Configuring the Service Router

The following sections describe how to configure a Service Router (SR):

- Activating a Service Router, page 6-1
- Configuring Application Control, page 6-4
- Configuring Last-Resort Routing, page 6-5
- Configuring Transaction Logs for the Service Router, page 6-8
- Where to Go Next, page 6-10

Tip For information on configuring the general settings, except last-resort routing and transaction logging, see the "General Settings" section on page 5-69.

Activating a Service Router

Activating an SR can be done through the Devices home page initially, or through the Device Activation page.

To activate an SR from the Device Activation page:

Step 1 Choose **Devices** > **Devices**. The Devices Table page is displayed.

Step 2 Click the **Edit** icon next to the device you want to configure. The Devices home page is displayed.

Step 3 Click **Show All** to display the top-level menu options, and choose **Device Activation**. The Device Activation page is displayed.

Step 4 Enter the settings as appropriate. See Table 6-1 for a description of the fields.

Table 6-1 Service Router Activation Fields

Field	Description
Name	Name of the device.
Location	The Location drop-down list lists all the location configured for the ECDS.

Table 6-1 Service Router Activation Fields (continued)

Field	Description
Activate	To activate or deactivate the device, check or uncheck the **Activate** check box. Alternatively, you can click the **Deactivate Device** icon in the task bar. When you uncheck the **Activate** check box and click **Submit**, the **Replaceable** check box is displayed. Check the **Replaceable** check box when you need to replace the device or recover lost registration information. For more information, see the "Recovering ECDS Network Device Registration Information" section on page 11-20.
Server Offload	To offload this device for maintenance or a software upgrade, check the **Server Offload** check box. When checked, the Service Router stops processing client requests. When the SR is marked as inactive or is marked with server offload on the CDSM it stops responding to DNS queries. Instead, the SR sends a SERVFAIL error as the DNS response, and for RTSP/HTTP requests, the SR sends a 503 Service Unavailable message. To monitor the current activity on an SR during the Server Offload state, use the **show interface** command. If the packets received or packets sent is increasing then the SR is processing client requests. **Note** We recommend separating the management traffic from the client request traffic by using the port channel configuration. • If management and client request traffic are separated, the **show interface** command for the client request port channel displays information on active sessions. • If management and streaming traffic are not separated, the **show interface** command shows very low traffic; the packets received and packets sent are lower than a client request session. Once the SR has finished processing client requests, you can perform maintenance or upgrade the software on the device. For information about upgrading the software, see the "Upgrading Software" section on page 11-1. The Status field on the Device Activation page and the Devices Table page displays "offloading" when **Server Offload** is checked. Once the software upgrade or maintenance is complete, you need to uncheck the **Server Offload** check box so that the device can again participate in the system.

Table 6-1 Service Router Activation Fields (continued)

Field	Description
Server Maintenance	To prevent raising of OFFLINE device alarms in CDSM during pre-staging or location movement of devices, check the **Server Maintenance** check box and click **Submit**. When the device goes to the Maintenance mode, CDSM suppresses displaying of the device alarms in the System Status. We recommend you not to operate the device in Maintenance mode for streaming operations, because some functionalities will not work. **Note** The Server Maintenance mode is applicable to only Service Engines & Service Routers. To bring back the device to ONLINE mode, uncheck the **Server Maintenance** check box and click **Submit**. **Note** This feature is supported in all releases starting from ECDS Release 2.6.6.
Work Type	From the **Work Type** drop-down list, choose **Service Router only**. The **SR & Proximity Engine** option is not supported.
Coverage Zone File	To have a local Coverage Zone file overwrite the ECDS network-wide Coverage Zone file, choose a file from the **Coverage Zone** drop-down list. See the "Coverage Zone File Registration" section on page 9-15 for information about creating and registering a Coverage Zone file. Otherwise, choose **None**.
Use SR's primary IP address	Enables the CDSM to use the IP address on the primary interface of the SR for management communications. **Note** If the **Use SR's primary IP Address for Management Communication** check box is checked and the Management Communication Address and Port are configured, the CDSM uses the SR's primary IP address for communication. **Note** Do not check the **Use SR's primary IP Address for Management Communication** check box if you want to separate management and streaming traffic. Instead, use the Management Communication Address and Port fields to specify where management traffic should be sent.
Management Communication Address	Manually configures a management IP address for the CDSM to communicate with the SR. Manual configuration of the management IP address and port are used when using port channel configuration to separate management and streaming traffic. For more information about port channel configuration see the "Configuring Port Channel and Load Balancing Settings" section on page 5-89.
Management Communication Port	Port number to enable communication between the CDSM and the SR.
Comments	Information about the settings.

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

Configuring Application Control

The Application Control pages allow you to enable Flash Media Streaming, to enable HTTP proxy on an SR, and to enable HTTP 302 redirection for Windows Media Technology files with an .asx extension.

To configure the application control for the SR:

Step 1 Choose **Devices** > **Devices**. The Devices Table page is displayed.

Step 2 Click the **Edit** icon next to the SR you want to configure. The Devices home page is displayed.

Step 3 Click **Show All** to display the top-level menu options, and choose **Application Control**.

Step 4 To enable Flash Media Streaming on the SR, choose **Flash Media Streaming** > **General Settings**. The Flash Media Streaming Settings page is displayed.

a. Check the **Enable Flash Media Streaming** check box.

b. Click **Submit**.

To apply the factory default settings for the device, click the **Apply Defaults** icon in the task bar.

To remove the settings from the device, click the **Remove Settings** icon in the task bar.

Step 5 To enable service monitoring for Flash Media Streaming on the SR, choose **Flash Media Streaming** > **Service Monitoring**. The Service Monitoring Settings page is displayed.

a. Check the **Enable Service Monitoring** check box.

b. Click **Submit**.

To apply the factory default settings for the device, click the **Apply Defaults** icon in the task bar.

To remove the settings from the device, click the **Remove Settings** icon in the task bar.

Step 6 To enable HTTP proxy on the SR:

a. Choose **Web** > **HTTP** > **HTTP Connections**. The HTTP Connections Settings page is displayed.

b. Check the **Enable Incoming Proxy** check box.

c. Enter the port numbers that receive HTTP in the associated field.

Separate each port number by a space. The default is port 80.

d. Click **Submit** to save the settings.

To apply the factory default settings for the device, click the **Apply Defaults** icon in the task bar.

To remove the settings from the device, click the **Remove Settings** icon in the task bar.

Step 7 To enable the HTTP 302 redirection for Windows Media Technology files with an .asx extension:

a. Choose **Web** > **HTTP** > **HTTP Redirect**. The HTTP Redirect Settings page is displayed.

b. Check the **Enable HTTP 302 for .asx File** check box.

c. Click **Submit**.

To apply the factory default settings for the device, click the **Apply Defaults** icon in the task bar.

To remove the settings from the device, click the **Remove Settings** icon in the task bar.

Configuring Last-Resort Routing

Last-resort routing is useful when all Service Engines have exceeded their thresholds or all Service Engines in the domain are offline, or the client is unknown. If last-resort routing is configured, the Service Router redirects requests to a configurable alternate domain when all Service Engines serving a client network region are unavailable, or the client is unknown. A client is considered unknown if the client's IP address is not part of a subnet range listed in the Coverage Zone file or part of a defined geographical area listed in the Coverage Zone file.

See the following sections:

- Creating a New Service, page 6-5
- Error File Name Examples, page 6-7
- Creating ASX Error Message Files for Windows Media Live Programs, page 6-7

Note If the last-resort domain is not configured and the Service Engine thresholds are exceeded, known client requests are redirected to the origin server and unknown clients will either receive an error URL (if the Error Domain and Error Filename fields are configured), or a 404 "not found" message.

Unknown clients are only redirected to the alternate domain (last-resort domain) when the **Allow Redirect All Client Request** check box is checked or the equivalent **service-router last-resort domain** <*RFQDN*> **allow all** command is entered.

For information about configuring all general settings, except last-resort routing, see the "General Settings" section on page 5-69.

Creating a New Service

To configure last-resort routing:

Step 1 Choose **Devices** > **Devices**. The Devices Table page is displayed.

Step 2 Click the **Edit** icon next to the SR you want to configure. The Devices home page is displayed.

Step 3 Click **Show All** to display the top-level menu options.

Step 4 Choose **General Settings** > **Last Resort**. The Last Resort Table page is displayed.

The table is sortable by clicking the column headings.

Step 5 Click the **Create New** icon.

Click the **Edit** icon next to the domain name to edit a table entry.

Step 6 Enter the settings as appropriate. See Table 6-2 for a description of the fields.

Table 6-2 Service Router Last Resort Fields

Field	Description
Domain Name	The Service Routing Domain Name (SRDN) (for example, srfqdn.cisco.com).
Allow Redirect All Client Request	Check the **Allow Redirect All Client Request** check box to redirect all unknown clients to the alternate domain or content origin. If the **Allow Redirect All Client Request** check box is not checked, unknown clients (clients' subnets are not included in the Coverage Zone file) receive a 404 message if the error URL is not configured. If the error URL is configured, client requests are redirected to the Error URL. If the **Allow Redirect All Client Request** check box is checked, unknown client requests are redirected to the alternate domain; otherwise, they are redirected to the origin server.
Alternate Domain Name	The domain (for example, www.cisco.com) used to route requests to when the SEs are unavailable, or the client is unknown. A client is considered unknown if the client's IP address is not part of a subnet range listed in the Coverage Zone file. If an Alternate Domain Name is not specified, requests for the domain entered in the Domain Name are routed to the origin server. The Alternate Domain Name could be a domain outside the ECDS. It could be a third-party CDN or external server. No DNS lookup is performed by the SR to check the liveness of this domain.
Error Domain Name	To redirect the request to an error URL for any unknown clients or when all SEs in the delivery service are unavailable, enter the domain name of the URL. The Error Domain Name could be a domain outside the ECDS. It could be a third-party CDN or external server. No DNS lookup is performed by the SR to check the liveness of this domain.
Error File Name	The filename of the error URL (for example, error.html or error/errorfile.flv). The error URL is made using the Error Domain Name plus the Error File Name. The Error File Name could be a filename with an extension (for example, error.html or errorfile.flv), or a directory and filename (for example, error/errorfile.flv or reroute/reroute.avi), or a filename without an extension. If no extension is specified, the extension is determined by the protocol used in the request. If a filename has a specific extension, and the request comes from a protocol that does not support the configured extension, the filename extension is automatically changed to an extension that is supported by the protocol. **Note** For Flash Media Streaming, an external FMS server must exist that hosts an application for error handling. The SR redirects Flash Media Streaming requests to an application on the external FMS server. An example of a Flash Media Streaming error URL is rtmp://errordomain.com/<*application*>, where the application name is any application hosted on that server. The Error File Name, in the case of Flash Media Streaming, is the name of the application. See the "Error File Name Examples" section on page 6-7.

Step 7 Click **Submit** to save the settings. The entry is added to the Last Resort Table.

To delete a last-resort configuration, click the **Edit** icon for the configuration, then click the **Delete** icon in the task bar.

Error File Name Examples

- Domain Name—wmt.cdsordis.com
- Error Domain Name—ssftorig.ssft.com
- Error File Name—testMessage

This configuration states that for any request where the domain name is wmt.cdsordis.com, if the client IP address is not included in the Coverage Zone file (or the client is not part of a defined geographical area if location-based routing is enabled) or there are no available SEs assigned to the delivery service, redirect the request to ssforig.ssft.com/testMessage.<*original_extension*>.

For example, if the client request was http://wmt.cdsordis.com/vod/video.wmv and the service rule conditions were met, the client would receive a 302 redirect to http://ssftorig.ssft.com/testMessage.wmv.

If you want the Error File Name to reside in a different directory, you can configure that as well. If the error message file was located in the "vod" directory, then the Error File Name would be configured as vod/testMessage.

Creating ASX Error Message Files for Windows Media Live Programs

Note When redirecting a client request for live Windows Media Streaming programs, the error message must have the same format because live programs deliver an ASX file to the client. If you try to use an HTML or JPEG instead of an ASX file, the redirect will not work because the Windows Media player is trying to parse the ASX file.

To satisfy the requirements of the Windows Media player, create an ASX file for the error message file and put the URL to the error message file inside the ASX file. For example, below is a simple ASX file.

```
<ASX VERSION="3.0"> <Entry>

<REF HREF="http://<IP-Address-of-Server/path/filename"/>

</Entry> </ASX>
```

If you wanted the error file to be a GIF file on server 3.1.1.1 called testMessage.gif under the directory vod then this file would look like:

```
<ASX VERSION="3.0"> <Entry>

<REF HREF="http://3.1.1.1/vod-ecds/testMessage.gif"/>

</Entry> </ASX>
```

There are other ways to use an ASX file to display information. Below is an example of an approach to have the Windows Media player display an HTML web page with PARM HTMLView.

```
<ASX version="3.0"> <PARAM name="HTMLView"
value="http://111.254.21.99/playlist/error.htm"/> <REPEAT> <ENTRY>

<REF href="http://3.1.1.1/vod-ecds/testMessage.gif"/>

</ENTRY> </REPEAT> </ASX>
```

There are many ways to format and structure ASX files to display whatever error message you want, in whatever format you want.

Configuring Transaction Logs for the Service Router

Transaction logs allow administrators to view the traffic that has passed through the SR. The fields in the transaction log are the client's IP address, the date and time when a request was made, the URL that was requested, the SE selected to serve the content, the protocol, and the status of the redirect. The SR transaction log file uses the W3C Common Log file format. For more information about transaction logs and their formats, see the "Service Router Transaction Log Fields" section on page 10-65.

To enable transaction logging for the SR:

Step 1 Choose **Devices** > **Devices**. The Devices Table page is displayed.

Step 2 Click the **Edit** icon next to the device you want to configure. The Devices home page is displayed.

Step 3 Click **Show All** to display the top-level menu options.

Step 4 Choose **General Settings** > **Notification and Tracking** > **Transaction Logging**. The Transaction Log Settings page is displayed.

Step 5 Enter the settings as appropriate. See Table 6-3 for a description of the fields.

Table 6-3 Transaction Log Settings Fields

Field	Description
General Settings	
Transaction Log Enable	Enables transaction logging.
Compress Files before Export	When this check box is checked, archived log files are compressed into gzip format before being exported to external FTP servers
Archive Settings	
Max size of Archive File	Maximum size (in kilobytes) of the archive file to be maintained on the local disk. The range is from 1,000 to 2,000,000. The default is 2,000,000.
Max number of files to be archived	Maximum number of files to be maintained on the local disk. The range is from 1 to 1000. The default is 50.

Table 6-3 Transaction Log Settings Fields (continued)

Field	Description
Archive occurs	How often the working log is archived and the data is cleared from the working log. Choose one of the following: • Choose **every** to archive every so many seconds, and enter the number of seconds for the interval. The range is from 120 to 604800. • Choose **every hour** to archive using intervals of one hour or less, and choose one of the following: – **at**—Specifies the minute in which each hourly archive occurs – **every**—Specifies the number of minutes for the interval (2, 5, 10, 15, 20, or 30) • Choose **every day** to archive using intervals of one day or less, and choose one of the following: – **at**—Specifies the hour in which each daily archive occurs – **every**—Specifies the number of hours for the interval (1, 2, 3, 4, 6, 8, 12, 24) • Choose **every week on** to archive at intervals of one or more times a week, choose the days of the week, and choose what time each day.
Export Settings	
Enable Export	Enables exporting of the transaction log to an FTP server.
Export occurs	How often the working log is sent to the FTP server and the data is cleared from the working log. Choose one of the following: • Choose **every** to export every so many minutes, and enter the number of minutes for the interval. The range is from 1 to 100800. • Choose **every hour** to export using intervals of one hour or less, and choose one of the following: – **at**—Specifies the minute in which each hourly export occurs – **every**—Specifies the number of minutes for the interval (2, 5, 10, 15, 20, or 30) • Choose **every day** to export using intervals of one day or less, and choose one of the following: – **at**—Specifies the hour in which each daily export occurs – **every**—Specifies the number of hours for the interval (1, 2, 3, 4, 6, 8, 12, 24) • Choose **every week on** to export using intervals of one or more times a week, choose the days of the week, and what time each day.
FTP Export Server	IP address or hostname of the FTP server.
Name	Name of the user.
Password	Password for the user.

Table 6-3 Transaction Log Settings Fields (continued)

Field	Description
Confirm Password	Confirms the password for the user.
Directory	Name of the directory used to store the transaction logs on the FTP server.
SFTP	Check the **SFTP** check box, if you are using an SFTP server.

Step 6 Click **Submit** to save the settings.

To apply the factory default settings for the device, click the **Apply Defaults** icon in the task bar.

To remove the settings from the device, click the **Remove Settings** icon in the task bar.

Where to Go Next

Proceed to Chapter 7, “Configuring WCCP.”