tr>
<tr>
<td>Application: cache</td>
</tr>
<tr>
<td>Match Source Port:</td>
</tr>
</tbody>
</table>

All configured port lists are displayed here. You can only associate ports with user-configurable web cache services 90–97. For all other services, the Port List drop-down menu is disabled.

**Tip** To configure a port list for WCCP Version 2 dynamic services or if no port list already exists, see the “Configuring WCCP Port Lists” section on page 7-15.

**Step 2** From the Application drop-down list, choose the application running on the Service Engine to which intercepted traffic must be redirected. Table 7-3 describes the available options.

*Table 7-3 Application Redirect Options*

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cache</td>
<td>Redirects traffic to the caching application running on the Service Engine.</td>
</tr>
<tr>
<td>https-cache</td>
<td>Redirects traffic to the HTTPS caching application running on the Service Engine.</td>
</tr>
<tr>
<td>streaming</td>
<td>Redirects traffic to the streaming media application running on the Service Engine.</td>
</tr>
</tbody>
</table>

**Step 3** To match the source port for traffic redirection, select the Match Source Port check box.

**Step 4** Proceed to Configuring Load Balancing Hash.

Configuring Load Balancing Hash

In the Load Balancing Hash section:

**Step 1** To define the destination IP address load-balancing hash, check the Destination IP check box. Use the `wccp web-cache router-list-num 1 hash-destination-ip` command.

*Figure 7-5* shows the Load Balancing Hash section of the Creating New WCCP Service page.
Figure 7-5 Load Balancing Hash Settings

### Load Balancing Hash

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination IP:</td>
<td>Source IP:</td>
</tr>
<tr>
<td>Destination Port:</td>
<td>Source Port:</td>
</tr>
</tbody>
</table>

**Step 2** To define the source IP address load-balancing hash, select the **Source IP** check box. This method is the default hash assignment for HTTPS cache service.

Use the `wccp web-cache router-list-num 1 hash-source-ip` command.

**Step 3** To define destination port load-balancing hash, select the **Destination Port** check box.

Use the `wccp web-cache router-list-num 1 hash-destination-port` command.

**Step 4** To define the source port load-balancing hash, select the **Source Port** check box.

Use the `wccp web-cache router-list-num 1 hash-source-port` command.

**Tip** For most WCCP services, the destination IP is used for the default hashing target. For HTTPS service, the source IP is used for the default hashing target.

**Step 5** Proceed to Configuring Other Settings.

**Tip** For command examples, see the “Load Balancing Command Examples” section on page 7-33.

### Configuring Other Settings

In the Other Settings section:

**Step 1** To force WCCP to use the configured assignment method only, select the **Use Selected Assignment Method** check box. This setting can be configured only for HTTPS cache, custom web cache, web cache, and Windows Media services. When applied, both hash and mask assignment load balancing methods can be used.

*Figure 7-6 shows the Other Settings section of the Creating New WCCP Service page.*
Step 2  To rewrite the packet Layer 2 MAC addresses to forward packets to the Service Engine, select the Layer2 Redirection check box.

Use the `wccp web-cache router-list-num 1 l2-redirect` command.

If negotiation fails using this method, negotiation uses the default GRE method instead.

Step 3  To rewrite the packet Layer 2 MAC addresses to return packets to the switch, select the Packet return by Layer 2 rewrite check box.

Use the `wccp web-cache router-list-num 1 l2-return` command.

If negotiation fails using this method, negotiation uses the default GRE method instead.

Step 4  In the Password field, specify the password to be used for secure traffic between the Service Engines within a cluster and the router for a specified service. Be sure to enable all other Service Engines and routers within the cluster with the same password.

Use the `wccp web-cache router-list-num 1 password` command.

Tip  Passwords must not exceed 8 characters in length.

Step 5  Reenter the password in the Confirm Password field.

Step 6  In the Assignment Weight field, specify the weight parameter that represents a percentage of the total load redirected to the Service Engine (for example, a Service Engine with a weight of 30 receives 30 percent of the total load). If the total of all weight parameters in a Service Engine cluster exceeds 100, the percentage load for each Service Engine is recalculated as the percentage that its weight parameter represents of the combined total.

Use the `wccp web-cache router-list-num 1 weight` command.

Step 7  In the Port field, specify the port number other than port 80 that will accept redirected HTTP traffic (configurable only for custom web cache service).

Step 8  To use the mask method for Service Engine assignment instead of the hash method, check the Use Mask Assignment check box. If negotiation fails, negotiation uses the hash method, which is the default.

Use the following commands:

- `wccp web-cache router-list-num 1 mask-assign`—If mask negotiation fails, negotiation uses the hash method, which is the default.
Chapter 7  Configuring WCCP

Configuring WCCP Services

- **wccp web-cache router-list-num 1 mask-assign assign-method-strict**—Mask assignment only. Use `assign-method-strict` to establish WCCP service exclusively. If negotiation fails or the router does not support WCCP, no WCCP service is created. If `mask-assign` and `assign-method-strict` both appear in the command, the result will be either mask assignment or no WCCP service.

- **wccp web-cache router-list-num 1 assign-method-strict**—Hash assignment only. Use `assign-method-strict` to establish WCCP service exclusively. If negotiation fails, no WCCP service is created. If only `assign-method-strict` appears in the command, the result will be hash assignment only or no WCCP service.

**Step 9** Click **Submit** to save the settings on the WCCP Service page.

- To create a new WCCP service mask, click the **Create Mask** button. For more information about creating service masks, see the “Configuring WCCP Service Masks” section on page 7-9.

- To modify or delete a configured service mask, click the **Edit Mask** button. For more information about modifying service masks, see the “Modifying WCCP Service Masks” section on page 7-10.

- To view all configured service masks, click the **View Masks Configured for All Services** button. For more information about viewing service masks, see the “Viewing WCCP Service Masks” section on page 7-11.

---

Managing WCCP Service Masks

Use the information in this section to manage WCCP service masks:

- Configuring WCCP Service Masks, page 7-9
- Modifying WCCP Service Masks, page 7-10
- Viewing WCCP Service Masks, page 7-11
- Deleting a WCCP Service Mask, page 7-11

Configuring WCCP Service Masks

Bit masks are specified as hexadecimal numbers. All the specified bit masks together cannot have more than 7 bits set. For example, a correct way of using three masks is OxF (4 bits), Ox1 (1 bit), and Ox3 (2 bits) for a total of 7 bits. In this case, you cannot configure any additional mask other than 0x0. Otherwise, an error message is displayed.

An example of using four masks could be 0xA (2 bits), 0x7 (3 bits), 0x8 (1 bit), 0x1 (1 bit) for a total of 7 bits. You can configure up to 16 WCCP service masks.

To configure WCCP service masks on the Service Engine:

**Step 1** Choose **Devices > Devices**. The Devices window appears, listing all the device types configured in the network.

**Step 2** Click the **Edit** icon next to the Service Engine for which you want to configure WCCP service masks. The Device Home for Service Engine window appears.

**Step 3** To display the entire table of contents, click the **Show All** button above the Contents pane.

**Step 4** In the Contents pane, choose **Request Routing > WCCP > Services**. The WCCP Service Settings for Service Engine window appears.
Step 5  Click the Create New WCCP Service Setting icon in the taskbar to configure router lists for a new service. The Creating New WCCP Service window appears.

Step 6  Alternatively, click the Edit WCCP Service Setting icon next to an existing WCCP service for which you want to configure router lists. The Modifying WCCP Service window appears.

Step 7  Under the WCCP Service section, choose a WCCP service from the Service Type drop-down list.

Step 8  Under the Other Settings section, click the Create Mask button next to the Use Mask Assignment check box to configure a service mask and associate it with a WCCP Version 2 service. The Creating New WCCP Service Mask window appears.

Step 9  Choose the type of WCCP service from the Service Type drop-down list. Table 7-2 describes these service types.

Step 10  In the Source IP Mask field, specify the IP address mask defined by a hexadecimal number (for example, 0xFE000000) used to match the packet source IP address. The range is 0x00000000–0xFE000000. The default is 0x00000000.

Step 11  In the Source Port Mask field, specify the port mask defined by a hexadecimal number (for example, 0xFE00) used to match the packet source port number. The port mask range is 0x00–0xFE. The default is 0x0.

Step 12  In the Destination IP Mask field, specify the IP address mask defined by a hexadecimal number (for example, 0xFE000000) used to match the packet destination IP address. The range is 0x00000000–0XFE000000. The default is 0x00001741.

Step 13  In the Destination Port Mask field, specify the port mask defined by a hexadecimal number (for example, 0xFE00) used to match the packet destination port number. The port mask range is 0x00–0xFE. The default is 0x0.

Step 14  To save the settings, click Submit. The Creating New WCCP Service window or the Modifying WCCP Service window appears, depending on the window from which you navigated.

---

Modifying WCCP Service Masks

To modify a WCCP service mask on the Service Engine:

Step 1  Choose Devices > Devices. The Devices window appears, listing all the device types configured in the ECDS network.

Step 2  Click the Edit icon next to the Service Engine for which you want to configure WCCP service masks. The Device Home for Service Engine window appears.

Step 3  To display the entire table of contents, click the Show All button above the Contents pane.

Step 4  In the Contents pane, choose Request Routing > WCCP > Services. The WCCP Service Settings for Service Engine window appears.

Step 5  Click the Create New WCCP Service Setting icon in the taskbar to configure router lists for a new service. The Creating New WCCP Service window appears.

Alternatively, click the Edit WCCP Service Setting icon next to an existing WCCP service for which you want to configure router lists. The Modifying WCCP Service window appears.

Step 6  Under the WCCP Service section, choose a WCCP service from the Service Type drop-down list.

Step 7  Under the Other Settings section, click the Edit Mask button next to the Use Mask Assignment check box to modify a service mask and associate it with a WCCP Version 2 service. The Modifying WCCP Service Mask window appears.
Step 8  The Edit Mask button toggles with the Create Mask button if a service mask has already been configured for a WCCP service.

Step 9  Choose the type of WCCP service from the Service Type drop-down list. See Table 7-2 for a description of the service types.

Step 10  In the Source IP Mask field, specify the IP address mask defined by a hexadecimal number (for example, 0xFE000000) used to match the packet source IP address. The range is 0x00000000–0xFE000000. The default is 0x00000000.

Step 11  In the Source Port Mask field, specify the port mask defined by a hexadecimal number (for example, 0xFE00) used to match the packet source port number. The port mask range is 0x00–0xFE. The default is 0x0.

Step 12  In the Destination IP Mask field, specify the IP address mask defined by a hexadecimal number (for example, 0xFE000000) used to match the packet destination IP address. The range is 0x00000000–0xFE000000. The default is 0x00001741.

Step 13  In the Destination Port Mask field, specify the port mask defined by a hexadecimal number (for example, 0xFC00) used to match the packet destination port number. The port mask range is 0x0–0xFE. The default is 0x0.

Step 14  To save the settings, click Submit. The Creating New WCCP Service window or the Modifying WCCP Service window appears depending on the window from which you navigated.

---

**Viewing WCCP Service Masks**

To view all masks configured for a WCCP service:

Step 1  From the Creating New WCCP Service window or Modifying WCCP Service window, click the View Masks Configured for All Services button to view all configured service masks for WCCP services. The WCCP Service Mask Settings for Service Engine window appears. A list of all services for which masks have been configured to match the packet source IP address, source port number, destination IP address, or destination port number are displayed.

Step 2  To return to the Creating New WCCP Service or Modifying WCCP Service window, click the Back (left arrow) icon in the taskbar.

Step 3  To configure a new service mask, click the Create New WCCP Service Mask Setting icon in the taskbar. The Creating New WCCP Service Mask window appears. Alternatively, click the Edit WCCP Service Mask Setting icon next to an existing WCCP service mask for which you want to change the mask settings. The Modifying WCCP Service Mask window appears.

---

**Deleting a WCCP Service Mask**

To delete a service mask on the Service Engine:

Step 1  From the WCCP Service Mask Settings for Service Engine window, click the Edit WCCP Service Mask Setting icon next to an existing WCCP service mask for which you want to change the mask settings. The Modifying WCCP Service Mask window appears.
Configuring WCCP Services

Chapter 7 Configuring WCCP

Configuring WCCP Services

Step 2 Click the **Delete WCCP Service Mask** icon in the taskbar. The system displays a dialog box asking you to confirm whether you want to permanently delete the service mask configuration.

Step 3 Click **OK** to confirm. The WCCP Service Mask Settings for Service Engine window appears.

Managing WCCP Router Lists

Use the information in this section to manage router lists while configuring WCCP services in **Devices > Request Routing > WCCP > Services**. See “Configuring WCCP Services” section on page 7-5 for more information.

- Creating WCCP Router Lists, page 7-12
- Modifying WCCP Router Lists, page 7-13
- Viewing WCCP Router Lists, page 7-14

Creating WCCP Router Lists

You can create up to 8 different router lists with up to 32 IP addresses per list for use with WCCP Version 2 services. A router list must be contain at least one IP address.

To create WCCP router lists:

Step 1 Choose **Request Routing > WCCP > Services**.

Step 2 Click the **New Router List** button. The Creating New WCCP Router window appears (Figure 7-7).

![Figure 7-7 WCCP New Router List](image)

Step 3 In the Router IP Address field, specify the IP address of the router to be added to the list.

**Tip** You must enter at least one IP address and all IP addresses added must be unique within the router list.
Step 4 To add an IP address to the list, click **Add Router**. This list represents the IP address of every router that will redirect traffic to this Service Engine for a particular service. If different routers will be used for different services, you must create more than one router list.

The window refreshes and the addresses are listed in numerical order. The order might not match the order in which IP addresses were entered. IP addresses will be displayed in red until settings are saved.

Step 5 To save the router list or to save any edits you have made to the router IP addresses, click **Submit**. You will be returned to the WCCP Service window.

---

**Modifying WCCP Router Lists**

To add or delete an IP address from a router list or to delete a router list:

**Step 1** From the Creating New WCCP Service window or Modifying WCCP Service window, choose the router list number from the List Number drop-down list.

**Step 2** Click the **Edit Router List** button. The Modifying WCCP Router List window appears (Figure 7-8).

*Figure 7-8  Modifying a WCCP Router List*

**Step 3** To add a router to the router list, enter the router’s IP address in the Router IP Address field, and click the **Add Router** button.

**Step 4** To remove a router from the router list, select the check box next to the router in the list and click the **Remove Router** button.

**Step 5** To modify the router IP address, click the **Edit IP Address** icon next to the IP address that you want to modify (Figure 7-9).
Figure 7-9   Edit Router List

Step 6   The IP address will be displayed in the Router IP Address field. Once you have changed the IP address, click the Edit button to add the modified IP address to the list. The window refreshes itself, and the changed IP address will be displayed in purple until settings are saved.

Tip   The Edit button next to the Router IP Address field is displayed as Add Router to allow you to add any new IP address to the list. The Edit button toggles with the Add Router button.

Step 7   To save the settings, click Submit. The window refreshes itself, and the settings are saved.

Step 8   To delete a router list, follow these steps:

a. From the Modifying WCCP Router window, click the trash can icon (Delete WCCP Router List) in the taskbar. The system displays a dialog box asking you to confirm that you want to permanently delete the router list configuration.

Note   When you delete a router list, the WCCP Version 2 services that have been configured to use this router list are also deleted. Make sure that the WCCP service is associated with a different router list, if required, before deleting the previously configured router list.

b. Click OK to confirm. The selected router list and the services with which it is associated are deleted.

Viewing WCCP Router Lists

To view all router lists configured for a WCCP Version 2 dynamic service:

Step 1   To view all configured router lists for WCCP Version 2, click the View All Router List button from the Creating New WCCP Service window or the Modifying WCCP Service window. The WCCP Router List Configurations for Service Engine window appears.

The List Number column displays all configured router list numbers. The Router IP Addresses column displays a list of IP addresses that were added to the router list. From this window you can perform the following actions:
Managing WCCP Port Lists

Use the information in this section to manage WCCP port lists:

- Configuring WCCP Port Lists, page 7-15
- Modifying WCCP Port Lists, page 7-17

Configuring WCCP Port Lists

With eight custom services that use a maximum number of eight ports each, the maximum number of ports that can be specified for transparent redirection is 64.

The legacy custom web cache services (service number 98) can be configured with only one port. If only one legacy service is configured, the total maximum number of transparent redirection ports is 57. If both legacy services are configured, the maximum port total is 50.

All ports receiving HTTP that are configured as members of the same WCCP service share the following characteristics:

- They have the same hash or mask parameters as configured using the Creating New WCCP Service window.
- The service on individual ports cannot be stopped or started individually (WCCP Version 2 restriction).

With Service Engines in a farm, the following restrictions apply:

- All Service Engines that use the same WCCP service are required to configure the same list of ports and the same hash or mask parameters.
- A Service Engine that tries to join the farm with the same WCCP service using a different list of ports or different hash or mask parameters is rejected by the router.
- To change the port list for a particular WCCP service, WCCP service must be stopped on all involved Service Engines, and then all must be restarted with the new parameters.

Procedure

To configure WCCP ports:
Step 1 Choose **Devices > Devices**. The Devices window appears, listing all the device types configured in the network.

Step 2 Click the **Edit** icon next to the Service Engine for which you want to configure WCCP port lists. The Device Home for Service Engine window appears.

Step 3 To display the entire table of contents, click the **Show All** button above the Contents pane.

Step 4 In the Contents pane, choose **Request Routing > WCCP > Services**. The WCCP Service Settings for Service Engine window appears.

Step 5 Click the **Create New WCCP Service Setting** icon in the taskbar to configure router lists for a new service. The Creating New WCCP Service window appears.

Step 6 Alternatively, click the **Edit WCCP Service Setting** icon next to an existing WCCP service for which you want to configure router lists. The Modifying WCCP Service window appears.

Step 7 In the WCCP Service section, choose a WCCP dynamic redirection service from the Service Type drop-down list.

Step 8 In the Dynamic Service Settings section, click the **New Port List** button to configure a port list number to associate ports for a WCCP Version 2 dynamic service (*Figure 7-10*).

*Figure 7-10* **New Port List Button**

<table>
<thead>
<tr>
<th>Dynamic Service Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port List:</td>
</tr>
<tr>
<td>Application: cache</td>
</tr>
<tr>
<td>Match Source Port:</td>
</tr>
</tbody>
</table>

The WCCP Port List Settings window appears (*Figure 7-11*).

*Figure 7-11* **WCCP Port List Settings**

<table>
<thead>
<tr>
<th>WCCP Port List Settings</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>List Number</td>
<td>Ports</td>
</tr>
<tr>
<td>1</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td></td>
</tr>
</tbody>
</table>

**Note** *- Required Field*
Step 9 Under the Ports column and against a port list number, specify the port number to be added to the list. You can configure a maximum of 8 port numbers per list.

Each port number added must be unique among all configured port lists. Otherwise, an error message is displayed on submit.

For a port list, port numbers need not necessarily be entered in successive fields under the Ports column. Blank fields in between will be removed on submit and all added port numbers will be reordered and displayed in ascending order when you visit the window the next time.

Step 10 Click Submit to save the settings. The Creating New WCCP Service window or Modifying WCCP Service window appears depending where you began.

---

Modifying WCCP Port Lists

To modify a port list:

Step 1 From the Creating New WCCP Service window or Modifying WCCP Service window, click the Edit Port List button to configure a port list for WCCP Version 2 dynamic services. The WCCP Port List Settings window appears.

Step 2 To modify port numbers in the port list:
   a. Choose a port list number and edit any of the port numbers that you wish to change in the Ports column for that row.
   b. Click Submit to save the settings. The Creating New WCCP Service window or Modifying WCCP Service window appears depending on the window from which you traversed.

Step 3 To delete a port list:
   a. Check the Clear List check box next to the port list that you want to delete. All added port numbers will be removed from the port list.
   b. Click Submit to save the settings. The Creating New WCCP Service window or Modifying WCCP Service window appears depending on the window from which you traversed.

To configure dynamic service on the port list, enter the following commands:

```config
SE(config)# wccp port-list 1 5566
SE(config)# wccp service-number 91 router-list-num 1 port-list-num 1 application cache
```

This command example configures port 5566 on port list #1. At the same time dynamic service with service number 91 is created using preconfigured router-list-num 1 and using the cache application.

The following application types are supported:

- **cache**: Redirects incoming traffic to port 80—Standard port for the HTTP server.
- **https-cache**: Redirects incoming traffic to port 443—Standard port for the HTTPS server.
- **streaming**: Redirects incoming traffic to port 554—Standard port for the RTSP server.
Configuring WCCP Transparent Routing Bypass Settings

To configure WCCP bypass settings.

**Step 1** Choose Request Routing > WCCP > Bypass. The WCCP Bypass Settings window appears (Figure 7-12).

**Figure 7-12 Configuring WCCP Bypass Settings**

<table>
<thead>
<tr>
<th>WCCP Bypass Settings for Service Engine, query</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current applied settings from Service Engine:</td>
</tr>
<tr>
<td>Bypass Enable</td>
</tr>
<tr>
<td>Load Bypass Enable</td>
</tr>
<tr>
<td>Minimum interval between putting system to bypass mode</td>
</tr>
<tr>
<td>Time will last when system put into bypass mode</td>
</tr>
<tr>
<td>Time interval for polling system back from bypass</td>
</tr>
</tbody>
</table>

**Step 2** To enable the Service Engine to bypass incoming requests from clients, select the Bypass Enable check box.

**Note** Some websites may not allow the Service Engine to connect directly on behalf of the client. To avoid a disruption of service when traffic is bypassed, the Service Engine can use authentication bypass to generate a dynamic access list for these client/server pairs. Authentication bypass triggers are also propagated upstream and downstream in an ECDS network environment.

**Step 3** Select the Load Bypass Enable check box to enable traffic bypass.

Use the `bypass load enable` command.

**Step 4** In the Minimum interval between putting system to bypass mode field, enter a number of seconds between 4 and 600.

Use the `bypass load time-interval` command.

**Step 5** In the Time will last when system put into bypass mode field, enter a number of minutes between 1 and 1440.

**Step 6** In the Time interval for polling system back from bypass field, enter a number of seconds between 2 and 600.

**Step 7** Click Submit to save the settings.
Creating WCCP Bypass List Entries

To create WCCP bypass list entries:

**Step 1**  Choose Devices > Devices > Request Routing > WCCP > Bypass List.

**Step 2**  Click the Create New WCCP Bypass List icon. The Creating new WCCP Bypass List window appears (Figure 7-13).

**Step 3**  Enter the IP address for the client in the Client Address field.

**Step 4**  Enter the IP address for the server in the Server Address field.

**Step 5**  Check Submit to save the settings.

Use the following commands:

- To create a WCCP bypass list:
  ```
  bypass static {clientip [serverip | any-server] | any-client serverip}
  ```

- To bypass all except a specific server on a specific port:
  ```
  bypass static port 80 except-server 1.1.1.1
  ```

The system bypasses all the traffic to this port, except the traffic that has a destination IP on the configured list.

Tip  Each Service Engine can have up to 50 bypass list entries.

---

Configuring HTTP IP Spoofing with WCCP

Note  You must configure WCCP before you can enable IP Spoofing. Disable the IP Spoofing feature by unchecking the Enable IP Spoofing check box in the ECDS GUI before configuring WCCP. See the “Configuring WCCP General Settings” section on page 7-1 to enable WCCP.

When configured for IP spoofing, the Service Engine connects to the origin server using the client IP address instead of its own IP address.

IP Spoofing does not support the following:

- Non-HTTP protocols
To configure IP Spoofing on WCCP-enabled system:

**Step 1** Choose **Devices > Devices > Application Control > Web > HTTP > HTTP Connections**.

**Step 2** Select the Enable IP Spoofing check box (Figure 7-14).

**Step 3** Click **Submit** to save the settings.

### IP Spoofing Commands

To configure IP Spoofing on a service group with a single router and a single Service Engine:

1. Two WCCP services need to be configured on the Service Engine:
   a. Configure WCCP HTTP redirection.
      
      ```
      wccp web-cache router-list-num [number]
      ```
   
   b. Configure WCCP dynamic service.
      
      ```
      wccp service-number [number] router-list-num [number] port-list-num [number] application cache match-source-port
      ```

2. Two WCCP services need to be configured on the Router:
   
   ```
   ip wccp web-cache
   ip wccp [91]
   ```

3. Two interface interception and redirection instances need to be configured on the Router:
   a. Enter the following on the interface to the Origin Server:
      
      ```
      ip wccp web-cache redirect out
      ```
   b. Enter the following on the interface to Origin Server Clients:
      
      ```
      ip wccp [91] redirect out
      ```

**Note** To allow client request interception, the **ip wccp redirect out** command must be configured on those interfaces connected to the client and the WAN.
4. Enter the following on the interface to the Service Engine:

   `ip wccp redirect exclude in`

   **Note** The router cannot identify requests coming from the Service Engine because the source IP address of the request is not that of Service Engine. To prevent these Service Engine requests from being returned to the Service Engine unresolved, the `ip wccp redirect exclude in` command must be applied to the WCCP-enabled router interface to which the Service Engine is connecting. The `ip wccp redirect exclude in` command prevents the WCCP-enabled router from intercepting any requests coming in on this interface.

   **Caution** If you are using IP Spoofing with multiple Service Engines, the traffic coming back from Origin Server must be redirected to the correct service engine or the flow will break. Because WCCP assignment cannot be controlled, IP Spoofing with multiple Service Engines is not recommended. Use caution configuring multiple Service Engines to use HTTP proxy; the traffic destination IP will be different than expected.

---

**WCCP Interception for Live Streaming**

For WCCP Interception, there are no additional configurations required on the CDSM side for the Managed Live Programs.

The following configurations are to be done specific to WCCP:

1. WCCP Version 2 to be enabled in SE.
2. WCCP Services to be enabled in SE.
3. WCCP Service Group to be enabled in Router.
4. WCCP Router & WCCP enabled SE should be visible to each other.

   **Note** On the Delivery Service configuration in CDSM, the Origin Server Qualified Domain Names must be resolvable.

---

**Configuring WCCP for WMT Manage Live Streaming**

To configure WCCP for WMT Manage Live Streaming:

**Step 1** Select Devices -> Request Routing -> WCCP -> General Settings.
Step 2  To configure WCCP Services in CDSM GUI, go to Request Routing -> WCCP -> Services page. Click on the new icon and select Windows Media service as Service Type and assign the Router List.

Click on the new icon and select RTSP service as Service Type and assign the Router List as well.
Example CLI:

```
wccp-se(config)# wccp version 2
wccp-se(config)# wccp router-list 1 <router_ip>
wccp-se(config)# wccp wmt router-list-num 1
wccp-se(config)# wccp rtsp router-list-num 1
```

**Step 3** On the routers running WCCP Version 2, turn WCCP on for the specified service groups used to redirect the WMT traffic to the Service Engine by entering the following commands:

```
Router(config)# ip wccp 80
Router(config)# ip wccp 81
Router(config)# ip wccp 82
```

**Step 4** Configure the interfaces for WCCP redirection, in case if WMT RTSP traffic comes in on the Ethernet interface and needs to be redirected to SE, enable WCCP redirection to service groups 81 and 82 on the specified interface by entering the following commands:

```
Router(config)# interface Ethernet 0
Router(interface)# ip wccp 80 redirect in
Router(interface)# ip wccp 81 redirect in
Router(interface)# ip wccp 82 redirect in
```

**Step 5** Refer to Configuring Programs Section in Configure Services for Live Program configuration on CDSM.

**Output Example:**

```
Stream-SE#sh prog program-name wmt-live-video
Current Time          : Feb 21 2008 @ 20:40:17 UTC      (1203626417)
Program ID            : 992
Program Name          : wmt-live-video
Delivery Service ID   : 998
Delivery Service Name : wmt-live
Type                  : WMT Managed Continuous Live
Forwarder List        : 10.77.166.139 <- 10.77.166.157
Schedules             :
Schedule #1:
  Start Time (loc) : Always started
  End Time (loc) : N/A
  Duration       : Forever
```
### WCCP Interception for Live Streaming

<table>
<thead>
<tr>
<th>Repeat</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Repeatdays</td>
<td>N/A</td>
</tr>
<tr>
<td>Time spec</td>
<td>local</td>
</tr>
</tbody>
</table>

**Source**

- **Server**: http://10.77.166.157:8080

**Destination**

- **Unicast Access URL**: rtsp://www.ecds.com/wmt-live-video
- **Multicast URL**: http://www.ecds.com/wmt-live-video.nsc.asx
- **Multicast Address**: 224.22.2.2:8080

**Start Time (loc)**: Always started
**Start Time**: Always started
**End Time (loc)**: N/A
**End Time**: N/A

**Current Status**: Playing
**Time left**: N/A

---

**Stream-SE#sh distribution delivery-service delivery-service-name wmt-live-ds**

**Delivery Service Configuration**

<table>
<thead>
<tr>
<th>Delivery Service ID</th>
<th>998</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delivery Service Name</td>
<td>wmt-live-ds</td>
</tr>
<tr>
<td>Content Origin Name</td>
<td>wmt-live</td>
</tr>
<tr>
<td>Content Origin fqdn</td>
<td><a href="http://www.ecds.com">www.ecds.com</a></td>
</tr>
<tr>
<td>Content Origin FQDN</td>
<td>10.77.166.157</td>
</tr>
<tr>
<td>Delivery Service Priority</td>
<td>500</td>
</tr>
<tr>
<td>Delivery Service Type</td>
<td>live</td>
</tr>
<tr>
<td>Configured Distribution Type</td>
<td>Unicast only</td>
</tr>
</tbody>
</table>

**Content Acquirer Information**

| ID of Configured Content Acquirer | 561          |
| Name of Configured Content Acquirer | Stream-SE    |
| IP of Configured Content Acquirer | 10.77.166.139 |
| ID of Effective Content Acquirer | 0            |
| Name of Effective Content Acquirer | N/A          |
| IP of Effective Content Acquirer | N/A          |
| Current content-Acquirer-uid | 0            |
| This SE's Role | Configured Content Acquirer |
| This SE in Full Reload | No           |

---

**Note**

OFQDN Refers to Windows Media Live Server IP (Origin Server) & RFQDN resolves to Origin Server FQDN.

---

### Configuring WCCP for Movie Streamer Managed Live Streaming

- The CDN Administrator configures RTSP live stream service on CDSM, WCCP for RTSP on the SE and the corresponding WCCP enabled router, to allow the SE to intercept client requests.
- RTSP client sends a content request to the OS.
- The request is transparently intercepted by the SE and handed over to the RTSP Proxy.
• The RTSP live request is relayed from the RTSP proxy to the OS. When the RTSP proxy gets the content from the OS, the live stream can then be fanned out to multiple downstream clients.

WCCP supports Movie Streamer RTSP live in a managed scenario.

To configure WCCP for Movie Streamer Managed Live Streaming:

Step 1  Select Devices -> Request Routing -> WCCP -> General Settings.

Step 2  To configure WCCP Services for WCCP in the CDSM GUI go to the Request Routing -> WCCP -> Services page. Click on the new icon and select RTSP service as Service Type and assign the Router List.

Example CLI:
```
wccp-se{config}# wccp version 2
wccp-se{config}# wccp router-list 1 <router_ip>
wccp-se{config}# wccp rtsp router-list-num 1
WCCP configuration for RTSP succeeded. Please remember to config WCCP service 80 on the corresponding router.
```
Step 3  On the routers running WCCP Version 2, turn WCCP on for the specified service groups used to redirect RTSP traffic to the Service Engine by entering the following command:

Router(config)# ip wccp 80

Step 4  Configure the interfaces for WCCP redirection, in case of RTSP traffic that comes in on an Ethernet interface and needs to be redirected to SE, enable WCCP redirection to service group 80 on the specified interface by entering the following commands:

Router(config)# interface Ethernet 0
Router(interface)# ip wccp 80 redirect in

Step 5  Refer to Configuring Programs Section in Configure Services for Live Program configuration on CDSM.

Output Example:

Stream-SE#sh programs program-name ms-live
Current Time : Feb 21 2008 @ 19:48:43 UTC (1203623323)
Program ID : 1422
Program Name : ms-live
Delivery Service ID : 1421
Delivery Service Name : ms-live-new
Type : MS Managed Continuous Live
Forwarder List : 10.77.166.139 <- 10.77.166.156
Schedules :
Schedule #1:
  Start Time (loc) : Always started
  End Time (loc)  : N/A
  Duration : Forever
  Repeat : N/A
  Repeatdays : N/A
  Time spec : local

Source :
  Primary Source URL : rtsp://10.77.166.156/wccp-test.sdp [serving]

Destination :
  Unicast Access URL: rtsp://ms.ecds.com/ms-live.sdp
  Unicast SR URL : rtsp://ms.ecds.com/ms-live.sdp
  Multicast URL : http://ms.ecds.com/ms-live.sdp
  Multicast Address : 224.20.20.20:8010  224.20.20.20:8012

Start Time (loc) : Always started
Start Time   : Always started
End Time (loc) : N/A
End Time     : N/A

Current Status : Playing
Time left     : N/A

Stream-SE#sh distribution delivery-service delivery-service-name ms-live-new
Delivery Service Configuration
---------------------
Delivery Service ID : 1421
Delivery Service Name : ms-live-new
Content Origin Name : ms-live
Content Origin fqdn : ms.ecds.com
Content Origin Origin FQDN : 10.77.166.156
Delivery Service Priority : 500
Delivery Service Type : live
### Configured Distribution Type
- **Unicast only**

### Content Acquirer Information

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID of Configured Content Acquirer</td>
<td>561</td>
</tr>
<tr>
<td>Name of Configured Content Acquirer</td>
<td>Stream-SE</td>
</tr>
<tr>
<td>IP of Configured Content Acquirer</td>
<td>10.77.166.139</td>
</tr>
<tr>
<td>ID of Effective Content Acquirer</td>
<td>0</td>
</tr>
<tr>
<td>Name of Effective Content Acquirer</td>
<td>N/A</td>
</tr>
<tr>
<td>IP of Effective Content Acquirer</td>
<td>N/A</td>
</tr>
<tr>
<td>Current content-Acquirer-uid</td>
<td>0</td>
</tr>
<tr>
<td>This SE’s Role</td>
<td>Configured Content Acquirer</td>
</tr>
<tr>
<td>This SE in Full Reload</td>
<td>No</td>
</tr>
</tbody>
</table>

---

**Note**

OFQDN Refers to Darwin Streaming Server IP (Origin Server) & RFQDN resolves to Origin Server FQDN.

**Note**

RTSP live does not work when SE is behind NAT, this is a well known limitation due to the fact that when the RTSP negotiated video/audio data stream UDP ports are behind NAT, origin server can not reach the UDP ports.

---

**Configuring WCCP for Flash Media Streaming**

- To allow the service engine to intercept client requests, the CDN Administrator configures wccp for rtmp on the service engine and wccp for service group number 84 on the wccp enabled router.
- Flash client sends a flash content request to the OS.
- The request is transparently intercepted by SE and handed over to the FMS Proxy.
- The request is relayed from the edge proxy to the OS.

To configure WCCP for flash media streaming:

**Step 1** Select Devices -> Request Routing -> WCCP -> General Settings.
Step 2   To configure WCCP Services in CDSM GUI, go to the Request Routing -> WCCP -> Services page.
Click on the new icon and select RTMP Service as Service Type and assign the Router List.

Example CLI:
```
se(config)#wccp version 2
se(config)#wccp router-list 1 <router_ip>
se(config)#wccp rtmp router-list-num 1
```

Step 3   On the router side, enable WCCP service for the service Group 84 by executing the following command:
```
router(config)# ip wccp 84
```

Step 4   Configure the interfaces for WCCP redirection, in case of RTMP traffic that comes in on the Ethernet interface and needs to be redirected to SE, enable WCCP redirection to service groups 84 on the specified interface by entering the command:
```
Router(config)# interface Ethernet 0
```
Router(interface)# ip wccp 84 redirect in

**Step 5**  
In order for the SE to actually handle the intercepted request (cache unmanaged vods/split unmanaged live streams) and not bypass the request directly to the origin, the following configuration must be entered on the desired SE:

SE (config)# bypass static port 1935 except-server <fms-origin>

**Step 6**  
Configure Delivery Service in CDSM with FMS Live Server as Origin Server. For more information refer to Configuring Delivery Services section.

No Program configuration is needed on CDSM for FMS Live Streaming. For more information refer to Live Streaming section.

---

**Note**  
WCCP RTMP Unmanaged Live stream splitting is not supported.

**Example URL:**

rtmp://<RFQDN>/live-ecds/<live-stream-name>

**Output Example:**

Stream-SE#sh distribution delivery-service delivery-service-name fms-ds  
Delivery Service Configuration

<table>
<thead>
<tr>
<th>Delivery Service ID</th>
<th>459</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delivery Service Name</td>
<td>fms-ds</td>
</tr>
<tr>
<td>Content Origin Name</td>
<td>fms-os</td>
</tr>
<tr>
<td>Content Origin fqdn</td>
<td><a href="http://www.fms.com">www.fms.com</a></td>
</tr>
<tr>
<td>Content Origin Origin FQDN</td>
<td>10.77.144.137</td>
</tr>
<tr>
<td>Delivery Service Priority</td>
<td>500</td>
</tr>
<tr>
<td>Configured Distribution Type</td>
<td>Unicast only</td>
</tr>
</tbody>
</table>

Content Acquirer Information

| ID of Configured Content Acquirer | 561 |
| Name of Configured Content Acquirer | Stream-SE |
| IP of Configured Content Acquirer | 10.77.166.139 |
| ID of Effective Content Acquirer | 561 |
| Current content-Acquirer-uid | 1203623846 |
| This SE's Role | Configured Content Acquirer |
| This SE in Full Reload | No |

---

**Note**  
OFQDN Refers to FMS Media Server IP (Origin Server) & RFQDN resolves to Origin Server FQDN.

## Troubleshooting WCCP Live Streaming

For troubleshooting WCCP Live Streaming setup refer the section below:

- Check for WCCP formation in Service Engine using the following command:

  Stream-SE#sh wccp routers

  Router Information for Service: RTMP cache
  Routers Configured and Seeing this Service Engine(1)
  Router Id  Sent To  Recv ID
WCCP Interception for Live Streaming

- Check for services enabled on the Service Engine using the following command:

  Stream-SE#sh wccp services

  Services configured on this Service Engine
  RTSP
  WMT
  MMSU

- Check for specific services up & running in SE using the following command:

  Stream-SE#sh wccp services detail

  Service Details for WMT Service
  Service Enabled: Yes
  Service Priority: 201
  Service Protocol: 6
  Application: windows-media
  Service Flags (in Hex): 512
  Service Ports: 1755 0 0 0
  Security Enabled for Service: No
  Multicast Enabled for Service: No
  Weight for this Web-CE: 0
  Negotiated forwarding method: GRE
  Negotiated assignment method: HASH
  Received Values:
  Source IP mask (in Hex): 0
  Destination IP mask (in Hex): 0
  Source Port mask (in Hex): 0
  Destination Port mask (in Hex): 0
  Calculated Values:
  Source IP mask (in Hex): 0
  Destination IP mask (in Hex): 1741
  Source Port mask (in Hex): 0
  Destination Port mask (in Hex): 0

<<Output truncated>>

- Check for packet redirection in the Service Engine using the following command:

  Stream-SE#sh wccp gre

  Transparent GRE packets received: 64
  Transparent non-GRE packets received: 0
  Transparent non-GRE packets passed through: 0
  Total packets accepted: 64
  Invalid packets received: 0
  Packets received with invalid service: 0
  Packets received on a disabled service: 0
  Packets received too small: 0
  Packets dropped due to zero TTL: 0
  Packets dropped due to bad buckets: 0
  Packets dropped due to no redirect address: 0
  Packets dropped due to loopback redirect: 0
  Connections bypassed due to load: 0
  Packets sent back to router: 0
Packets sent to another SE: 0
GRE fragments redirected: 1 -> Counter incremented on successful redirection
Packets failed GRE encapsulation: 0
Packets dropped due to invalid fwd method: 0
Packets dropped due to insufficient memory: 0
Packets bypassed, no conn at all: 0
Packets bypassed, no pending connection: 0
Packets due to clean wccp shutdown: 0
Packets bypassed due to bypass-list lookup: 0
Packets received with client IP addresses: 0
Conditionally Accepted connections: 0
Conditionally Bypassed connections: 0
L2 Bypass packets destined for loopback: 0
Packets w/WCCP GRE received too small: 0
Packets dropped due to IP access-list deny: 0
Packets fragmented for bypass: 0
Packet pullups needed: 1
Packets dropped due to no route found: 0
Packets redirected back to router: 0
Fragmented packets received in GRE: 0
Fragmented packets dropped in GRE: 0
Spoofed packets dropped: 0
Packets received on loopback interface: 0
Count of large egress packets: 0
Packets count for passthrough: 0

• On the Router, use the command `sh ip wccp <service-no> detail` to list down the Service Engines in Router visibility

callista-DCR#sh ip wccp 80 detail
WCCP Client information:
                      WCCP Client ID: 10.77.166.147
                      Protocol Version: 2.0
                      State: Usable
                      Redirection: GRE
                      Packet Return: GRE
                      Assignment: HASH
                      Initial Hash Info: 00000000000000000000000000000000
                      Assigned Hash Info: FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
                      Hash Allotment: 128 (50.00%)
                      Packets s/w Redirected: 43
                      Connect Time: 2d15h
                      Bypassed Packets
                         Process: 1
                         CEF: 1816
                         Errors: 0

For all WCCP show & debug commands Verifying and Troubleshooting WCCP section.

Basic WCCP CLI Configuration Examples

• Enabling WCCP on the Router, page 7-32
• Configuring the Router List Example, page 7-32
Enabling WCCP on the Router

To enable an interface to redirect web traffic to the Service Engine using WCCP Version 2, perform the following tasks beginning in global configuration mode on the router:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1: <code>Router(config)# ip wccp enable</code></td>
<td>Enables the router to use WCCP.</td>
</tr>
<tr>
<td>Step 2: `Router(config)# ip wccp redirect-list [number</td>
<td>acl-name]`</td>
</tr>
<tr>
<td>Step 3: <code>Router(config)# interface type number</code></td>
<td>Enters interface configuration mode.</td>
</tr>
<tr>
<td>Step 4: <code>Router(config-if)# ip web-cache redirect</code></td>
<td>Configures the interface connected to the Internet to redirect web traffic to the Service Engine.</td>
</tr>
<tr>
<td>Step 5: <code>Router(config-if)# ip route-cache same-interface</code></td>
<td>(Optional) If the client and a Service Engine are located on the same network, configures the router to use the fast switching path on the interface.</td>
</tr>
<tr>
<td>Step 6: <code>Router(config-if)# end</code></td>
<td>Exits configuration mode.</td>
</tr>
<tr>
<td>Step 7: <code>Router(config)# copy running-config startup-config</code></td>
<td>Saves the configuration.</td>
</tr>
</tbody>
</table>

Configuring the Router List Example

Use the following commands for basic WCCP Version 2 router configuration:

```
Se(config)# wccp router-list N <ip-address-list>
Se(config)# wccp version 2
Se(config)# wccp port-list 1 8443
Se(config-if)# wccp web-cache router-list-num 1
Se(config-if)# wccp rtmp router-list-num 1
Se(config-if)# wccp wmt router-list-num 1
Se(config)# wccp https-cache router-list-num 1 hash-destination-ip
```

Configuring a Multiple Router/Multiple SE WCCP Service Example

Use the following commands when configuring a multi-router, multi-Service Engine WCCP Service Group. In this example, IP addresses are being configured for SE 1 and 2, and routers 1 and 2:

```
SE1(config)# wccp router-list-num 1 R1-ip R2-ip
SE1(config)# wccp web-cache router-list-num 1
SE2(config)# wccp router-list-num 1 R1-ip R2-ip
SE2(config)# wccp web-cache router-list-num 1
SE(config)# wccp slow-start enable
SE(config)# no wccp slow-start enable
```
Load Balancing Command Examples

- Hash Assignment Command Example, page 7-33
- Mask Assignment Command Example, page 7-33
- Weight Assignment Command Example, page 7-34

Hash Assignment Command Example

The following example configures RTSP service with the hash assignment method using the source IP:

```
SE1(config)# wccp rtsp router-list-num 1 hash-source-ip
```

Check your configuration using the following `show` command:

```
MF-3825# show ip wccp 80 detail
```

```
WCCP Client information:
    WCCP Client ID:          192.168.1.5
    Protocol Version:        2.0
    State:                   Usable
    Redirection:             GRE
    Packet Return:           GRE
    Assignment:              HASH
    Initial Hash Info:       00000000000000000000000000000000
                               00000000000000000000000000000000
    Assigned Hash Info:      FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
                               00000000000000000000000000000000
    Hash Allotment:          128 (50.00%)
    Packets s/w Redirected: 44
    Connect Time:            06:11:51
    Bypassed Packets
        Process:               0
        CEF:                   0
        Errors:                0
```

```
WCCP Client ID:          192.168.1.54
    Protocol Version:        2.0
    State:                   Usable
    Redirection:             GRE
    Packet Return:           GRE
    Assignment:              HASH
    Initial Hash Info:       00000000000000000000000000000000
                               00000000000000000000000000000000
    Assigned Hash Info:      00000000000000000000000000000000
                               FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
    Hash Allotment:          128 (50.00%)
    Packets s/w Redirected: 0
    Connect Time:            00:46:50
    Bypassed Packets
        Process:               0
        CEF:                   0
        Errors:                0
```

Mask Assignment Command Example

Mask assignment is configured correctly by using the following command:

```
SE(config)# wccp web-cache mask src-ip-mask 0x1
SE(config)# wccp web-cache router-list-num 1 mask-assign
SE(config)# wccp web-cache mask src-ip-mask 0x1
```
Basic WCCP CLI Configuration Examples

**SE(config)# wccp web-cache router-list-num 1 mask-assign**

Check your configuration using the following `show` command:

```
router# show ip wccp web-cache detail
```

**WCCP Client information:**

- WCCP Client ID: 192.168.1.54
- Protocol Version: 2.0
- State: Usable
- Redirection: GRE
- Packet Return: GRE
- Packets Redirected: 0
- Connect Time: 00:02:03
- Assignment: MASK

<table>
<thead>
<tr>
<th>Mask</th>
<th>SrcAddr</th>
<th>DstAddr</th>
<th>SrcPort</th>
<th>DstPort</th>
</tr>
</thead>
<tbody>
<tr>
<td>----</td>
<td>-------</td>
<td>-------</td>
<td>-------</td>
<td>-------</td>
</tr>
<tr>
<td>0000: 0x00000001</td>
<td>0x00000000</td>
<td>0x0000</td>
<td>0x0000</td>
<td></td>
</tr>
</tbody>
</table>

**Value**

<table>
<thead>
<tr>
<th>Mask</th>
<th>SrcAddr</th>
<th>DstAddr</th>
<th>SrcPort</th>
<th>DstPort</th>
<th>SE-IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>0000: 0x00000000</td>
<td>0x00000000</td>
<td>0x0000</td>
<td>0x0000</td>
<td>0xC0A80136 (192.168.1.54)</td>
<td></td>
</tr>
</tbody>
</table>

**WCCP Client ID:** 192.168.1.5

- Protocol Version: 2.0
- State: Usable
- Redirection: GRE
- Packet Return: GRE
- Packets Redirected: 0
- Connect Time: 00:02:03
- Assignment: HASH

Initial Hash Info:

- 00000000000000000000000000000000
- 00000000000000000000000000000000

---

**Weight Assignment Command Example**

In the following example, SE 1 has better performing hardware than the SE 2. The administrator wants to have more buckets claimed by the SE 1. The following shows that a higher weight number is assigned to the service engine that has better equipment:

**SE 1(config)# wccp service-number 91 router-list-num 1 port-list-num 1 application cache weight 1000**

**SE 2(config)# wccp service-number 91 router-list-num 1 port-list-num 1 application cache weight 9000**

Check the results by entering the following `show` command:

```
ServiceEngine# show ip wccp 91 detail
```

**WCCP Client information:**

- WCCP Client ID: 192.168.1.5
- Protocol Version: 2.0
- State: Usable
- Redirection: GRE
- Packet Return: GRE
- Assignment: HASH
- Initial Hash Info:
  - 00000000000000000000000000000000
  - 00000000000000000000000000000000
Web Caching Command Examples

When WCCP support is enabled on the router and on the Service Engines, the devices can communicate and deliver the services for which they are configured. To suspend these services, you can disable WCCP support on the router rather than powering off or otherwise disabling individual Service Engines. (For instance, use the `no ip wccp` router command to disable WCCP support on the router.)

Many WCCP Version 2 services also require a configuration of the appropriate `wccp` global configuration command. Refer to the Cisco ECDS Command Reference.

See the following sections for more information:

- Web Cache Service Configuration with Clients and Service Engine on the Same Subnet, page 7-35
- Configuring the Service Engine for Web Cache Service—Clients and Service Engine on the Same Subnet, page 7-35
- Configuring the Router for Web Cache Service—Clients and Service Engine on the Same Subnet, page 7-36
- Configuration Examples—Web Cache Service with Clients and Service Engine on the Same Subnet, page 7-36
- Web Cache Service Configuration with Clients and Service Engine on Different Subnets, page 7-37
- Configuring the Service Engine for Web Cache Service—Clients and Service Engine on Different Subnets, page 7-37
- Configuring the Router for Web Cache Service—Clients and Service Engine on Different Subnets, page 7-38
- Configuration Examples—Web Cache Service with Clients and Service Engine on Different Subnets, page 7-39

Web Cache Service Configuration with Clients and Service Engine on the Same Subnet

In this scenario, the Service Engine and the requesting clients are on the same subnet A router running WCCP Version 2 transparently redirects client HTTP traffic bound for router interfaces s0/0 to the Service Engine. The web cache service redirects HTTP traffic on port 80 only.

Configuring the Service Engine for Web Cache Service—Clients and Service Engine on the Same Subnet

To configure the Service Engine for web cache service, perform the following steps while logged in to the ECDS software in global configuration mode:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ServiceEngine(config)# wccp version 2</code></td>
<td>Ensures that the Service Engine is running WCCP Version 2.</td>
</tr>
<tr>
<td><code>ServiceEngine(config)# wccp router-list 1 10.10.10.1</code></td>
<td>Configures a router list.</td>
</tr>
<tr>
<td><code>ServiceEngine(config)# wccp web-cache router-list-num 1</code></td>
<td>Informs the routers in the specified router list that the Service Engine is accepting web cache service.</td>
</tr>
</tbody>
</table>
Basic WCCP CLI Configuration Examples

### Configuring the Router for Web Cache Service—Clients and Service Engine on the Same Subnet

To configure the router for web cache service, perform the following steps while logged in to the router in global configuration mode:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Router(config)# ip wccp web-cache</td>
</tr>
<tr>
<td>Step 2</td>
<td>Router(config)# interface Ethernet0</td>
</tr>
<tr>
<td>Step 3</td>
<td>Router(config-if)# ip route-cache same-interface</td>
</tr>
<tr>
<td>Step 4</td>
<td>Router(config)# interface Serial0</td>
</tr>
<tr>
<td>Step 5</td>
<td>Router(config-if)# ip wccp web-cache redirect out</td>
</tr>
<tr>
<td>Step 6</td>
<td>Router(config-if)# exit</td>
</tr>
</tbody>
</table>

Configuration Examples—Web Cache Service with Clients and Service Engine on the Same Subnet

This example shows a Service Engine and router configured for web cache service:

**Service Engine**

```bash
hostname Service_engine_2.5.5
!
clock timezone pst -8 0
!
ip domain-name cu.net
!
interface FastEthernet 0
ip address 10.10.20.10 255.255.255.0
no autosense
bandwidth 100
full-duplex
exit
interface FastEthernet 1
shutdown
```
exit
!
ip default-gateway 10.10.20.1
!
ip name-server 10.10.10.100
!
ip wccp router-list 1 10.10.20.1
wccp web-cache router-list-num 1
wccp version 2
!

WCCP-Enabled Router

Building configuration...

Current configuration:
!
version 12.0
!
hostname WCCP-Router
!
ip wccp web-cache
!
interface Ethernet0
   ip address 10.10.10.1 255.255.255.0
   ip route-cache same-interface
!
interface Serial0
   ip address 192.168.1.2 255.255.255.252
   no ip directed-broadcast
   no ip mroute-cache
   ip wccp web-cache redirect out
!
end

Web Cache Service Configuration with Clients and Service Engine on Different Subnets

In this scenario, the Service Engine and the requesting clients are on different subnets, a router running WCCP Version 2 transparently redirects client HTTP traffic bound for router interface s0/0 to the Service Engine. The web cache service redirects HTTP traffic on port 80 only.

Configuring the Service Engine for Web Cache Service—Clients and Service Engine on Different Subnets

To configure the Service Engine for web cache service, perform the following steps while logged in to the ECDS software in global configuration mode:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> ServiceEngine(config)# wccp version 2</td>
<td>Ensures that the Service Engine is running WCCP Version 2.</td>
</tr>
<tr>
<td><strong>Step 2</strong> ServiceEngine(config)# wccp router-list 1 10.10.20.1</td>
<td>Configures a router list.</td>
</tr>
</tbody>
</table>
Configuring the Router for Web Cache Service—Clients and Service Engine on Different Subnets

To configure the router for web cache service, perform the following steps while logged in to the router in global configuration mode:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 Router(config)# ip wccp web-cache</td>
<td>Instructs the router to run the web cache service.</td>
</tr>
<tr>
<td>Step 2 Router(config)# interface Serial0</td>
<td>Specifies which router interface to configure. In this scenario, Serial0 is the router interface to the Internet.</td>
</tr>
<tr>
<td>Step 3 Router(config-if)# ip wccp web-cache redirect out</td>
<td>Instructs the router to redirect web cache traffic bound for the specified interface to Service Engines that accept web cache service. In this scenario there is only one router. Web cache traffic is defined as HTTP packets on port 80.</td>
</tr>
<tr>
<td>Step 4 Router(config-if)# exit</td>
<td>Exits interface configuration mode.</td>
</tr>
</tbody>
</table>
Configuration Examples—Web Cache Service with Clients and Service Engine on Different Subnets

This example shows a Service Engine and router configured for web cache service:

**Service Engine Configuration**

```
hostname Service_engine_2.5.5
!
clock timezone pst -8 0
!
ip domain-name cisco.com
!
exec-timeout 20
!
interface FastEthernet 0
ip address 10.10.20.10 255.255.255.0
no autosense
bandwidth 100
full-duplex
exit
interface FastEthernet 1
shutdown
exit
!
ip default-gateway 10.10.20.1
!
ip name-server 10.10.10.100
!
```

```
wccp router-list 1 10.10.20.1
wccp web-cache router-list-num 1
wccp version 2
```

```
...
```

**WCCP-Enabled Router Configuration**

```
Building configuration...
```

```
Current configuration:
!
hostname WCCP-Router
!
!
ip subnet-zero
!
```

```
ip wccp web-cache
!
interface Ethernet0
  ip address 10.10.10.1 255.255.255.0
!
interface Ethernet1
  ip address 10.10.20.1 255.255.255.0
!
interface Serial0
  ip address 192.168.1.2 255.255.255.252
  no ip directed-broadcast
  no ip mroutecache

ip wccp web-cache redirect out
end
```
Where to Go Next

Proceed to Chapter 8, “Configuring Services” for information about configuring ECDS delivery services and programs.

For more information about WCCP, see the following resources:

• Web Cache Communication Protocol v2

Tip

For the most current information, refer to the Cisco ECDS 2.6 Software Administration Configuration Guide on Cisco.com.