



CHAPTER 9

Using the Service Configuration Editor: Traffic Control

Published: August 08, 2013, OL-26821-06

Introduction

The Traffic Control capabilities of the Service Control Engine (Service Control platform, and the Cisco Service Control Application for Broadband) are used to limit and prioritize traffic flows. Control of traffic is based on parameters such as the service of the flow, the package of the subscriber, and the quota state of the subscriber. This chapter consists of these sections:

- [Managing Bandwidth, page 9-2](#)
- [Managing Virtual Links, page 9-44](#)
- [Managing Packages, page 9-51](#)
- [Managing Rules, page 9-61](#)
- [Managing Quotas, page 9-83](#)
- [Unknown Subscriber Traffic, page 9-99](#)

Managing Bandwidth

The upstream and downstream interfaces are each assigned one default global controller. You can add additional global controllers.

The number of global controllers a service configuration can contain varies based on the Cisco SCE hardware. The maximum number of global controllers including the default global controllers are:

- Cisco SCE 2000—1024 upstream and 1024 downstream
- Cisco SCE 8000 multi-Gigabit Ethernet—1024 upstream and 1024 downstream
- Cisco SCE 8000 10 Gigabit Ethernet—4096 upstream and 4096 downstream

After you have defined global controllers, you can add subscriber BW controllers (BWCs) to packages, and map these subscriber BWCs to different global controllers.



Note

In release 3.7.5, the global bandwidth controller for IPv6 works in the subscriberless mode. The IPv6 traffic is mapped to a default subscriber (N/A). Bandwidth control should be performed on the Unknown Subscriber Package. The maximum and the default package ID of the Unknown Subscriber value is 4999.



Caution

If you enable or disable Virtual Links mode, all user-defined global controllers are deleted from the service configuration. A subscriber BWC that pointed to a user-defined global controller now points to the default global controller. (Other parameters of these subscriber BWCs remain unchanged.)

- [Managing Global Bandwidth, page 9-2](#)
- [How to View Global Controller Settings, page 9-3](#)
- [How to Edit the Total Link Limits, page 9-5](#)
- [How to Add Global Controllers, page 9-7](#)
- [How to Set the Maximum Bandwidth of Global Controllers, page 9-9](#)
- [How to Delete Global Controllers, page 9-11](#)
- [How to Define Global Controllers, page 9-11](#)
- [Managing Subscriber Bandwidth, page 9-29](#)
- [Managing Bandwidth: A Practical Example, page 9-33](#)
- [How to Set BW Management Prioritization Mode, page 9-42](#)

Managing Global Bandwidth

The upstream and downstream interfaces are each assigned one default global controller that, by default, controls the total link traffic. Based on the Cisco SCE hardware, the number of global controllers you can add to a service configuration varies. For details, see the [“Managing Bandwidth” section on page 9-2](#).

You can also define the bandwidth total link limit to be less than the physical capacity of the Cisco SCE platform for each interface separately. When another device that has limited BW capacity is next to the Cisco SCE platform on the IP stream, you can have this limitation enforced in a policy-aware manner by the Cisco SCE platform, instead of having it enforced arbitrarily by the other device.

How to View Global Controller Settings



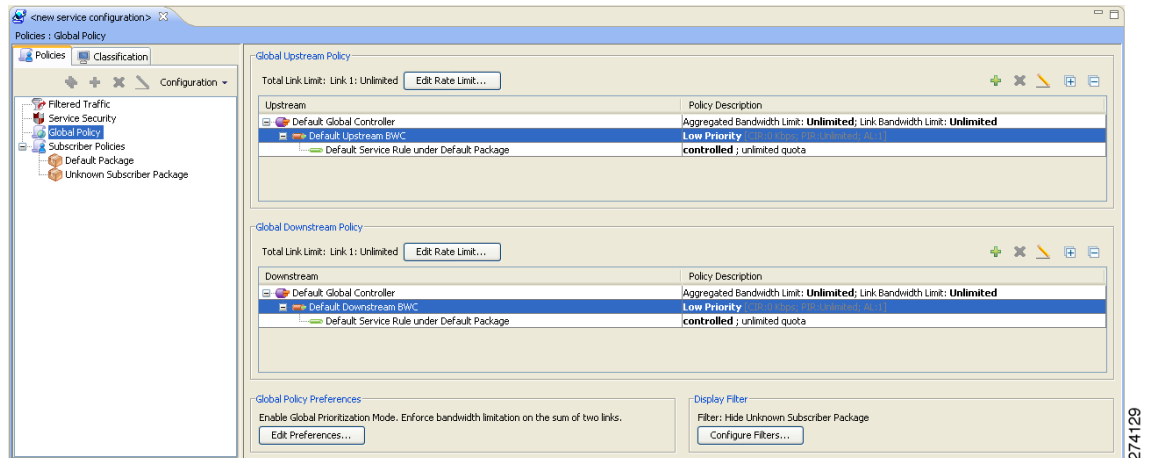
Note

Global controller bandwidth is based on Layer 1 volume. Accounting, reporting, and subscriber bandwidth control in Cisco SCA BB is based on Layer 3 volume.

Step 1 In the Policies tab, click **Global Policy**.

The Global Bandwidth Settings dialog box is displayed in the right (Rule) pane ([Figure 9-1](#)).

Figure 9-1 Global Bandwidth Settings



The two check boxes near the top of the Global Controllers tab are used only in dual-link systems (see [“How to Define Global Controllers”](#) section on page 9-11).

The main part of the pane contains the Upstream area listing upstream global controllers and the Downstream area listing downstream global controllers. Each list has two columns:

- **Upstream or Downstream**—Displays the hierarchy of global controllers, bandwidth controllers, and service rules. Each global controller has the bandwidth controllers that are connected to it listed as children. Each bandwidth controller has the service rules associated with it listed as children.
- **Policy Description**—Summarizes the details of the global controller, bandwidth controller, or service rule in the corresponding column. In the rows containing the global controller details, the maximum bandwidth value permitted to this global controller is displayed.

For each global controller, you can set different values for the maximum bandwidth for each of the four time frames defined by the default calendar. For details, see [“Managing Calendars”](#) section on page 9-76.

- A single value in this field indicates that the maximum bandwidth for this global controller is constant.
- If each time frame has a different maximum bandwidth, the maximum bandwidth for each time frame is displayed, separated by commas ([Figure 9-2](#)).

Figure 9-2 Time Frame Display

Upstream	Policy Description
Default Global Controller	Aggregated Bandwidth Limit: 2.0 Mbps, 3.0 Mbps, 4.0 Mbps, 6.0 Mbps; Link Bandwidth Limit: ...
Default Upstream BWC	Low Priority (CIR:0 Kbps; PIR:Unlimited; AL:1)

- If two time frames have the same maximum bandwidth, the value is not repeated (Figure 9-3). (So 40,,,100 means that the first three time frames have a maximum bandwidth of 40 percent of the total link limit, and the fourth time frame has a maximum bandwidth equal to the total link limit.)

Figure 9-3 Time Frame Details

Name	CIR (L3 Kbps)	PIR (L3 Kbps)
Primary Upstream BWC	0	Unlimited
Default Upstream BWC	0	Unlimited
BWC 1	9000	Unlimited

Above the area (Upstream or Downstream) of each interface, the total link limit is displayed (Figure 9-4).

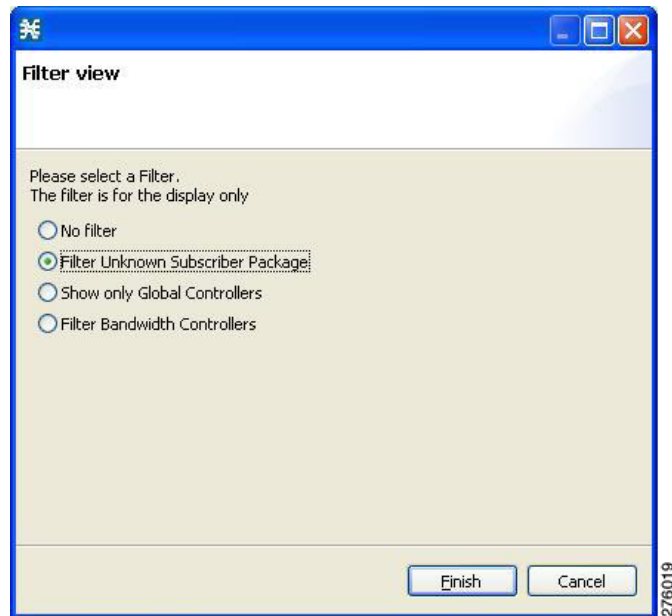
Figure 9-4 Total Link Time

Name	CIR (L3 Kbps)	PIR (L3 Kbps)	Global Controller	AL
Primary Upstream BWC	0	Unlimited		
Default Upstream BWC	9000	Unlimited	Default Global Controller	1
BWC 1	9000	Unlimited	Default Global Controller	1

How to Filter Global Controllers

- Step 1** In the Policies tab, click **Global Policy**.
The Global Bandwidth Settings are displayed in the right (Rule) pane.
- Step 2** Click **Configure Filters**.
The Filter View dialog box appears (Figure 9-5).

Figure 9-5 Filter View



- Step 3** Choose one of the filter radio buttons:
- **No Filter**
 - **Filter Unknown Subscriber Package**
 - **Show only Global Controllers**
 - **Filter Bandwidth Controllers**
- Step 4** Click **Finish**.
The Filter View dialog box closes and the right (Rule) pane is filtered according to your selection.

How to Edit the Total Link Limits

You can limit the total bandwidth for each Cisco SCE link passing through the Cisco SCE platform.

For example, if a device connected to the Cisco SCE platform on the IP stream has limited BW capacity, you can limit the bandwidth for each Cisco SCE link passing through the Cisco SCE platform to match the capacity of the other device.

**Note**

The total bandwidth here means the limit for each Cisco SCE link and not the aggregated limit on all the links.

The total link limits, for each Cisco SCE link, for upstream and downstream traffic are defined independently.

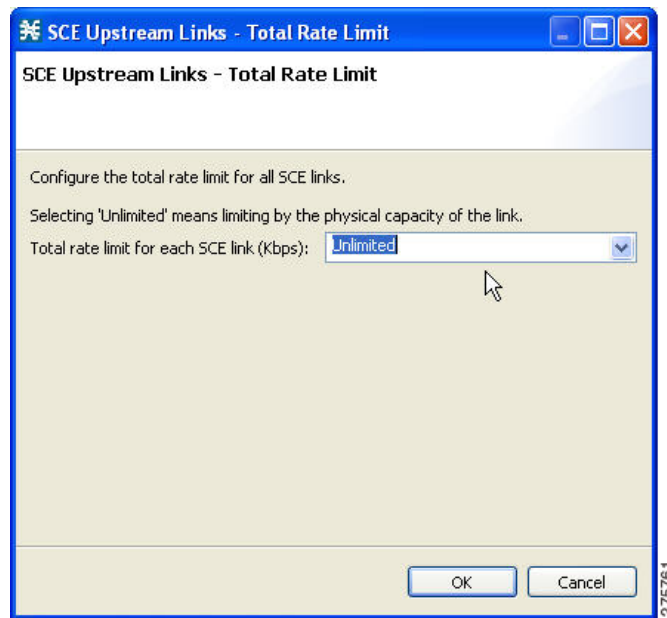
To edit the total link limits, complete the following steps:

- Step 1** In the Policies tab, click **Global Policy**.
The Global Bandwidth Settings dialog box is displayed in the right (Rule) pane.
- Step 2** In the Upstream or Downstream section, click **Edit Rate Limit** (Figure 9-6).

**Note**

The display appearance of Figure 9-6 depends on the global controller mode setting.

Figure 9-6 SCE Upstream Links - Total Rate Limit



- Step 3** Select the total rate limit in the Total rate limit for each Cisco SCE link (Kbps) field.
- Step 4** Click **OK**.

Your changes are saved.

The Global Controller Settings dialog box closes.

How to Add Global Controllers

Based on the Cisco SCE hardware, the number of global controllers you can add to a service configuration varies. For details, see the [“Managing Bandwidth” section on page 9-2](#).


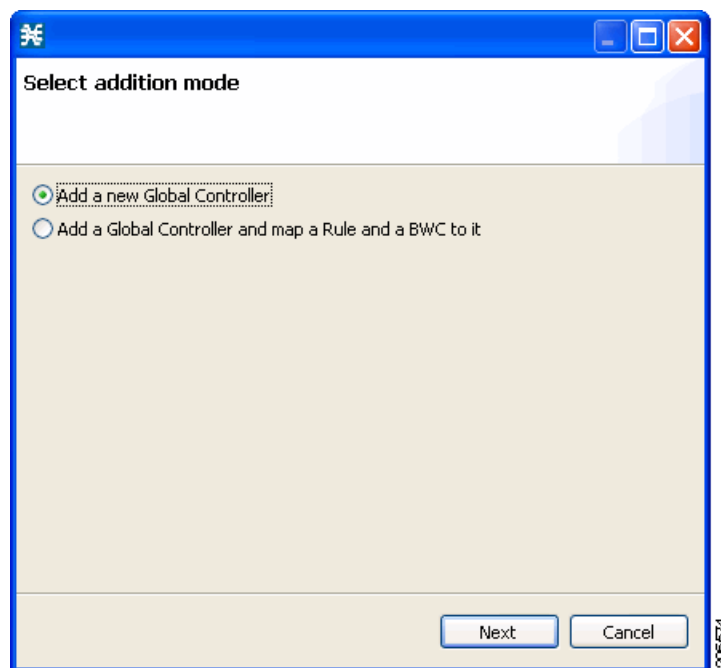
- Step 1** In the Policies tab, click **Global Policy**.
- The Global Bandwidth Settings dialog box is displayed in the right (Rule) pane.
- Step 2** Above the area (Upstream or Downstream) of the desired interface, click the **Add** () icon.
- The Select Addition mode dialog box appears ([Figure 9-7](#)).

Figure 9-7 Select Addition Mode



- Step 3** Choose the **Add a new Global Controller** radio button, to add a new global controller.

Step 4 Click **Finish**.

The Global Controller Settings dialog box appears (Figure 9-8).



Note

The display of Figure 9-8 depends on the global controller mode setting.

Figure 9-8 Upstream Global Controller Settings

Global Controller Settings

Global Controller must have a gcNameText

Name:

The global controller enforces a L1 rate limit on traffic that is mapped to it. The global controller can enforce an aggregate rate limit across all SCE links, as well as a separate rate limit per SCE link.

Aggregate Global Controller

The global controller can enforce a different rate limit per time frame.

The same rate limit for all time frames

A different rate limit per time frame

Single Rate Limit (Kbps)

Global Controller	Rate Limit
Aggregate	Unlimited

Per Link Global Controller

The global controller can enforce a different rate limit per time frame.

The same rate limit for all time frames

A different rate limit per time frame

Single Rate Limit (Kbps)

Global Controller	Rate Limit
For all Links	Unlimited

OK Cancel

2007-2009

Step 5 In the **Name** field enter a meaningful name.

Step 6 To edit the maximum bandwidth of the global controller, continue with the instructions in the section [How to Set the Maximum Bandwidth of Global Controllers](#), page 9-9.

Step 7 Click **OK**.

Your changes are saved.

The Global Controller Settings dialog box closes.

How to Set the Maximum Bandwidth of Global Controllers

You can edit the maximum bandwidth that a global controller can carry.


You can set a different maximum bandwidth for each of the four available time frames.

You can set different values for each link and for the aggregated BW of all links.

Step 1 In the Policies tab, click **Global Policy**.

The Global Bandwidth Settings dialog box is displayed in the right (Rule) pane.

Step 2 Select a global controller.

Step 3 Click the Edit () icon.

The Global Controller Settings dialog box appears ([Figure 9-9](#)).



Note

The display of [Figure 9-9](#) depends on the global controller mode setting.

Figure 9-9 Upstream Global Controller Settings

Upstream Global Controller Settings

Global Controller Settings
Configure the rate limit that this global controller should enforce.

Name:

The global controller enforces a L1 rate limit on traffic that is mapped to it. The global controller can enforce an aggregate rate limit across all SCE links, as well as a separate rate limit per SCE link.

Per Link Global Controller

The global controller can enforce a different rate limit per time frame.

The same rate limit for all time frames

A different rate limit per time frame

Single Rate Limit (Kbps)

Global Controller	Rate Limit
For all Links	Unlimited

OK Cancel

275763

Step 4 Set a single value for the maximum bandwidth limit that this global controller carries.

- Choose the **The same rate limit for all time frames** radio button, and in the Single Rate Limit (Kbps) field, enter the desired value in Kbps for the maximum bandwidth.

- Step 5** Set the maximum limit that this global controller carries to vary according to time frame.
- Choose the **A different rate limit per time frame** radio button, and enter the desired value for each time frame (Figure 9-10).

**Note**

The display of Figure 9-10 depends on the global controller mode setting.

Figure 9-10 Upstream Global Controller Settings

Global Controller Settings
Configure the rate limit that this global controller should enforce.

Name:

The global controller enforces a L1 rate limit on traffic that is mapped to it. The global controller can enforce an aggregate rate limit across all SCE links, as well as a separate rate limit per SCE link.

Aggregate Global Controller
The global controller can enforce a different rate limit per time frame.

The same rate limit for all time frames
 A different rate limit per time frame

Rate Limit per Time Frame (Kbps)

Global Controller	Time Frame T1	Time Frame T2	Time Frame T3	Time Frame T4
Aggregate	Unlimited	Unlimited	Unlimited	Unlimited

Per Link Global Controller
The global controller can enforce a different rate limit per time frame.

The same rate limit for all time frames
 A different rate limit per time frame

Rate Limit per Time Frame (Kbps)

Global Controller	Time Frame T1	Time Frame T2	Time Frame T3	Time Frame T4
For all Links	Unlimited	Unlimited	Unlimited	Unlimited

OK Cancel

**Note**

These values are applied to the time frames of the default calendar.

- Step 6** Click **OK**.
Your changes are saved.
The value in the Policy Description column changes to reflect the new bandwidth limits.
- Step 7** Repeat [Step 2](#) through [Step 6](#) for other global controllers.

How to Delete Global Controllers

You can delete unused global controllers at any time. The default global controller and the Total Link Limit cannot be deleted.

Step 1 In the Policies tab, click **Global Policy**.
The Global Bandwidth Settings dialog box appears.

Step 2 Select a global controller.

Step 3 Click the **Delete** () icon.



Note If a subscriber BWC is using the specified global controller (see [“How to Edit Package Subscriber BWCs” section on page 9-30](#)), a global controller cannot be removed message is displayed. The global controller cannot be deleted until you unassign it from all subscriber BWCs.

The global controller is deleted.

Step 4 Click **OK**.

Your changes are saved.

The Global Bandwidth Settings dialog box closes.

How to Define Global Controllers

This section describes how to define global controllers in both dual-link and multi-gigabit Ethernet systems.

In both systems, you can define each link separately with equal rates or you can define each link separately with different rates.

Alternatively, you can apply bandwidth limitations as an aggregate for all links or as an aggregate with individual control of each links.

You can:

1. Control each link separately with equal rate to all links.
2. Control each link separately without with different rate per link.
3. Control the links in aggregate and in addition maximum rate per-link, which is equal between all links.
4. Control the links in aggregate and in addition maximum rate per-link, which is different between the links.
5. Control the links in Virtual Link mode.



Note If Virtual Links mode is enabled, bandwidth limitations are applied to the sum of the all links.

**Note**

Any attempt to change the global controller bandwidth for invalid link results in an error message during apply policy, similar to the following:

“Invalid value set on Link ID 6 for upstream GC ‘Default Global Controller’. Link ID 6 does not exist. Available Link IDs: 1, 2, 3, 4”

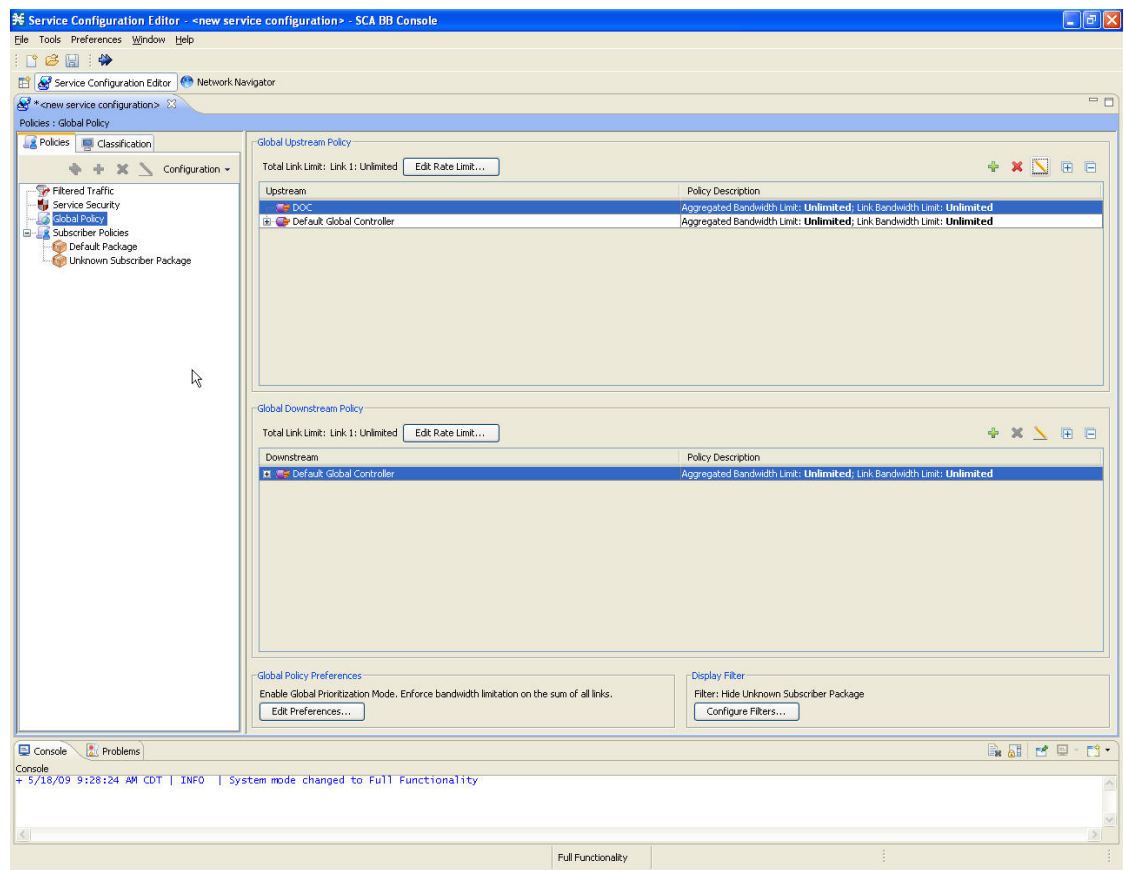
To activate the respective edit dialog of the Global Controller settings (Figure 9-11):

- Double click on a global controller row in the global controller table view on the right main panel of the Global Policy setting.
- Click on the edit button that is located on the top right main panel of the Global Policy setting.

**Note**

The behavior is the same whether you configure upstream or downstream GC.

Figure 9-11 Global Controller Settings Activation



275765

Refer to the following sections for configuration details:

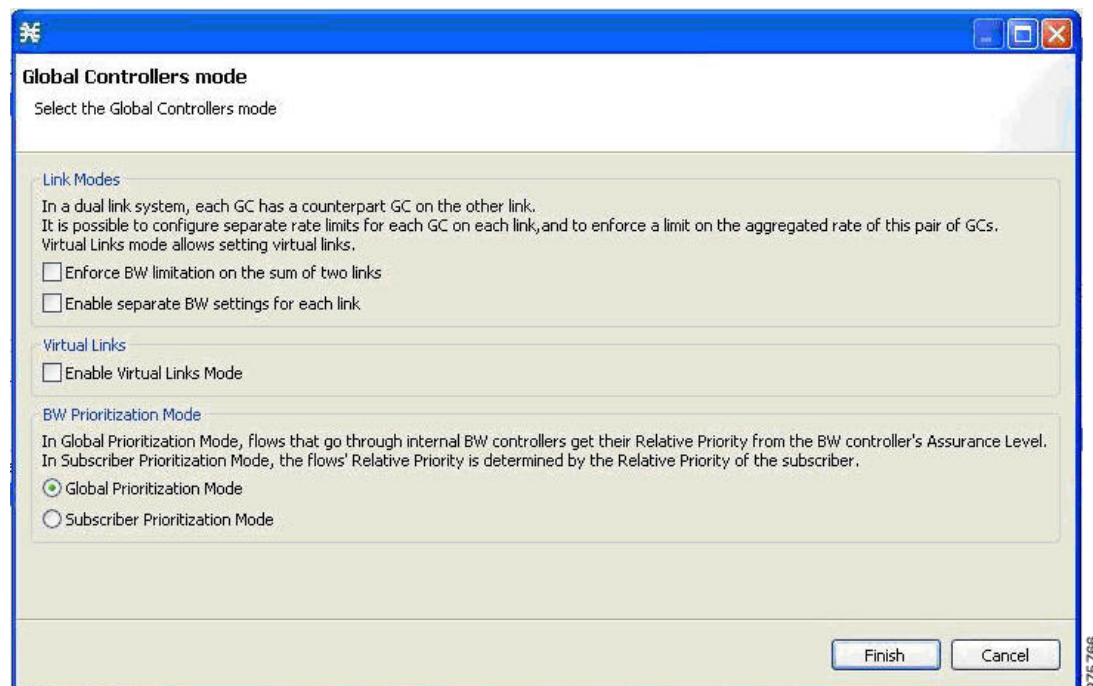
- [How to Set Global Controller Bandwidth Limits with Equal Rate for All Links](#), page 9-13
- [How to Set Global Controller Bandwidth Limits Separately with a Different Rate Per Link](#), page 9-15
- [How to Set Global Controller Bandwidth Limits as the Sum of All Links with an Equal Rate Per Link](#), page 9-18
- [How to Set Global Controller Bandwidth Limits as the Sum of All Links with a Different Rate Per Link](#), page 9-21
- [How to Set Global Controller Bandwidth for Virtual Links](#), page 9-24

How to Set Global Controller Bandwidth Limits with Equal Rate for All Links

Use the following procedure to configure the global controller with equal rate for all links.

- Step 1** In the Policies tab, click **Global Policy**.
The Global Bandwidth Settings dialog box in the right (Rule) pane.
- Step 2** Add global controllers, as described in [How to Add Global Controllers](#), page 9-7.
- Step 3** Click **Edit Preferences**.
The Global Controllers mode dialog box appears ([Figure 9-12](#)).

Figure 9-12 Global Controllers Mode



- Step 4** Verify that the Link Modes check boxes are unchecked.
- Step 5** Click **Finish**.
The Global Controllers mode dialog box closes.


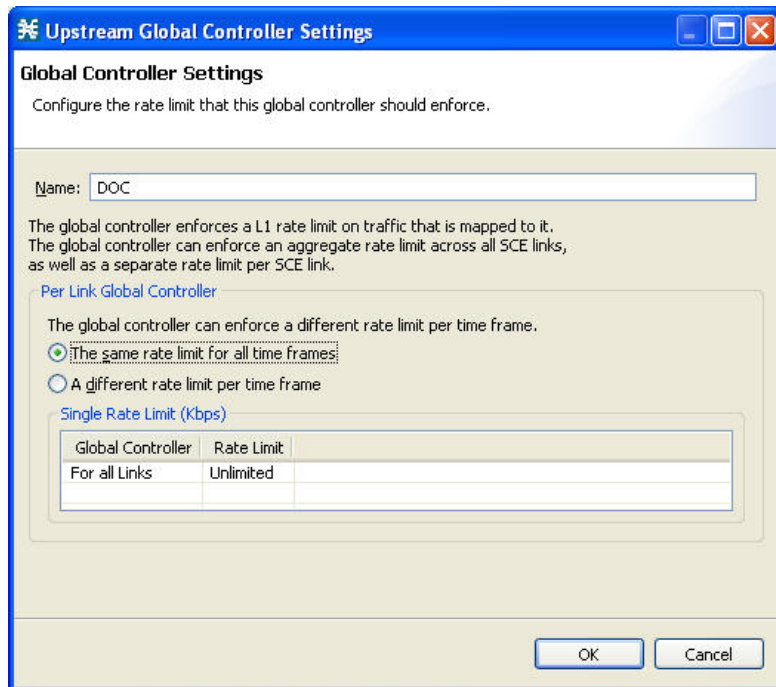
- Step 6** In the Policies tab, click **Global Policy**.
The Global Bandwidth Settings dialog box is displayed in the right (Rule) pane.
- Step 7** Select a global controller.
- Step 8** Click the Edit () icon.
The Global Controller Settings dialog box appears (Figure 9-13).

Figure 9-13 Upstream Global Controller Settings



Note

If the rate limit for all time frames is to be the same, use Step 9. If the rate limit for all time frames is to vary by time frame, use Step 10.

- Step 9** Set a single value for the maximum bandwidth limit that this global controller carries.
- a. Choose the **The same rate limit for all time frames** radio button.
 - b. Enter the desired value in Kbps for the maximum bandwidth in the Rate limit for the Per Link Global Controller (in Kbps) field.

- Step 10** Set the maximum limit that this global controller carries to vary according to time frame.
- Choose the **A different rate limit per time frame** radio button.
 - Enter the desired value for each time frame (Figure 9-14).

Figure 9-14 Upstream Global Controller Settings

Upstream Global Controller Settings

Global Controller Settings
Configure the rate limit that this global controller should enforce.

Name:

The global controller enforces a L1 rate limit on traffic that is mapped to it. The global controller can enforce an aggregate rate limit across all SCE links, as well as a separate rate limit per SCE link.

Per Link Global Controller

The global controller can enforce a different rate limit per time frame.

The same rate limit for all time frames

A different rate limit per time frame

Rate Limit per Time Frame (Kbps)

Global Controller	Time Frame T1	Time Frame T2	Time Frame T3	Time Frame T4
For all Links	Unlimited	Unlimited	Unlimited	Unlimited

OK Cancel

- Step 11** Click **OK**.
Your changes are saved.

How to Set Global Controller Bandwidth Limits Separately with a Different Rate Per Link

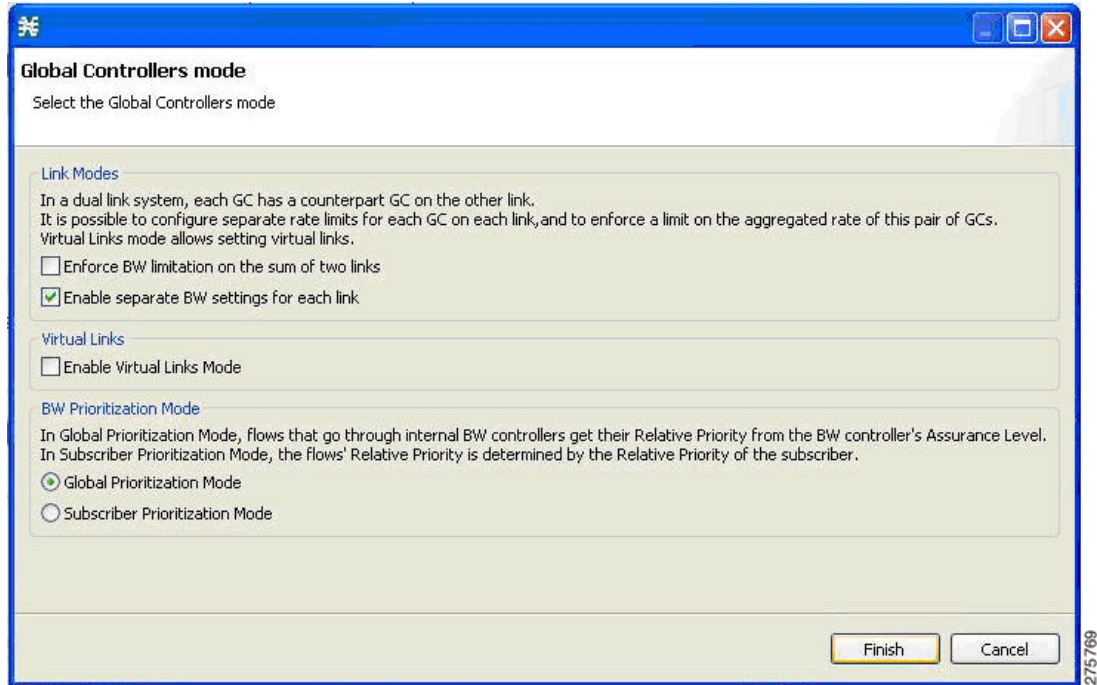
Use the following procedure to configure the global controller with a different rate per link.

- Step 1** In the Policies tab, click **Global Policy**.
The Global Bandwidth Settings dialog box in the right (Rule) pane.
- Step 2** Add global controllers, as described in [How to Add Global Controllers, page 9-7](#).

Step 3 Click **Edit Preferences**.

The Global Controllers mode dialog box appears (Figure 9-15).

Figure 9-15 Global Controller Mode



Step 4 Check the **Enable separate BW setting for each link** check box.

Step 5 Click **Finish**.

The Global Controllers mode dialog box closes.

Step 6 In the Policies tab, click **Global Policy**.

The Global Bandwidth Settings dialog box is displayed in the right (Rule) pane.

Step 7 Select a global controller.


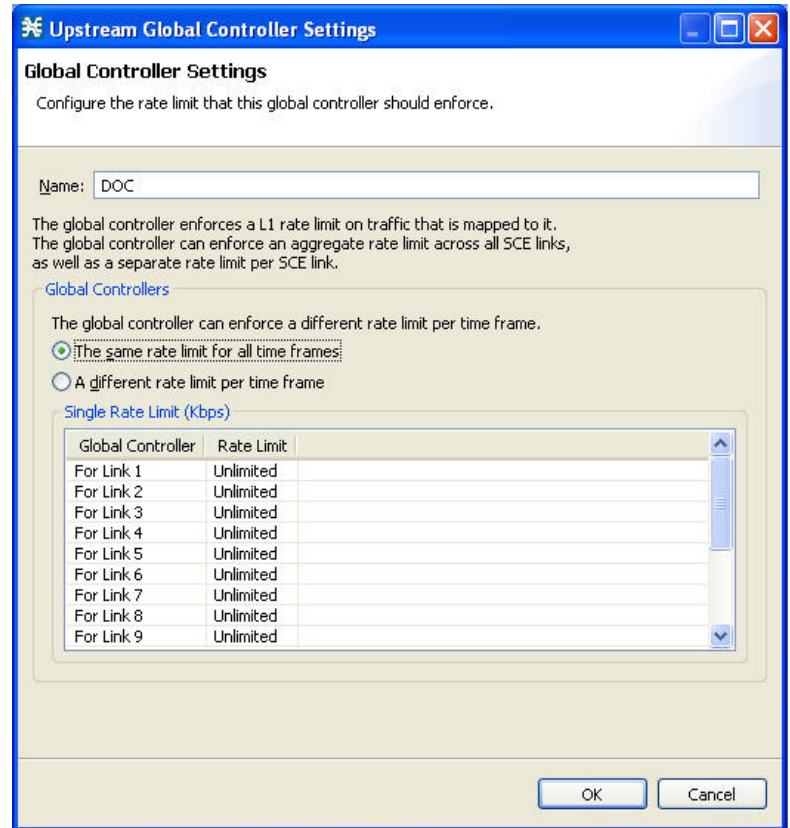
- Step 8** Click the Edit () icon.
The Global Controller Settings dialog box appears (Figure 9-16).

Figure 9-16 Downstream Global Controller Settings



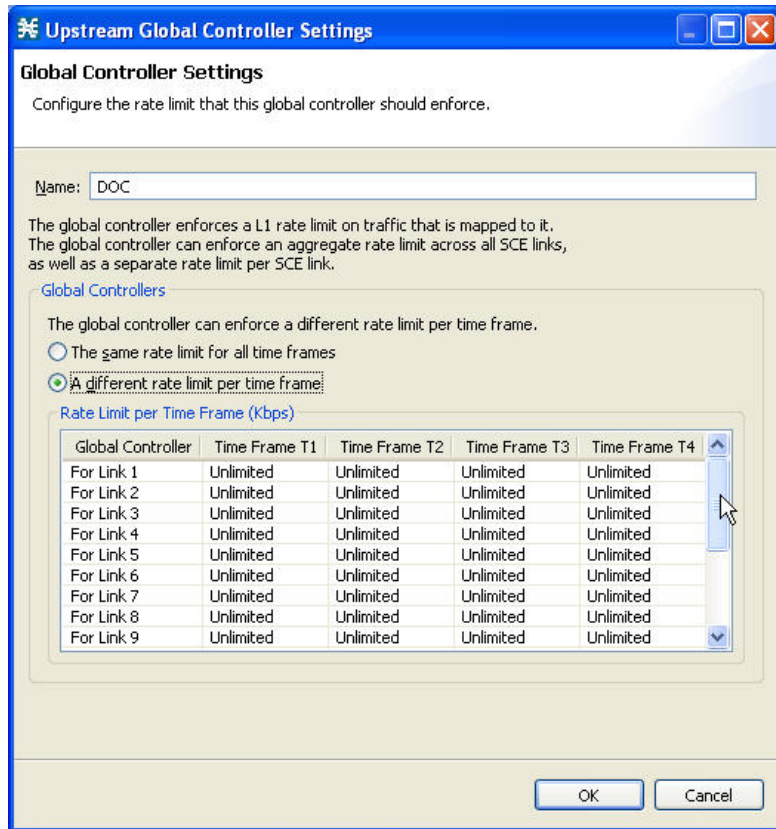
Note

If the rate limit for all time frames is to be the same, use Step 9. If the rate limit for all time frames is to vary by time frame, use Step 10.

- Step 9** Set a single value for the maximum bandwidth limit that this global controller carries for each link.
- a. Choose the **The same rate limit for all time frames** radio button.
 - b. Enter the desired value in Kbps for the maximum bandwidth in the Rate limit for the Per Link Global Controller (in Kbps) field.

- Step 10** Set the maximum limit that this global controller carries to vary according to time frame for each link.
- Choose the **A different rate limit per time frame** radio button.
 - Enter the desired value for each time frame (Figure 9-17).

Figure 9-17 Upstream Global Controller Settings



- Step 11** Click **OK**.
Your changes are saved.

How to Set Global Controller Bandwidth Limits as the Sum of All Links with an Equal Rate Per Link

In this link control mode, the maximum bandwidth limitation is configured as sum of all links. When you create a GC in this mode, you can configure the aggregate global controller of the link and configure the maximum rate per link. In this mode, you can enforce bandwidth limitation on the sum of all links and control the links in aggregate and in addition maximum per-link which is equal between all links.

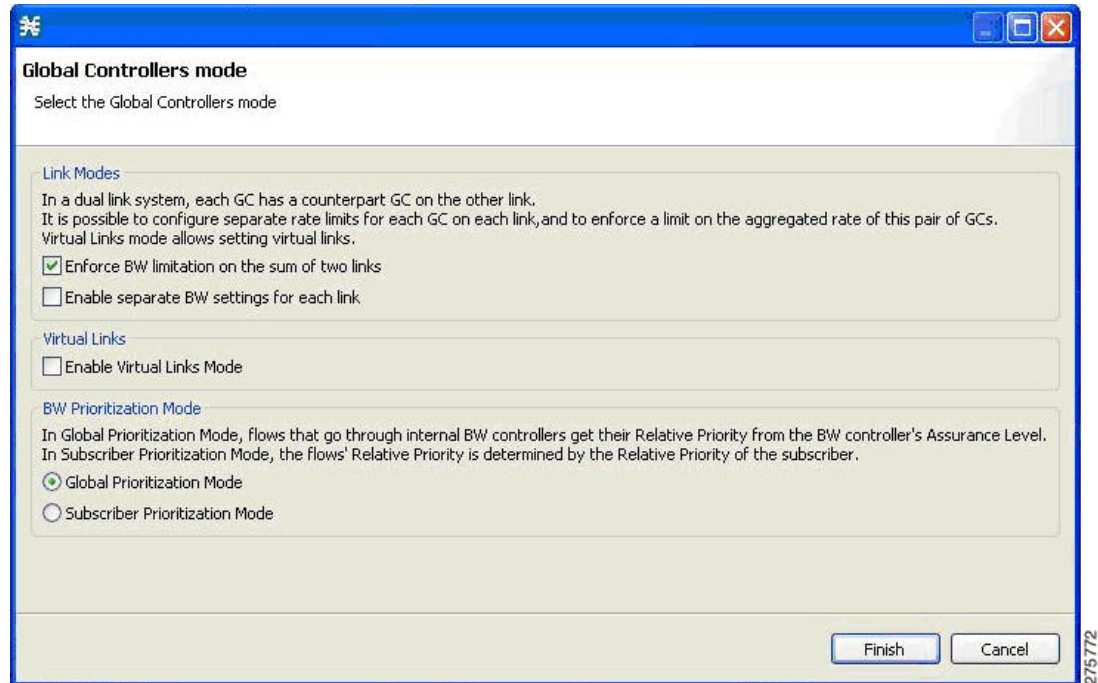
Use the following procedure to configure global controller as the sum of all links with an equal rate per link.

- Step 1** In the Policies tab, click **Global Policy**.
The Global Bandwidth Settings dialog box in the right (Rule) pane.
- Step 2** Add global controllers, as described in [How to Add Global Controllers, page 9-7](#).

Step 3 Click **Edit Preferences**.

The Global Controllers mode dialog box appears (Figure 9-18).

Figure 9-18 Global Controllers Mode



Step 4 Check the **Enforce BW limitation on the sum of the links** check box.


Step 5 Click **Finish**.

The Global Controllers mode dialog box closes.

Step 6 In the Policies tab, click **Global Policy**.

The Global Bandwidth Settings dialog box is displayed in the right (Rule) pane.

Step 7 Select a global controller.

Step 8 Click the Edit () icon.

The Global Controller Settings dialog box appears (Figure 9-19).

Figure 9-19 Upstream Global Controller Settings

Global Controller Settings
Configure the rate limit that this global controller should enforce.

Name:

The global controller enforces a L1 rate limit on traffic that is mapped to it. The global controller can enforce an aggregate rate limit across all SCE links, as well as a separate rate limit per SCE link.

Aggregate Global Controller

The global controller can enforce a different rate limit per time frame.

The same rate limit for all time frames

A different rate limit per time frame

Single Rate Limit (Kbps)

Global Controller	Rate Limit
Aggregate	Unlimited

Per Link Global Controller

The global controller can enforce a different rate limit per time frame.

The same rate limit for all time frames

A different rate limit per time frame

Single Rate Limit (Kbps)

Global Controller	Rate Limit
For all Links	Unlimited

OK Cancel

275773



Note

If the rate limit for all time frames is to be the same, use Step 9. If the rate limit for all time frames is to vary by time frame, use Step 10.

Step 9 Set a single value for the maximum bandwidth limit that this global controller carries.

- a. Choose the **The same rate limit for all time frames** radio button on the Aggregate Global Controller tab.
- b. Enter the desired value in Kbps for the maximum bandwidth in the Rate limit for the Per Link Global Controller (in Kbps) field.

- Step 10** Set the maximum limit that this global controller carries to vary according to time frame.
- Choose the **A different rate limit per time frame** radio button on the Aggregate Global Controller tab.
 - Enter the desired value for each time frame (Figure 9-20).

Figure 9-20 Upstream Global Controller Settings

Upstream Global Controller Settings

Global Controller Settings
Configure the rate limit that this global controller should enforce.

Name: DOC

The global controller enforces a L1 rate limit on traffic that is mapped to it. The global controller can enforce an aggregate rate limit across all SCE links, as well as a separate rate limit per SCE link.

Aggregate Global Controller

The global controller can enforce a different rate limit per time frame.

The same rate limit for all time frames

A different rate limit per time frame

Rate Limit per Time Frame (Kbps)

Global Controller	Time Frame T1	Time Frame T2	Time Frame T3	Time Frame T4
Aggregate	Unlimited	Unlimited	Unlimited	Unlimited

Per Link Global Controller

The global controller can enforce a different rate limit per time frame.

The same rate limit for all time frames

A different rate limit per time frame

Rate Limit per Time Frame (Kbps)

Global Controller	Time Frame T1	Time Frame T2	Time Frame T3	Time Frame T4
For all Links	Unlimited	Unlimited	Unlimited	Unlimited

OK Cancel

- Step 11** Click **OK**.
- Your changes are saved.

How to Set Global Controller Bandwidth Limits as the Sum of All Links with a Different Rate Per Link

In this link control mode, the maximum bandwidth is the sum of links but bandwidth settings can be configured for each link up to the maximum bandwidth for all links. When you create a GC in this mode you can configure the aggregate global controller of the link and in addition specify a bandwidth limitation per link. This mode is used when the Cisco SCE serves multiple edge devices and you want to enforce two rules: One aggregate rule on all the links together and one rule per specific link. In this mode, you can enforce bandwidth limitation on the sum of all links and enable separate bandwidth settings for each link. You can control the links in aggregate and set maximum rate per-link which is different between the links.

Use the following procedure to configure global controller as the sum of all links with a different rate per link.

Step 1 In the Policies tab, click **Global Policy**.

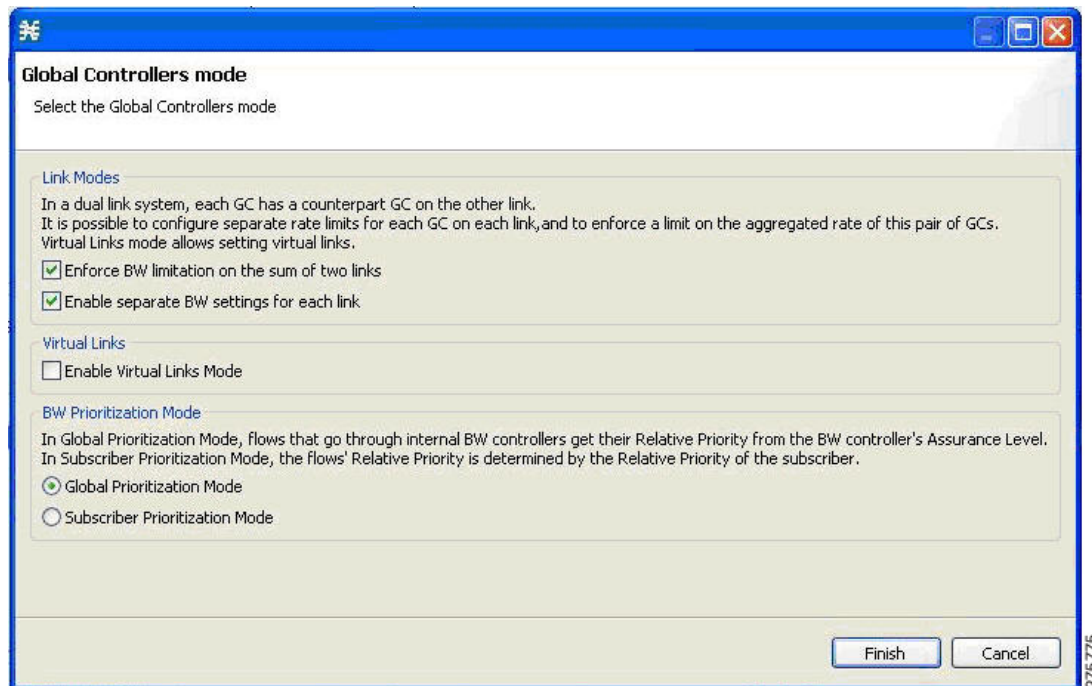
The Global Bandwidth Settings dialog box in the right (Rule) pane.

Step 2 Add global controllers, as described in [How to Add Global Controllers, page 9-7](#).

Step 3 Click **Edit Preferences**.

The Global Controllers mode dialog box appears ([Figure 9-21](#)).

Figure 9-21 Global Controllers Mode



Step 4 Check the **Enforce BW limitation on the sum of the links and Enable separate BW setting for each link** check boxes.

Step 5 Click **Finish**.

The Global Controllers mode dialog box closes.

Step 6 In the Policies tab, click **Global Policy**.

The Global Bandwidth Settings dialog box is displayed in the right (Rule) pane.

Step 7 Select a global controller.


- Step 8** Click the Edit () icon.
The Global Controller Settings dialog box appears (Figure 9-22).

Figure 9-22 Upstream Global Controller Settings

Global Controller Settings
Configure the rate limit that this global controller should enforce.

Name:

The global controller enforces a L1 rate limit on traffic that is mapped to it. The global controller can enforce an aggregate rate limit across all SCE links, as well as a separate rate limit per SCE link.

Aggregate Global Controller
The global controller can enforce a different rate limit per time frame.

The same rate limit for all time frames
 A different rate limit per time frame

Single Rate Limit (Kbps)

Global Controller	Rate Limit
Aggregate	Unlimited

Per Link Global Controller
The global controller can enforce a different rate limit per time frame.

The same rate limit for all time frames
 A different rate limit per time frame

Single Rate Limit (Kbps)

Global Controller	Rate Limit
For Link 1	Unlimited
For Link 2	Unlimited
For Link 3	Unlimited
For Link 4	Unlimited
For Link 5	Unlimited
For Link 6	Unlimited
For Link 7	Unlimited
For Link 8	Unlimited
For Link 9	Unlimited

OK Cancel

275776



Note

If the rate limit for all time frames is to be the same, use Step 9. If the rate limit for all time frames is to vary by time frame, use Step 10.

- Step 9** Set a single value for the maximum bandwidth limit that this global controller carries.
- Choose the **The same rate limit for all time frames** radio button on the Per Link Global Controller tab.
 - Enter the desired value in Kbps for the maximum bandwidth in the Rate limit for the Link 1 (in Kbps) field.
 - Repeat Step 9b for each link.

- Step 10** Set the maximum limit that this global controller carries to vary according to time frame.
- Choose the **A different rate limit per time frame** radio button the Per Link Global Controller tab.
 - Enter the desired value for each time frame.
 - Repeat Step 10b for each link (Figure 9-23).

Figure 9-23 Downstream Global Controller Settings

Upstream Global Controller Settings

Global Controller Settings
Configure the rate limit that this global controller should enforce.

Name:

The global controller enforces a L1 rate limit on traffic that is mapped to it. The global controller can enforce an aggregate rate limit across all SCE links, as well as a separate rate limit per SCE link.

Aggregate Global Controller
The global controller can enforce a different rate limit per time frame.

The same rate limit for all time frames
 A different rate limit per time frame

Rate Limit per Time Frame (Kbps)

Global Controller	Time Frame T1	Time Frame T2	Time Frame T3	Time Frame T4
Aggregate	1024	2048	4096	Unlimited

Per Link Global Controller
The global controller can enforce a different rate limit per time frame.

The same rate limit for all time frames
 A different rate limit per time frame

Rate Limit per Time Frame (Kbps)

Global Controller	Time Frame T1	Time Frame T2	Time Frame T3	Time Frame T4
For all Links	512	2048	1024	512

OK Cancel

249835

- Step 11** Click **OK**.
Your changes are saved.

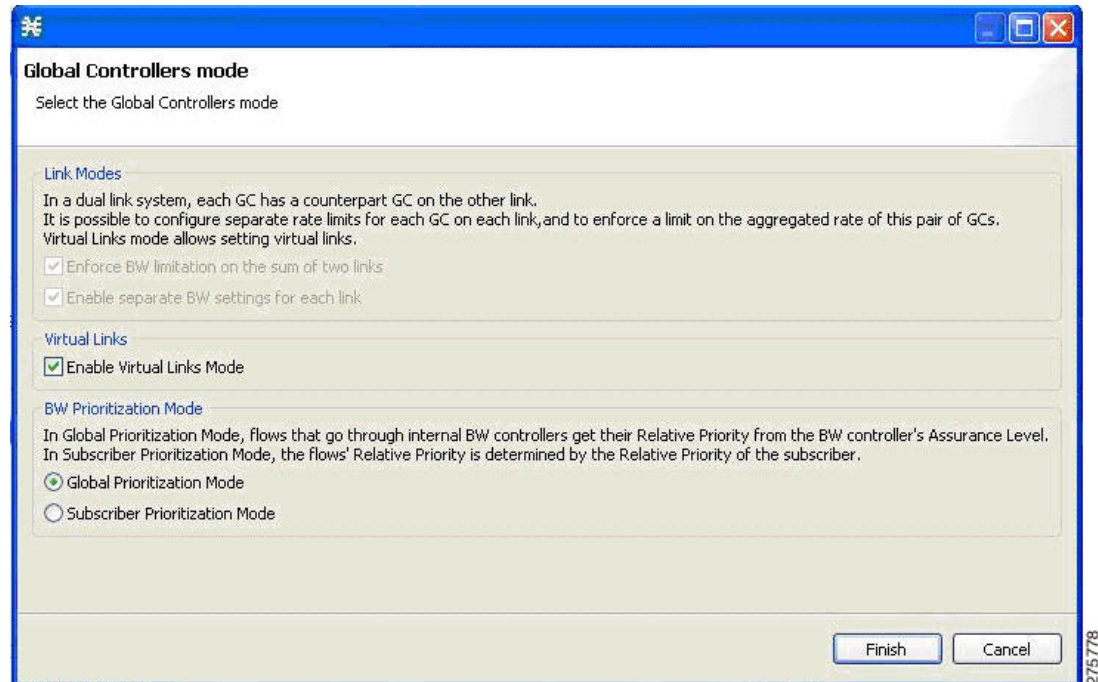
How to Set Global Controller Bandwidth for Virtual Links

In this mode, you can control each link separately using configured rate templates and default rates. The template rate limits are applied to newly created virtual links. The default rate limits are applied to the default virtual link (virtual link 0).

Use the following procedure to configure Global Controller for Virtual links.

- Step 1** In the Policies tab, click **Global Policy**.
The Global Bandwidth Settings dialog box in the right (Rule) pane.
- Step 2** Add global controllers, as described in [How to Add Global Controllers, page 9-7](#).
- Step 3** Click **Edit Preferences**.
The Global Controllers mode dialog box appears ([Figure 9-24](#)).

Figure 9-24 Global Controllers Mode




- Step 4** Check the **Enable Virtual Links Mode** check box.
- Step 5** Click **Finish**.
The Global Controllers mode dialog box closes.



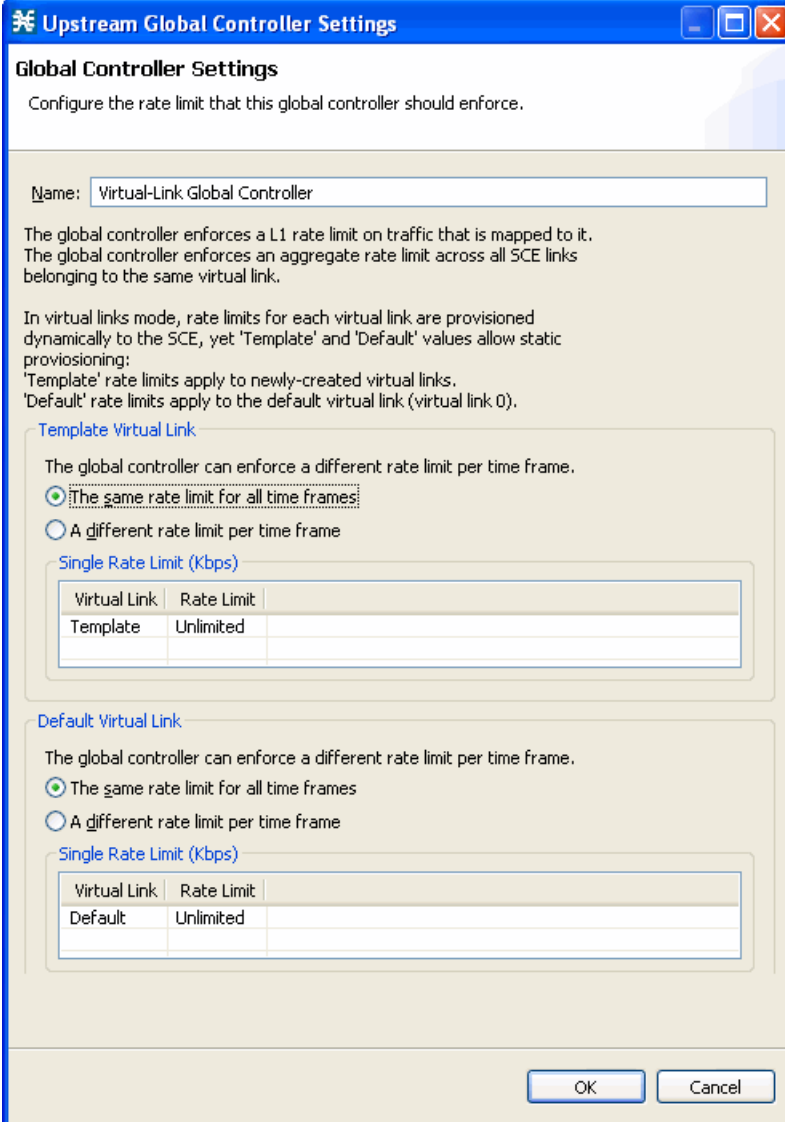
Note By default, the Virtual Link Mode works only in Subscriber Prioritization Mode.

- Step 6** In the Policies tab, click **Global Policy**.
The Global Bandwidth Settings dialog box is displayed in the right (Rule) pane.
- Step 7** Select a global controller.

Step 8 Click  (**Edit**).

The Global Controller Settings dialog box appears (Figure 9-25).

Figure 9-25 Upstream Global Controller Settings



Global Controller Settings

Configure the rate limit that this global controller should enforce.

Name: Virtual-Link Global Controller

The global controller enforces a L1 rate limit on traffic that is mapped to it. The global controller enforces an aggregate rate limit across all SCE links belonging to the same virtual link.

In virtual links mode, rate limits for each virtual link are provisioned dynamically to the SCE, yet 'Template' and 'Default' values allow static provisioning:
 'Template' rate limits apply to newly-created virtual links.
 'Default' rate limits apply to the default virtual link (virtual link 0).

Template Virtual Link

The global controller can enforce a different rate limit per time frame.

The same rate limit for all time frames
 A different rate limit per time frame

Single Rate Limit (Kbps)

Virtual Link	Rate Limit
Template	Unlimited

Default Virtual Link

The global controller can enforce a different rate limit per time frame.

The same rate limit for all time frames
 A different rate limit per time frame

Single Rate Limit (Kbps)

Virtual Link	Rate Limit
Default	Unlimited

OK Cancel



Note

If the rate limit for all time frames is to be the same for the Template Virtual Link, use Step 9. If the rate limit for all time frames is to vary by time frame for the Template Virtual Link, use Step 10.

Step 9 Set a single value for the maximum bandwidth limit that this global controller carries.

- a. Choose the **The same rate limit for all time frames** radio button on the Template Virtual Link tab.
- b. Enter the desired value in Kbps for the maximum bandwidth in the Rate limit for the Link 1 (in Kbps) field.

- Step 10** Set the maximum limit that this global controller carries to vary according to time frame.
- a. Choose the **A different rate limit per time frame** radio button on the Template Virtual Link tab.
 - b. Enter the desired value for each time frame.



Note If the rate limit for all time frames is to be the same for the Default Virtual Link, use Step 11. If the rate limit for all time frames is to vary by time frame for the Default Virtual Link, use Step 12.

- Step 11** Set a single value for the maximum bandwidth limit that this global controller carries.
- a. Choose the **The same rate limit for all time frames** radio button on the Default Virtual Link tab.
 - b. Enter the desired value in Kbps for the maximum bandwidth in the Rate limit for the Link 1 (in Kbps) field.

- Step 12** Set the maximum limit that this global controller carries to vary according to time frame.
- Choose the **A different rate limit per time frame** radio button the Default Virtual Link tab.
 - Enter the desired value for each time frame (Figure 9-26).

Figure 9-26 Upstream Global Controller Settings

Global Controller Settings
Configure the rate limit that this global controller should enforce.

Name:

The global controller enforces a L1 rate limit on traffic that is mapped to it. The global controller can enforce an aggregate rate limit across all SCE links, as well as a separate rate limit per SCE link.

Aggregate Global Controller

The global controller can enforce a different rate limit per time frame.

The same rate limit for all time frames

A different rate limit per time frame

Rate Limit per Time Frame (Kbps)

Global Controller	Time Frame T1	Time Frame T2	Time Frame T3	Time Frame T4
Aggregate	1024	2048	Unlimited	4096

Per Link Global Controller

The global controller can enforce a different rate limit per time frame.

The same rate limit for all time frames

A different rate limit per time frame

Rate Limit per Time Frame (Kbps)

Global Controller	Time Frame T1	Time Frame T2	Time Frame T3	Time Frame T4
For Link 1	1024	256	Unlimited	2048
For Link 2	Unlimited	248	512	124
For Link 3	Unlimited	Unlimited	1024	Unlimited
For Link 4	512	1024	Unlimited	Unlimited
For Link 5	Unlimited	Unlimited	1024	Unlimited
For Link 6	Unlimited	Unlimited	Unlimited	Unlimited
For Link 7	Unlimited	Unlimited	Unlimited	Unlimited
For Link 8	Unlimited	Unlimited	1024	Unlimited

OK Cancel

- Step 13** Click **OK**.
Your changes are saved.

243843

Managing Subscriber Bandwidth

After you have defined global controllers, you can add subscriber BWCs to packages and map these subscriber BWCs to different global controllers.

A Subscriber BWC controls subscriber bandwidth consumption for upstream or downstream flows. It controls and measures the bandwidth of an aggregation of traffic flows of a service or group of services.

Each package has its own set of BWCs that determine the bandwidth available per package subscriber for each available service.

The two Primary BWCs, one for upstream traffic and one for downstream traffic, allocate bandwidth to specific subscribers. Bandwidth is allocated based on the Committed Information Rate (CIR), the Peak Information Rate (PIR), and the Subscriber relative priority settings. You can configure these parameters, but the Primary BWCs cannot be deleted.

There are two default BWCs, one for upstream traffic and one for downstream traffic. By default, all services are mapped to one of these two BWCs. The BWC mechanism controls rate subpartitioning within the default BWC rate control, based on the CIR, PIR, and AL. You can configure these parameters, but the default BWCs cannot be deleted.

You can add up to 32 user-defined BWCs per package:

- Subscriber BWCs operate at the service-per-subscriber level. They allocate bandwidth for services for each subscriber, based upon the CIR, PIR, global controller, and Assurance Level (AL) set for the BWC. Each rule defines a link between the flow of the service and one of the BWCs (unless the flows are to be blocked). See [“How to Define Per-Flow Actions for a Rule” section on page 9-66](#).
- Extra BWCs also operate at the subscriber level. Extra BWCs (based on the CIR, PIR, global controller, and AL) can be allocated for services that are not included in the Primary BWC. These are services that are not often used but have strict bandwidth requirements, for example, video conference calls. The Extra BWCs are BWCs that control a single service (or service group). BWCs cannot borrow bandwidth from Extra BWCs and vice versa.

Each user-defined BWC controls either downstream or upstream traffic.



Caution

If you enable or disable Virtual Links mode, all user-defined global controllers are deleted from the service configuration. A BWC that pointed to a user-defined global controller now points to the default global controller. Other parameters of these BWCs remain unchanged.

The Cisco SCE supports a maximum of 2000 BWCs. You cannot apply a PQB file to a Cisco SCE if the file contains more than 2000 BWCs. But, the Subscriber BWCs with same values for GC Index, AL Level, PIR, and CIR are considered as a single BWC; even if the BWCs are mapped to different flows. So, in effect, Cisco SCA BB may support more than 2000 BWCs.

- [Subscriber BWC Parameters, page 9-29](#)
- [How to Edit Package Subscriber BWCs, page 9-30](#)

Subscriber BWC Parameters

The Subscriber BW Controllers tab of the Package Settings dialog box has the following configuration parameters:

- Name—A unique name for each BWC.
- CIR (L3 Kbps)—The minimum bandwidth that must be granted to traffic controlled by the BWC.

- PIR (L3 Kbps)—The maximum bandwidth allowed to traffic controlled by the BWC.

**Note**

The minimum bandwidth for a subscriber BWC is 16 Kbps with a granularity of 1 Kbps and the maximum bandwidth is 500000 Kbps.

- Global Controller—The global controller with which this BWC is associated. The global controllers are virtual queues that are part of the bandwidth control mechanism. Direct traffic with similar bandwidth control properties to the same global controller.
- Assurance Level—How fast bandwidth either decreases from the PIR to the CIR as congestion builds or else increases from the CIR to the PIR as congestion decreases. A higher AL ensures a higher bandwidth compared to a similar BWC with a lower AL. The lowest assurance value is 1, the highest is Persistent (10).


Assurance Level 10 (persistent) never goes below the relevant CIR, unless the total line rate cannot sustain this value.

- Subscriber relative priority—Assurance Level given to the Primary BWC of the subscriber. It determines the assurance given to all the subscriber traffic when competing for bandwidth with subscribers to other packages. The lowest value is 1; the highest is 10.

**Note**

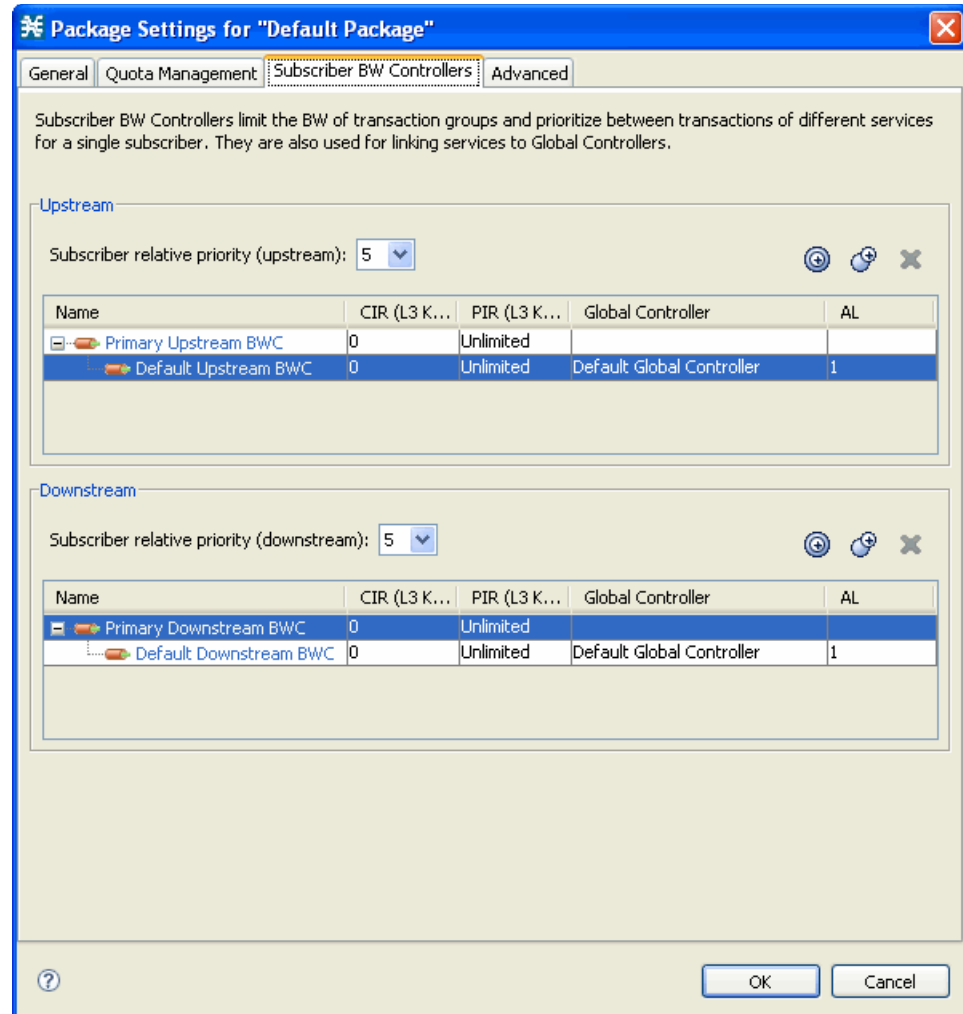
Subscriber bandwidth control (and accounting and reporting) is based on Layer 3 volume. Global controller bandwidth is based on Layer 1 volume.

How to Edit Package Subscriber BWCs

-
- Step 1** In the Policies tab, click **Global Policy**.
The Global Bandwidth Settings dialog box in the right (Rule) pane.
- Step 2** In the right (Rule) pane, select a BWC and click the Edit () icon.
The Package Settings dialog box appears.

- Step 3** In the Package Settings dialog box, click the **Subscriber BW Controllers** tab. The Subscriber BW Controllers tab opens (Figure 9-27).

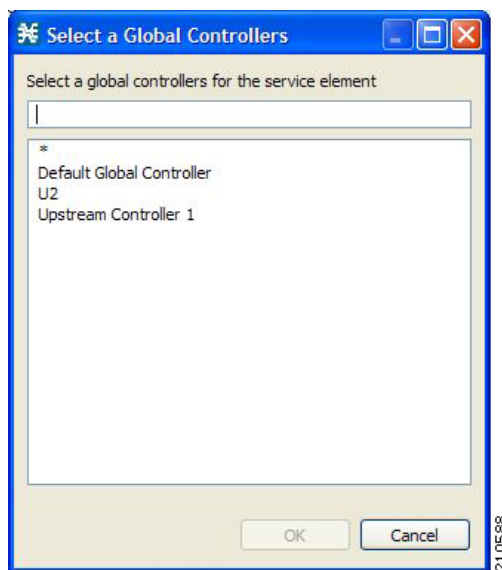
Figure 9-27 Subscriber BW Controllers Tab



- Step 4** Set your requirements for upstream bandwidth control in the Upstream area of the dialog box.
- Select a value from the Subscriber relative priority drop-down list.
 - Set the parameters for the Primary Upstream BWC.
 - In the CIR field, enter the BWC CIR in Kbps.
 - In the PIR field, select **Unlimited** from the drop-down list, or enter the BWC PIR in Kbps.
 - To add BWCs to the package, click the **Add a sub BW Controller** (+) icon once for each additional BWC.
 - To add Extra BWCs to the package, click the **Add an extra BW Controller** (+) icon once for each additional BWC.

- e. Set the parameters for each BWC (including the Primary and Default BWCs).
 - (Optional) In the Name field, enter a meaningful name for each BWC. (You cannot rename the Primary or Default BWCs.)
 - In the CIR field, enter a value for the BWC CIR in Kbps.
 - In the PIR field, select **Unlimited** from the drop-down list, or enter a value for the BWC PIR in Kbps.
 - To set the global controller, with which this BWC is associated:
Click in the Global Controller cell of the BWC, and then click the **Browse** button that appears.
The Select a Global Controller dialog box appears (Figure 9-28).

Figure 9-28 **Select a Global Controller**



- Select a global controller and click **OK**.
- Select a value from the AL drop-down list.

Step 5 Repeat Step 3 for downstream bandwidth control in the Downstream area of the dialog box.

Step 6 Click **OK**.

The Package Settings dialog box closes.

All changes to the BWC settings are saved.

The effect of Assurance Level on bandwidth allocation for subscriber BWCs will be as follows:

If there are 4 BWCs namely “Priority”, “Gold”, “Silver” and “default” with Assurance Levels 9, 6, 3 and 1 respectively, the “priority” BWC gets the bandwidth first, followed by the “Gold” and the “Silver” BWC. The “default” BWC will be the last to get the bandwidth.

Managing Bandwidth: A Practical Example

This section explains how to achieve effective bandwidth control by combining the configuration of global controllers and subscriber BWCs, and gives a practical example.

- [How to Configure Total Bandwidth Control, page 9-33](#)
- [Example: How to Limit P2P and Streaming Traffic Using the Console, page 9-33](#)

How to Configure Total Bandwidth Control

-
- Step 1** Configure the necessary global controllers.
- Ascertain which services are likely to be problematic, and what the maximum total bandwidth should be for each. You do not need to configure services and packages that are unlikely to be problematic; you can include them in the default global controllers.
- Step 2** Configure the subscriber BWCs for the package.
- a. Add a subscriber BWC for each type of upstream or downstream traffic that you want to limit, and configure the CIR and the PIR accordingly.
 - b. Select an appropriate global controller for each subscriber BWC.
- Step 3** For each service that is to have its own BWC, create a rule and select appropriate upstream and downstream BWCs.
-

Example: How to Limit P2P and Streaming Traffic Using the Console

**Note**

This example assumes that the traffic flow is bidirectional; you may decide that you only need upstream controllers or downstream controllers.

**Note**

The P2P Traffic Optimization wizards allow you to create a simple model of devices, connect to them, and limit P2P traffic to a specified bandwidth. (See [“How to Use the P2P Traffic Optimization Wizards” section on page 4-45.](#))

- Step 1** In the Policies tab, click **Global Policy**.
- The Global Bandwidth Settings dialog box in the right (Rule) pane.
- Step 2** Add two upstream global controllers and two downstream global controllers and assign the desired bandwidth to each global controller ([Figure 9-29](#)).

Figure 9-29 Global Bandwidth Settings

Global Upstream Policy

Total Link Limit: Link 1: Unlimited

Upstream	Policy Description
Upstream Global Controller 2	Link Bandwidth Limit: 4.0 Mbps
Upstream Global Controller 1	Link Bandwidth Limit: 3.0 Mbps
Default Global Controller	Link Bandwidth Limit: Unlimited

Global Downstream Policy

Total Link Limit: Link 1: Unlimited

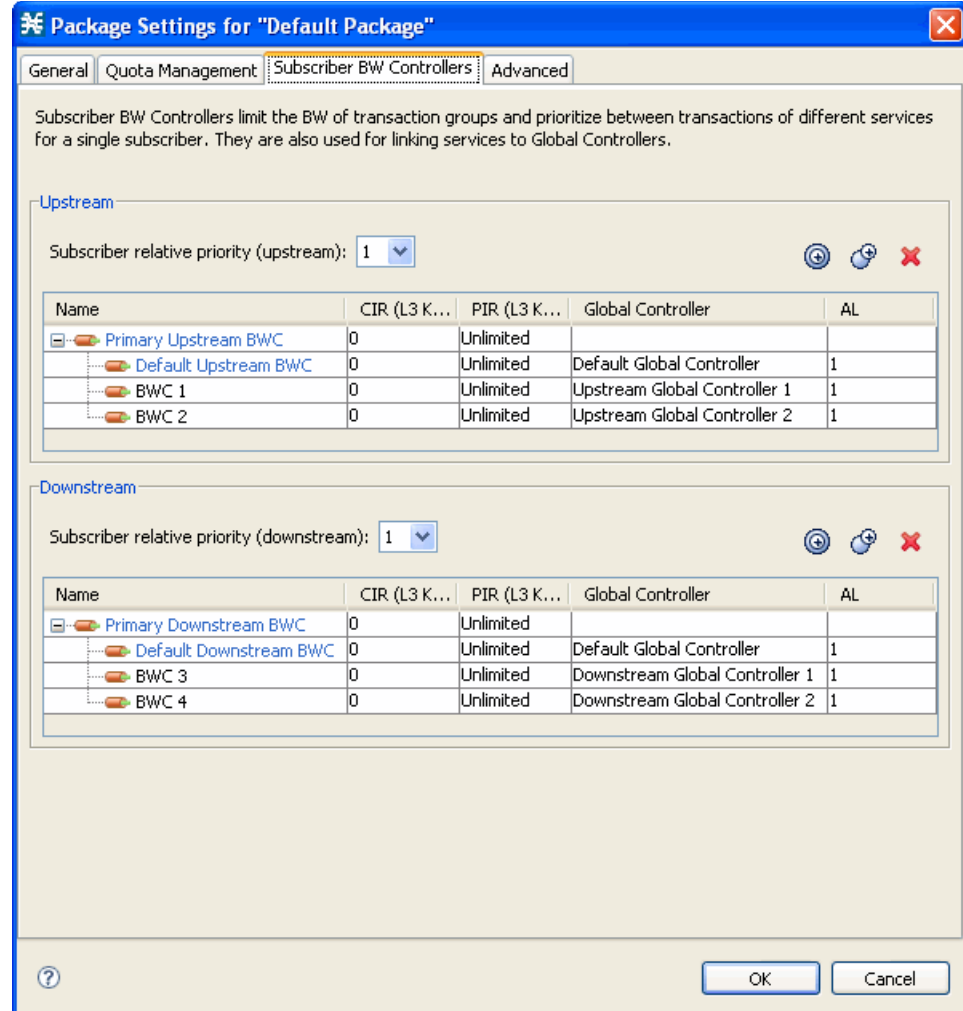
Downstream	Policy Description
Downstream Global Controller 2	Link Bandwidth Limit: 6.0 Mbps
Downstream Global Controller 1	Link Bandwidth Limit: 2.0 Mbps
Default Global Controller	Link Bandwidth Limit: Unlimited

274076

(Here, Upstream Controller 1 and Downstream Controller 1 is used for P2P traffic, and Upstream Controller 2 and Downstream Controller 2 is used for streaming traffic.)

- Step 3** In a Package Settings dialog box (Figure 9-30), add two upstream BWCs and two downstream BWCs, map them to the appropriate global controllers, and set their parameters (CIR, PIR, AL).

Figure 9-30 Package Settings



(Here, BWC1 is for upstream P2P traffic and BWC3 is for downstream P2P traffic; BWC2 is for upstream streaming traffic and BWC4 is for downstream streaming traffic.)

Step 4 Add a rule for the P2P service (Figure 9-31).

Figure 9-31 Add New Rule to Package

The screenshot shows a dialog box titled "Add New Rule to Package 'Gold'". It has four tabs: "General", "Control", "Usage Limits", and "Breach Handling". The "General" tab is selected. Inside the dialog, there are two main sections:

- Service:** A section with the text "Select the Service to which the Rule will relate:" followed by a dropdown menu. The dropdown menu is currently set to "P2P".
- Rule State:** A section with the text "Define the state of this Rule:" followed by two radio button options:
 - Enable reporting and active actions
 - Disable reporting and active actions

At the bottom right of the dialog, there are "OK" and "Cancel" buttons. A small vertical number "274075" is visible on the right edge of the dialog box.

- Step 5** In the Control tab (Figure 9-32), assign BWC 1 as the upstream BWC and BWC 3 as the downstream BWC.

Figure 9-32 Control Tab

The screenshot shows the 'Add New Rule to Package "Default Package"' dialog box with the 'Control' tab selected. The 'Control' tab is active, and the 'Control the flow's characteristics' radio button is selected. The configuration options are as follows:

- Block the flow
- Control the flow's characteristics:
 - Select an upstream Bandwidth Controller: BWC 1
 - Select a downstream Bandwidth Controller: BWC 3
 - Limit the flow's upstream bandwidth to [] kbps
 - Limit the flow's downstream bandwidth to [] kbps
 - Set the flow's upstream packets ToS (DSCP) to ToS 1 [0]
 - Set the flow's downstream packets ToS (DSCP) to ToS 1 [0]
 - Limit concurrent flows of this Service to []
 - Set CoS for flows of this Service to BE
 - Redirect profile for this service: []
 - Mirror traffic to server group: Server Group 0

Buttons for '?', 'OK', and 'Cancel' are visible at the bottom. A vertical number '274128' is on the right side of the dialog box.

- Step 6** Repeat Step 4 and Step 5 for the Streaming service, using BWC 2 as the upstream BWC and BWC 4 as the downstream BWC.

All subscriber traffic using these services are added to the virtual queue total for these queues. In turn, the bandwidth available to the subscriber for these protocols fluctuate, depending on how “full” these queues are.

Step 7 Click Global Policy to view the hierarchy of the GCs, BWCs, and rules (Figure 9-33).

Figure 9-33 Rule Hierarchy

The screenshot displays the 'Global Policy' configuration interface, divided into 'Global Upstream Policy' and 'Global Downstream Policy' sections. Each section shows a tree view of policy elements and a corresponding table of policy descriptions.

Global Upstream Policy

Upstream	Policy Description
Upstream Global Controller 2	Aggregated Bandwidth Limit: Unlimited ; Link Bandwidth Limit: ...
BWC 2	Low Priority [CIR:0 Kbps; PIR:Unlimited; AL:1]
Upstream Global Controller 1	Aggregated Bandwidth Limit: Unlimited ; Link Bandwidth Limit: ...
BWC 1	Low Priority [CIR:0 Kbps; PIR:Unlimited; AL:1]
P2P Rule under Default Package	controlled ; unlimited quota
Default Global Controller	Aggregated Bandwidth Limit: Unlimited ; Link Bandwidth Limit: ...
Default Upstream BWC	Low Priority [CIR:0 Kbps; PIR:Unlimited; AL:1]

Global Downstream Policy

Downstream	Policy Description
Downstream Global Controller 2	Aggregated Bandwidth Limit: Unlimited ; Link Bandwidth Limit: ...
BWC 4	Low Priority [CIR:0 Kbps; PIR:Unlimited; AL:1]
Downstream Global Controller 1	Aggregated Bandwidth Limit: Unlimited ; Link Bandwidth Limit: ...
BWC 3	Low Priority [CIR:0 Kbps; PIR:Unlimited; AL:1]
P2P Rule under Default Package	controlled ; unlimited quota
Default Global Controller	Aggregated Bandwidth Limit: Unlimited ; Link Bandwidth Limit: ...
Default Downstream BWC	Low Priority [CIR:0 Kbps; PIR:Unlimited; AL:1]

At the bottom, there are sections for 'Global Policy Preferences' (with an 'Edit Preferences...' button) and 'Display Filter' (with a 'Configure Filters...' button).

How to Configure a Rule, Bandwidth Controller, and Global Controller Using the Wizard

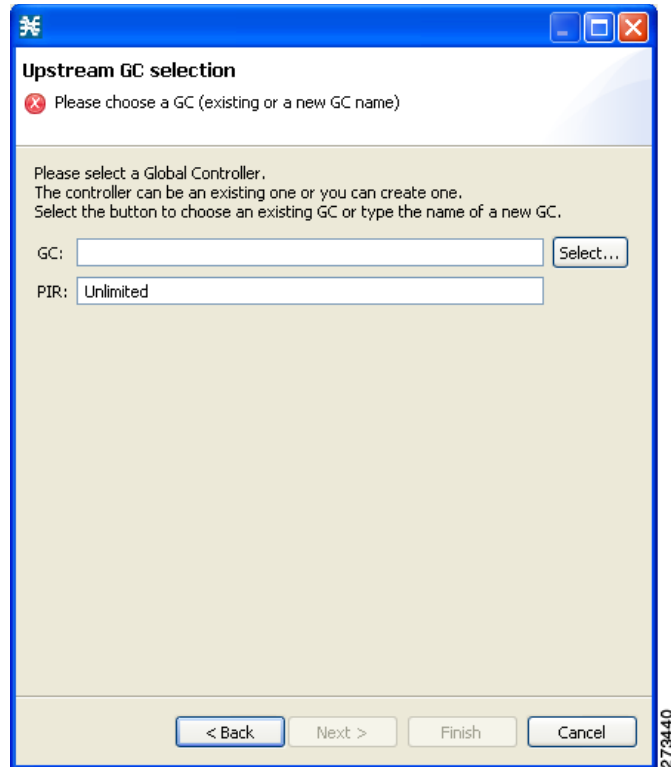
You can configure a rule, BWC, and GC together from the Global Policy window.

-
- Step 1** In the Policies tab, click **Global Policy**.
The Global Bandwidth Settings are displayed in the right (Rule) pane.
- Step 2** Above the area (Upstream or Downstream) of the desired interface, click the **Add** (+) icon.
The Select addition mode dialog box appears.
- Step 3** Choose the **Add a Global Controller and map a Rule and BWC to it** radio button.

Step 4 Click **Finish**.

The GC Selection dialog box appears (Figure 9-34).

Figure 9-34 Upstream GC Selection



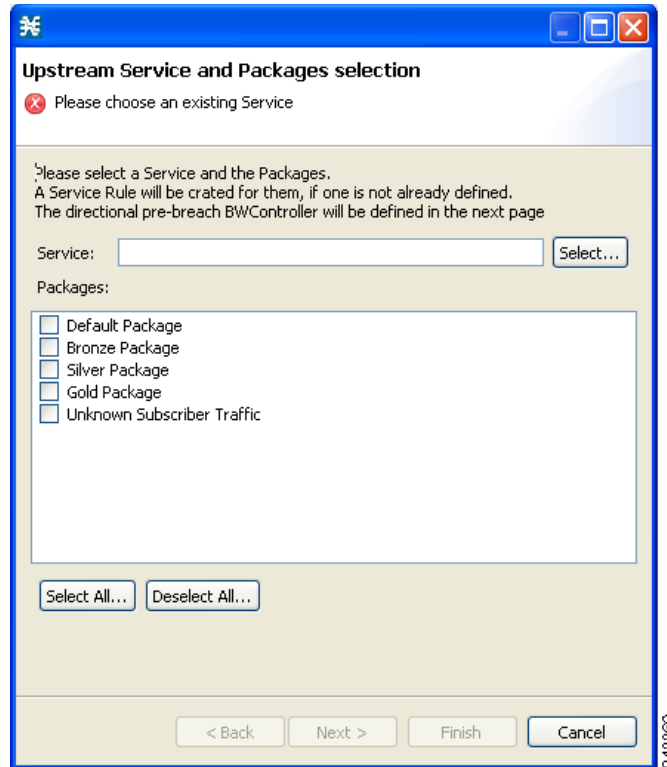
Step 5 In the GC field, enter a new GC name, or click **Select** to choose an existing GC.

Step 6 (Optional) In the PIR field, enter the maximum bandwidth limit that this global controller carries in Kbps.

Step 7 Click **Next**.

The Service and Packages selection dialog box appears (Figure 9-35).

Figure 9-35 Upstream Service and Packages Selection



Step 8 In the Service field, select an existing service.

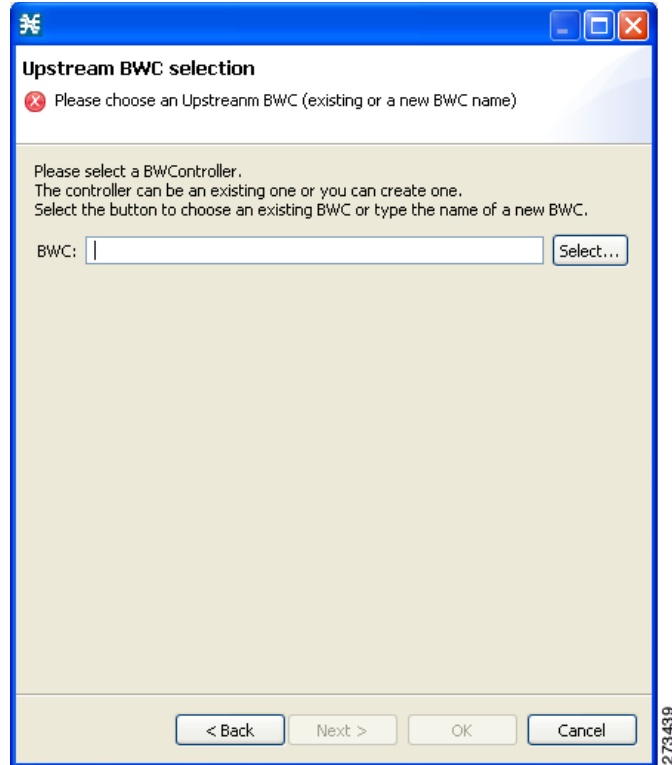
Step 9 In the Packages section, select one or more packages for the rule to apply to.

If a rule does not exist for the service, it is created. The new, or existing rule is then mapped to the selected package or packages.

Step 10 Click **Next**.

The BWC selection dialog box appears (Figure 9-36).

Figure 9-36 Upstream BWC Selection




Step 11 Enter a new BWC name, or click **Select** to choose an existing BWC.

Step 12 Click **OK**.

How to Configure the Upstream Configuration of the Global Bandwidth Controller for IPv6

You can configure the upstream configuration of the global bandwidth controller for IPv6 from the Global Policy window. For details on managing the bandwidth, see the “[Managing Bandwidth](#)” section on page 9-2. Perform the following procedures:

-
- Step 1** In the Service Configuration Editor window, click the **Policies** tab.
- Step 2** Under the Policies tab, click **Global Policy**.
The Global Bandwidth Settings dialog box is displayed in the right (Rule) pane.
- Step 3** Above the area (Upstream or Downstream) of the corresponding interface, click the **Add** () icon.
The Select Addition mode dialog box is displayed.
- Step 4** Click the **Add a Global Controller and map a Rule and a BWC to it** radio button to add a global controller with a rule mapped to it and a BWC added to it.
- Step 5** Select an existing global controller by clicking the **Select** button or create a new global controller by typing the name of a global controller.
- Step 6** Enter the PIR value and click **Next**.
- Step 7** Select the service to control and check the Unknown Subscriber Package check box and Click **Next**.
- Step 8** Select an existing BWC by clicking the **Select** button or create a new BWC by typing the name of the BWC. Click **Next**.
- Step 9** Double-click on the unknown subscriber package to verify the bandwidth controller and the global controller association.
Follow the same procedure for the downstream configuration of the global bandwidth controller for IPv6.

How to Set BW Management Prioritization Mode

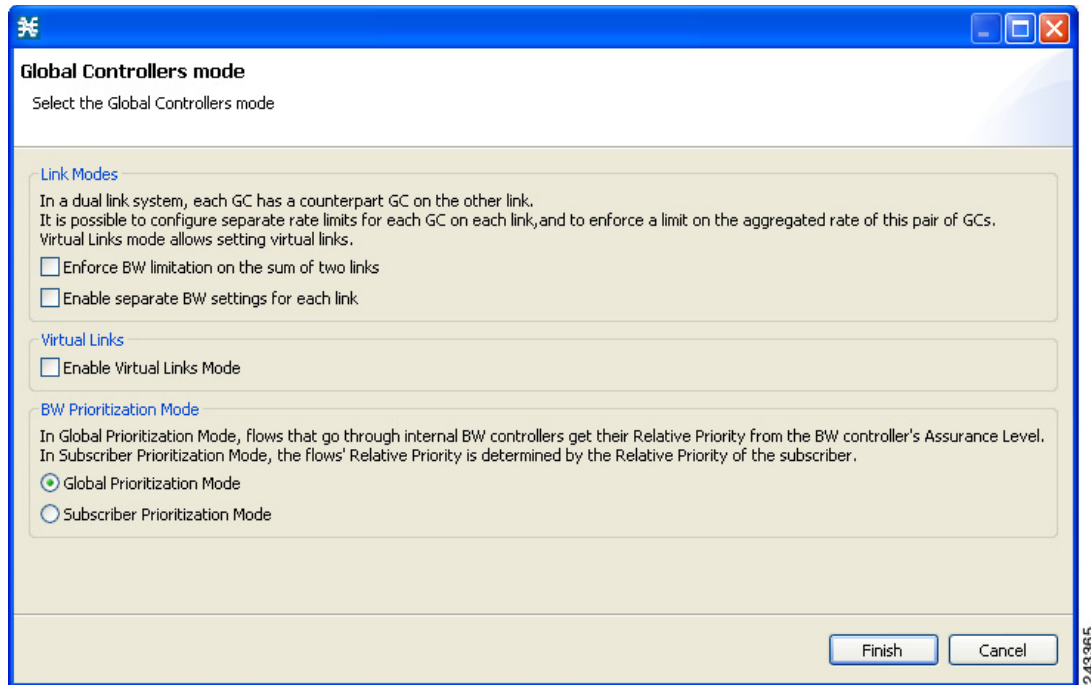
Relative priority is the level of assurance that an internal BWC (iBWC) receives when competing against other iBWCs for bandwidth.

The relative priority of one of the following modes determines the relative priority of the flow that goes through an iBWC:

- The iBWC—In Global Prioritization Mode
- The subscriber—In Subscriber Prioritization Mode

- Step 1** In the Policies tab, click **Global Policy**.
The Global Bandwidth Settings are displayed in the right (Rule) pane.
- Step 2** Click **Edit Preferences**.
The Global Controllers mode dialog box appears (Figure 9-37).

Figure 9-37 Global Controllers Mode



- Step 3** Select one of the **BW Prioritization Mode** radio buttons.
- **Global Prioritization Mode**
 - **Subscriber Prioritization Mode**
- Step 4** Click **OK**.
The Global Controllers mode dialog box closes.
The selected BW management parameter is saved.

Managing Virtual Links

In Virtual Links mode, template bandwidth controllers are defined for packages. Actual bandwidth parameters are assigned when a subscriber enters the system. This bandwidth depends on the package of the subscriber and the physical link assigned to the subscriber. The package of the subscriber defines the template controllers.

For each service configuration that has Virtual Links mode enabled, there is one default upstream virtual link and one default downstream virtual link. The upstream and downstream interfaces are each assigned one default template global controller.

You can add additional template global controllers. You can add, modify, and delete virtual links using a command-line interface (CLI).

The number of directional template global controllers limits the maximum number of virtual links. The number of template global controllers times the number of virtual links cannot exceed 1024 or 4096. Based on the Cisco SCE hardware, the number of global controllers varies. For details, see the [“Managing Bandwidth” section on page 9-2](#).

To support the DOCSIS 3.0 Downstream bonding, a two level virtual link hierarchy is created for the wideband channels. The wideband channels are associated with the Aggregate Global Control (AGC) that provides a constant output signal despite variations in input signal strength. Wideband channels are associated with three AGCs in a two level hierarchy. At the lower level of the hierarchy, all the DOCSIS 3.0 modems for wideband are aggregated into one AGC and the other AGC contains both legacy and 3.0 modems. The AGC at the top level of the hierarchy is used to limit the aggregated bandwidth of the wideband channel.

For more information on the support for DOCSIS 3.0 solution, see the *Cisco Service Control for Managing Remote Cable MSO Links Solution Guide*.

For more information on managing the virtual links global controllers, see [“Managing Virtual Links Global Controllers” section on page 9-48](#).



Caution

If you enable or disable Virtual Links mode, all user-defined global controllers are deleted from the service configuration. A subscriber BWC that pointed to a user-defined global controller now points to the default global controller. (Other parameters of these subscriber BWCs remain unchanged.)



Note

While applying a policy in virtual link mode, if the new template includes a different number of global controllers than the currently applied template, you must choose the Reset all Virtual Links to Template Rate Limits. Otherwise, selecting apply results in an error message, similar to the following:

“Template Upstream Virtual Link differ from the one in the SCE - cannot apply without the force template virtual link option.”

The following steps outline configuring a service configuration in Virtual Links mode. The procedure is similar to that for configuring any service configuration, but virtual links must be added using the CLI.

1. Create a new service configuration.
2. Open the Global Bandwidth Settings dialog box and check the Enable Virtual Links Mode check box.
3. Create template global controllers.
4. Create packages.

Add subscriber BW controllers to the packages and associate them with appropriate global controllers.

5. Apply the service configuration.

The bandwidth values of the default global controllers are set; the values of all other global controllers are not set – these global controllers are templates.

6. Add virtual links using the CLI.

Each virtual link gets a set of global controllers with the PIR values of the template global controller configuration.

If necessary, you can use the CLI to change the PIR values of the global controller.

7. A subscriber is introduced to the Cisco SCE platform. Upstream and downstream virtual links are associated with the subscriber as well as a package.
8. Rule resolution for each flow of the subscriber is according to the package of the subscriber and the global controller configuration of the virtual link.

Collection Manager Virtual Links Names Utility

The Collection Manager (CM) includes a command-line utility for managing the names of virtual links.

For more information about the CM Virtual Links Names Utility, see the “Managing Virtual Links” section in the “Managing the Collection Manager” chapter of *Cisco Service Control Management Suite Collection Manager User Guide*.

How to Enable Virtual Links Mode

To use virtual links, you must enable Virtual Links mode.

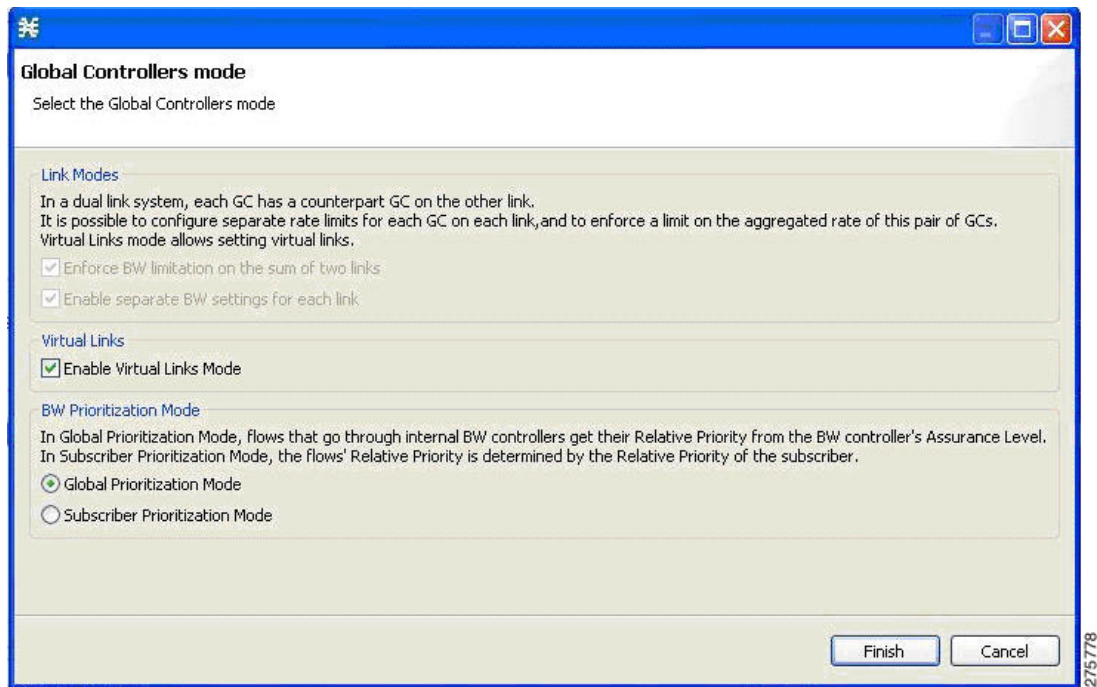


Caution

If you enable or disable Virtual Links mode, all user-defined global controllers are deleted from the service configuration.

- Step 1** In the Policies tab, click **Global Policy**.
The Global Bandwidth Settings are displayed in the right (Rule) pane.
- Step 2** Click **Edit Preferences**.
The Global Controllers mode dialog box appears (Figure 9-38).

Figure 9-38 Global Controllers Mode



- Step 3** Check the **Enable Virtual Links Mode** check box.



Note

If you have already added global controllers or if you selected asymmetric routing classification mode, a warning message appears. To continue, click **OK**.

The Virtual Links Global Controllers tab opens.

- Step 4** Click **Finish**.
The Global Bandwidth Settings dialog box closes.

How to View Virtual Links Global Controller Settings



Note

Global controller bandwidth is based on Layer 1 volume.
(Accounting, reporting, and subscriber bandwidth control in Cisco SCA BB is based on Layer 3 volume.)

Step 1 In the Policies tab, click **Global Policy**.

The Global Bandwidth Settings are displayed in the right (Rule) pane.

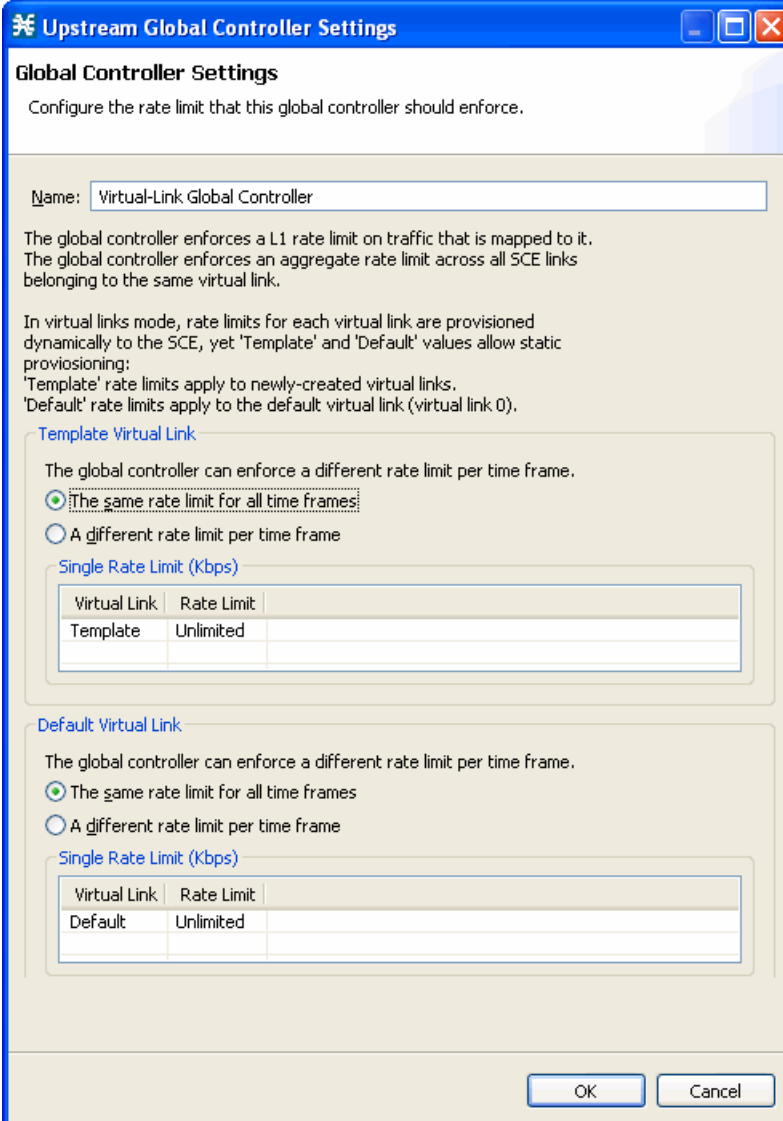
The maximum amount of bandwidth that can be used by any global controller is displayed at the top of the Global Bandwidth Settings:

- **Total Link Upstream Bandwidth Limit: Link 1**
- **Total Link Downstream Bandwidth Limit: Link 1**

Step 2 Select a global controller, and click the **Edit** () icon.

The Global Controller Settings dialog box appears ([Figure 9-39](#)).

Figure 9-39 Upstream Global Controller Settings



Upstream Global Controller Settings

Global Controller Settings
Configure the rate limit that this global controller should enforce.

Name:

The global controller enforces a L1 rate limit on traffic that is mapped to it. The global controller enforces an aggregate rate limit across all SCE links belonging to the same virtual link.

In virtual links mode, rate limits for each virtual link are provisioned dynamically to the SCE, yet 'Template' and 'Default' values allow static provisioning:
'Template' rate limits apply to newly-created virtual links.
'Default' rate limits apply to the default virtual link (virtual link 0).

Template Virtual Link

The global controller can enforce a different rate limit per time frame.

The same rate limit for all time frames
 A different rate limit per time frame

Single Rate Limit (Kbps)

Virtual Link	Rate Limit
Template	Unlimited

Default Virtual Link

The global controller can enforce a different rate limit per time frame.

The same rate limit for all time frames
 A different rate limit per time frame

Single Rate Limit (Kbps)

Virtual Link	Rate Limit
Default	Unlimited

OK Cancel

The values of the global controllers defined in the dialog box depends on the values displayed in the Global Bandwidth Settings. So, for example, if the Total Link Upstream Bandwidth Limit: Link 1 has a value of 10 Mbps then the upstream default global controller value cannot exceed 10 Mbps.

The **Name** field contains a unique name assigned to the global controller. The system automatically assigns the names Controller 1, Controller 2, and so on.

The dialog box contains the following two tabs:

- **Template Virtual Link**—The default maximum value of the total link limit permitted to global controllers of any created virtual links, either for all time frames or per time frame.
- **Default Virtual Link**—The maximum value of the total link limit permitted to global controllers of the default virtual link, either for all time frames or per time frame.

Step 3 Click **OK**.

The Global Bandwidth Settings dialog box closes.

Managing Virtual Links Global Controllers

Virtual link global controllers can be added edited and deleted in the same way as regular global controllers. For more information, see the following sections:

- [How to Add Global Controllers, page 9-7](#)
- [How to Set the Maximum Bandwidth of Global Controllers, page 9-9](#)
- [How to Delete Global Controllers, page 9-11](#)
- [Managing Subscriber Bandwidth, page 9-29](#)

How to Edit the Virtual Links Total Link Limits

You can limit the total bandwidth passing through the physical link.

The total link limits for upstream and downstream traffic are defined independently.

In Virtual Links mode, bandwidth limitations are applied to the sum of all links.

Step 1 In the Policies tab, click **Global Policy**.

The Global Bandwidth Settings dialog box is displayed in the right (Rule) pane.

Step 2 In the Upstream or Downstream section, click **Edit Rate Limit**.

The Total Rate Limit dialog box appears.

Step 3 In the **Total Rate Limit for each SCE link (Kbps)** field, enter the maximum bandwidth of the Cisco SCE platform capacity that the platform carries, or enter Unlimited.

Step 4 Click **OK**.

The Total Rate Limit dialog box closes.

The Total Link Bandwidth Limit: Link 1 field is updated.

Managing Virtual Links with CLI Commands

You can configure, enable, and disable virtual links using the Cisco SCE platform Command-Line Interface (CLI). For more information about the Cisco SCE platform CLI, see the *Cisco SCE8000 CLI Command Reference*.

- Use the following CLI commands to manage virtual links:

```
virtual-links index <index> direction [upstream | downstream]
virtual-links index <VL index> direction [upstream | downstream] gc <gc index> set-PIR
value <PIR 1, PIR2, PIR3, PIR4>
virtual-links index <VL index> direction [upstream | downstream] gc <gc index> set-PIR
value <PIR for all timeframes>
virtual-links index <VL index> direction [upstream | downstream] gc <gc index>
reset-PIR
no virtual-links index <index> direction [upstream | downstream]
```

These commands are line interface configuration commands. To run these commands see [“How to Enter Line Interface Configuration Mode” section on page 9-50](#).

- Use the following CLI command to set the virtual links index of a subscriber:

```
subscriber name <name> property name [vlUp | vlDown] value <vl index>
```

This command is a line interface configuration command. To run this command, see [“How to Enter Line Interface Configuration Mode” section on page 9-50](#).

- Use the following CLI command in EXEC mode to monitor the status of virtual links:

```
Show interface LineCard 0 virtual-links [all | changed | different-from-template]
```

Description of Virtual Links CLI Commands

Table 9-1 gives a description of the virtual links CLI commands.

Table 9-1 Virtual Links CLI Commands

Command	Description
virtual-links index <index> direction [upstream downstream]	Add a virtual link
virtual-links index <VL index> direction [upstream downstream] gc <gc index> set-PIR value <PIR 1, PIR2, PIR3, PIR4>	Update the global controller PIR values of a virtual link - separate values for each time frame
virtual-links index <VL index> direction [upstream downstream] gc <gc index> set-PIR value <PIR for all timeframes>	Update the global controller PIR values of a virtual link - one value for all time frames
virtual-links index <VL index> direction [upstream downstream] gc <gc index> reset-PIR	Update the global controller PIR values of a virtual link - take the values defined in the template global controller
no virtual-links index <index> direction [upstream downstream]	Delete a virtual link
subscriber name <name> property name [vlUp vlDown] value <vl index>	Set a virtual links index for the subscriber

Table 9-1 Virtual Links CLI Commands (continued)

Command	Description
show interface LineCard 0 virtual-links all	Show information about all virtual links
Show interface LineCard 0 virtual-links [all changed different-from-template]	Show information about virtual links whose PIR is changed or differs from the value defined in the template global controller

How to Enter Line Interface Configuration Mode

-
- Step 1** At the Cisco SCE platform CLI prompt (`SCE#`), type **configure**.
- Step 2** Press **Enter**.
The `SCE(config)#` prompt appears.
- Step 3** Type **interface LineCard 0**.
- Step 4** Press **Enter**.
The `SCE(config if)#` prompt appears.
-

Managing Packages

A package is a description of subscriber policy. It is a collection of rules that defines the reaction of the system when it encounters flows that are mapped to the service to which the rule is related. It is recommended that you first define services (see [“Managing Services” section on page 7-3](#)) and only then add and define packages.

Every Cisco SCA BB service configuration contains a package, the default package, which is the root package and cannot be deleted.

A subscriber is mapped to the default package in one of the following conditions:

- No other package is specifically assigned to the subscriber
- A nonexistent package is assigned to the subscriber.

A service configuration can contain up to 5000 packages.

- [Package Parameters, page 9-51](#)
- [How to View Packages, page 9-53](#)
- [How to Add Packages, page 9-55](#)
- [How to Set Advanced Package Options, page 9-57](#)
- [How to Duplicate Packages, page 9-58](#)
- [How to Edit Packages, page 9-59](#)
- [How to Delete Packages, page 9-60](#)

Package Parameters

The following parameters define a package:

- General parameters:
 - Package Name—A unique name for the package
 - Description—(Optional) A description of the package
- Quota Management parameters:
 - Quota Management Mode—Specifies how the subscriber quotas are managed—by external quota manager or replenished periodically by Cisco SCA BB.
 - Aggregation Period Type—The quota aggregation period used when quotas are replenished periodically.
 - Quota Buckets—16 resource buckets used for quota management.
- Subscriber BW Controllers parameters:
 - Subscriber relative priority—The relative priority given to subscribers of the package at times of Network congestion.
Separate priorities are defined for upstream and downstream flows.
 - Subscriber Bandwidth Controllers—A list of BW controllers (BWCs) that are available to services that are part of the package. Various parameters are defined for each BWC, including a mapping to a global controller.
Separate BWCs are defined for upstream and downstream flows.

- Advanced parameters:
 - Package Index—The unique number by which the system recognizes a package. Changing the package name does not affect Cisco SCE platform activity. The system provides a default value of the package index. Do not modify this value.
 - Parent Package—The package one level higher in the package hierarchy. The parent package is important when packages share usage counters. The default package is the base of the package hierarchy, and does not have a parent.
 - Package Usage Counter—Used by the system to generate data about the total use by each package. A package can use either an exclusive package usage counter or the package usage counter of the parent package.
Each usage counter has:
 - A name assigned by the system (based on the package name).

**Note**

An asterisk is appended to a package usage counter name whenever the counter applies to more than one package.

- A unique counter index—The system provides a default value of the counter index. Do not modify this value.
- Calendar—The calendar used as the basis for the time-based rules of the package.
- VAS Traffic Forwarding Table—The forwarding table used by the package.

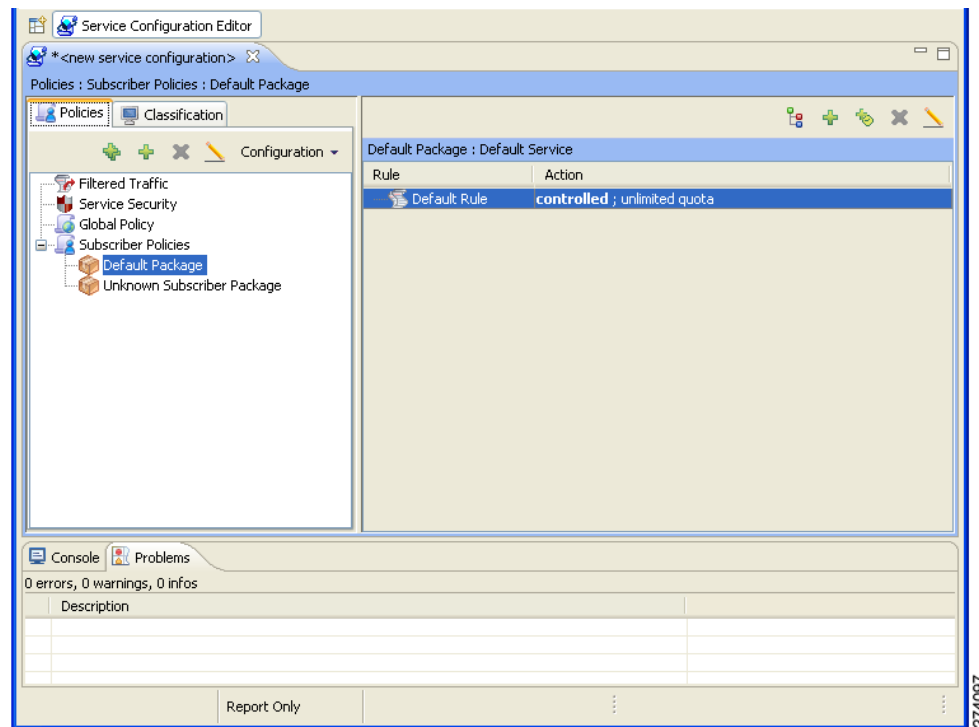
These parameters are defined when you add a new package (see [“How to Add Packages” section on page 9-55](#)). You can modify them at any time (see [“How to Edit Packages” section on page 9-59](#)).

How to View Packages

You can view a hierarchy tree of all existing packages, and you can see a list of services for which specific rules are defined for any selected package.

- Step 1** In the current service configuration, click the **Policies** tab (Figure 9-40).

Figure 9-40 Policies Tab



A list of all packages is displayed in the package tree.

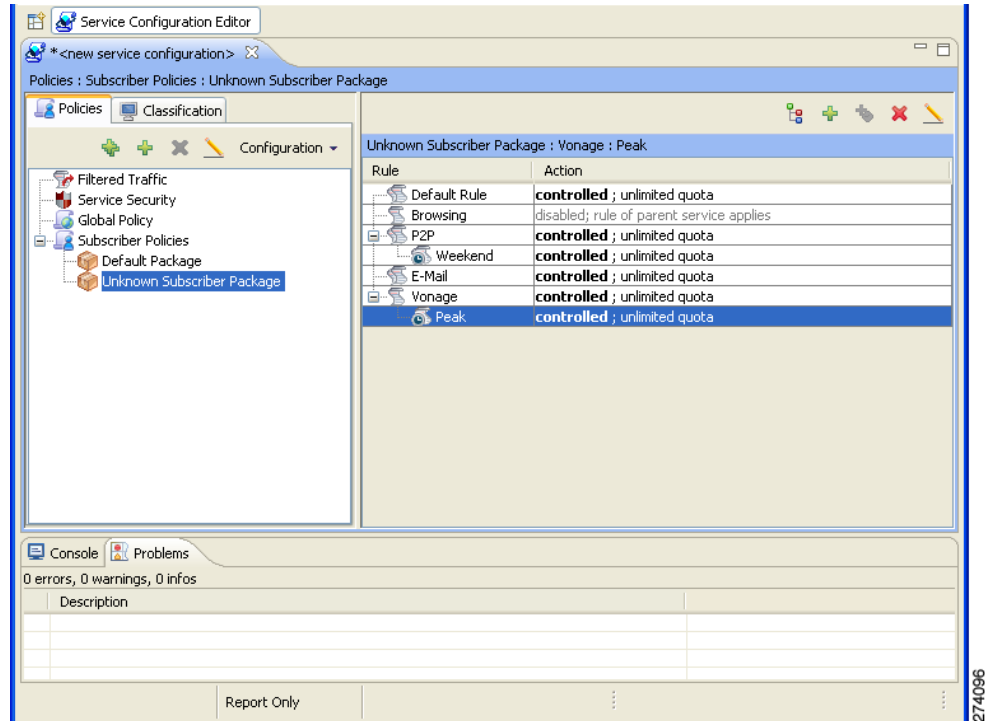


Note

To view more information about a package, open the Package Settings dialog box (see “[How to Edit Packages](#)” section on page 9-59).

- Step 2** Click a package in the hierarchy to display the rules of the package.
A list of all rules of this package is displayed in the right (Rule) pane (Figure 9-41).

Figure 9-41 Service Configuration Editor



274096

How to Add Packages

A default package is predefined in the Console installation. You can add additional packages to a service configuration, subject to the limit of 5000 packages per service configuration.

After you have added a new package, you can define rules for the package (see [“How to Add Rules to a Package” section on page 9-63](#)).


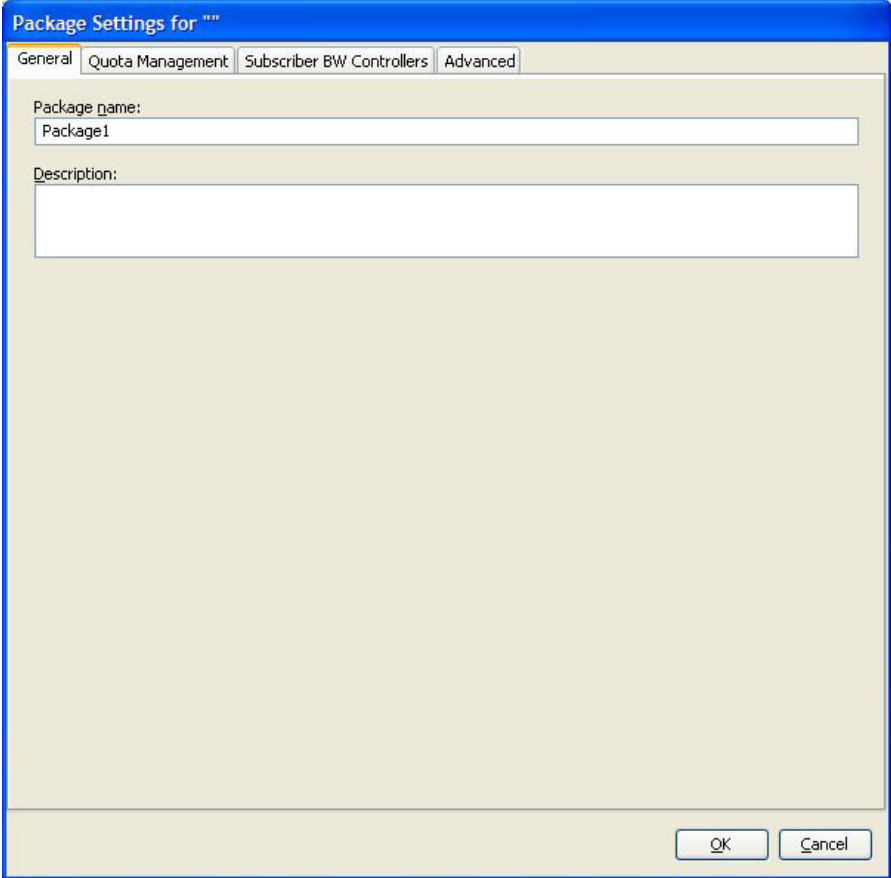
- Step 1** In the Policies tab, select a package from the package tree. This package is the parent of the package you are adding.
- Step 2** In the Policies tab, click the **Add Package** () icon.
The Package Settings dialog box appears ([Figure 9-42](#)).

Figure 9-42 *Package Settings*



- Step 3** In the Package name field, enter a unique and relevant name for the package.
- Step 4** (Optional) In the Description field, enter a meaningful and useful description of the package.
- Step 5** To configure parameters in the Advanced tab, continue with the instructions in the following section.

Step 6 Click **OK**.

The Package Settings dialog box closes.

The new package is added as a child to the package selected in the package tree and becomes the selected package. The default service rule is displayed in the right (Rule) pane.

To edit the default service rule, and to add new rules to the package, see [“Managing Rules” section on page 9-61](#).

What to Do Next

To configure parameters in the Quota Management tab see [“How to Edit Quota Management Settings for Packages” section on page 9-91](#).

To configure parameters in the Subscriber BW Controllers tab, see [“How to Edit Package Subscriber BWCs” section on page 9-30](#).

How to Set Advanced Package Options

You can change the index for the package, specify an exclusive usage counter, or select a calendar for the package in the Advanced tab.

- Step 1** In the Package Settings dialog box, click the **Advanced** tab.
The Advanced tab opens (Figure 9-43).

Figure 9-43 Advanced Tab

Package Settings for "Default Package"

General | Quota Management | Subscriber BW Controllers | **Advanced**

Package Index
Set the Index for this Package: 0

Parent Package
Select Parent Package (for sharing usage counters):

Package Usage Counters
A package can either be mapped to exclusive package usage counters, or share usage counters with its ancestor package.
 Map this Package to exclusive package usage counters
Package usage counter name for this package: Default Package Counter
Counter Index: 0

Calendar
Select Calendar for this Package: Default Calendar

VAS Traffic Forwarding Table
Select Traffic Forwarding Table for this Package: Default Table

OK Cancel

- Step 2** To change the package index for this package, from the Set the Index for this Package drop-down list, select a package index.



Note The system provides a default value of the index. Do not modify this value unless a specific index value must be assigned to the package.

- Step 3** To set a different parent package for this package, select the desired parent from the Select Parent Package drop-down list.

Step 4 By default, a new package uses an exclusive usage counter. To share the parent package usage counter, uncheck the **Map this Service to exclusive package usage counters** check box.

The name in the read-only Package usage counter name for this package field changes to reflect your choice.

The Counter Index drop-down list is dimmed.

Step 5 To change the counter index (if you are using an exclusive package usage counter), select a value for the index from the Counter Index drop-down list.

**Note**

The system provides a default value of the index. Do not modify this value.

Step 6 To set a calendar for this package (to use its time frames for time-based rules), select the desired calendar from the Select Calendar for this Package drop-down list.

Step 7 To set a VAS traffic-forwarding table for this package, select the desired traffic-forwarding table from the Select Traffic Forwarding Table for this Package drop-down list.

**Note**

If VAS traffic forwarding is disabled (the default), the drop-down list is dimmed. To enable VAS traffic forwarding, see [“How to Enable VAS Traffic Forwarding”](#) section on page 10-67.

Step 8 Click **OK**.

The Package Settings dialog box closes.

The new package is added as a child to the selected parent package and becomes the selected package. The default service rule is displayed in the right (Rule) pane.


To edit the default service rule, and to add new rules to the package, see [“Managing Rules”](#) section on page 9-61.

How to Duplicate Packages

Duplicating an existing package is a useful way to create a new package similar to an existing package. It is faster to duplicate a package and then modify it than to define the package from beginning.

A duplicated package is added at the same level in the package tree as the original package.

Step 1 In the Policies tab, select a package from the package tree.


Step 2 In the Policies tab, click the **Duplicate Package** () icon.

A duplicate package is created with all the same attributes as the original package. If the package is duplicated several times, the name of the new package is the name of the selected package followed by “(1)”, “(2)”, and so on.

Step 3 Modify the package parameters (see [“How to Edit Packages”](#) section on page 9-59).

How to Edit Packages

You can modify the parameters of a package (including the default package) at any time.

-
- Step 1** In the Policies tab, select a package from the package tree.
- Step 2** In the Policies tab, click the **Edit Package** () icon.
The Package Settings dialog box appears.
- Step 3** In the Package name field, enter a new name for the package.
- Step 4** In the Description field, enter a new description of the package.
- Step 5** (Optional) Change quota management settings, see Editing Package Quota Management Settings (Using the Quota Management Tab (Packages)) “[How to Edit Quota Management Settings for Packages](#)” section on page 9-91.
- Step 6** (Optional) Change bandwidth control settings, see “[How to Edit Package Subscriber BWCs](#)” section on page 9-30.
- Step 7** To change advanced settings, click the Advanced tab.
The Advanced tab opens.
- a. To change the package index for this package, from the Set the Index for this Package drop-down list, select a Package Index.



Note

The system provides a default value of the counter index. Do not modify this value unless a specific index value must be assigned to the package.

- b. To change the parent package of this package, select the desired parent from the Select Parent Package drop-down list.
- c. To share the parent package usage counter, uncheck the **Map this Service to exclusive package usage counters** check box.

The name in the read-only Package usage counter name for this package field changes to reflect your choice.

The Counter Index drop-down list is dimmed.
- d. To use an exclusive package usage counter, check the **Map this Service to exclusive package usage counters** check box.

The name in the read-only Package usage counter name for this package field changes to reflect your choice.

The Counter Index drop-down list is dimmed.
- e. To change the counter index if you are using the exclusive package usage counter, select a value for the index from the Counter Index drop-down list.



Note

The system provides a default value of the counter index. Do not modify this value.

- f. To change the calendar used by this package, select the desired calendar from the Select Calendar for this Package drop-down list.
- g. To change the VAS traffic-forwarding table for this package, select the desired traffic-forwarding table from the Select Traffic Forwarding Table for this Package drop-down list.

**Note**

If VAS traffic forwarding is disabled (the default), the drop-down list is dimmed. To enable VAS traffic forwarding, see [“How to Enable VAS Traffic Forwarding”](#) section on page 10-67.


Step 8 Click **OK**.

The Package Settings dialog box closes.

All changes to the package parameters are saved.

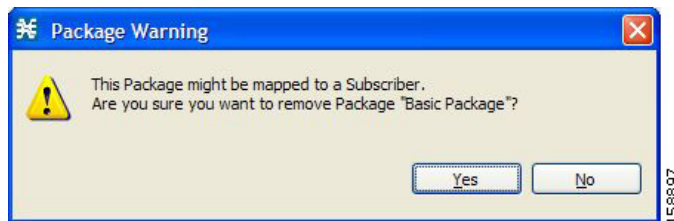
How to Delete Packages

You can delete user-defined packages. The default package cannot be deleted.

Step 1 In the Policies tab, select a package from the package tree.**Step 2** In the Policies tab, click the **Delete Package** () icon.

A Package Warning message appears ([Figure 9-44](#)).

Figure 9-44 Package Warning

**Step 3** Click **Yes**.

The package is deleted and is no longer displayed in the package tree.

Managing Rules

After you have defined services and basic packages, you can define rules for the package.

You can configure rules to do some or all of the following:

- Block the service
- Define maximum bandwidth for the service
- Change the DSCP ToS value of packets in a flow
- Set a quota for the service
- Define behavior when the quota for this service is breached

A rule usually applies at all times. To allow additional flexibility, you can divide the week into four separate time frames. You can define subrules—time-based rules—for each time frame.

**Note**

In Cisco SCA BB, the maximum number of unique rules that can be applied is limited to 5000. If the number of unique rules exceeds the maximum limit, an error occurs. The number of unique rules are identified from the Package ID, Service, and Timeframe fields.

- [The Default Service Rule, page 9-61](#)
- [Rule Hierarchy, page 9-61](#)
- [How to View the Rules of a Package, page 9-62](#)
- [How to Add Rules to a Package, page 9-63](#)
- [How to Define Per-Flow Actions for a Rule, page 9-66](#)
- [How to Edit Rules, page 9-68](#)
- [How to Delete Rules, page 9-70](#)
- [How to Display the Services Affected by a Rule, page 9-70](#)
- [Managing Time-Based Rules, page 9-71](#)
- [How to Manage DSCP ToS Marker Values, page 9-81](#)

The Default Service Rule

A default service rule is assigned to every package. It cannot be deleted or disabled.

The default values of this rule are:

- Admit (do not block) traffic.
- Map traffic to the default BWCs.
- Do not limit quotas for either upstream or downstream traffic.

Rule Hierarchy

The Cisco SCE platform applies the most specific rule to any flow.

For example, if you define rules for E-Mail and POP3:

- Any flow mapped to the SMTP or IMAP service is handled according to the e-mail rule.

- Any flow mapped to the POP3 service is handled according to the POP3 rule

This means, for example, that POP3 can have its own usage limits, whereas SMTP and IMAP must share usage limits.

**Note**



If you add a rule for a child service, the settings for the parent rule are not copied to the new rule. All new rules start with default values.



Indicates any rule that also applies to child services.



Indicates any rule that does not apply to any child services.

Time-based rules are shown as children of the relevant rule. The icon for a time-based rule also shows if the rule applies to child services ( or ).

See also “[How to Display the Services Affected by a Rule](#)” section on page 9-70.

How to View the Rules of a Package

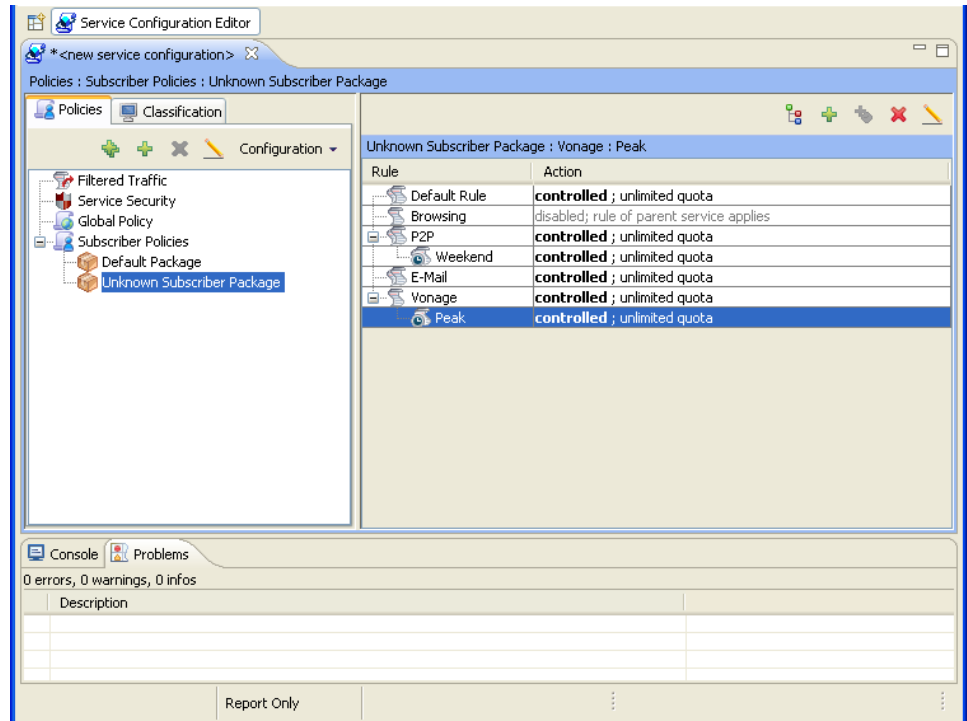
You can view a list of the rules of a package.

The listing for each rule includes an icon, the name of the service or group of services to which the rule applies, whether the rule is enabled or disabled, and a brief description of the rule.

Step 1 In the Policies tab, select a package from the package tree.

A list of all rules defined for this package is displayed in the right (Rule) pane ([Figure 9-45](#)).

Figure 9-45 Service Configuration Editor



What to Do Next

To see more information about a rule, open the Edit Rule for Service dialog box (see “[How to Edit Rules](#)” section on page 9-68).

To see more information about a time-based rule, open the Edit Time-Based Rule for Service dialog box (see “[How to Edit Time-Based Rules](#)” section on page 9-74).

How to Add Rules to a Package

A default service rule is assigned to every package. You can add additional rules to a package.

Adding time-based rules is described in the section [How to Add Time-Based Rules to a Rule](#), page 9-72.


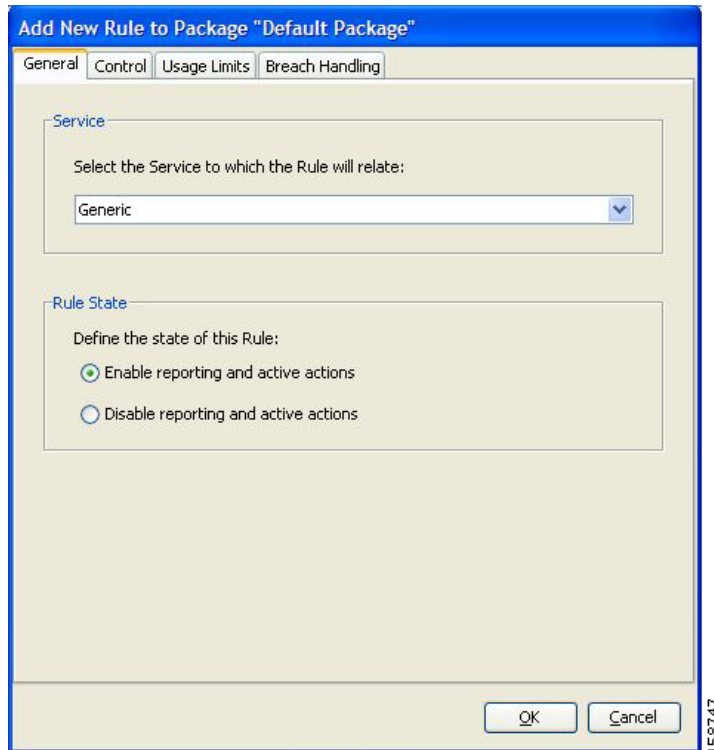
-
- Step 1** In the Policies tab, select a package from the package tree.
- Step 2** In the right (Rule) pane, click the **Add Rule** () icon.
- The Add New Rule to Package dialog box appears ([Figure 9-46](#)).

Figure 9-46 Add New Rule to Package

- Step 3** In the Service area of the Add New Rule to Package dialog box, select a service from the Select the Service to Which the Rule Relates drop-down list.



Note Services for which a rule is already defined for this package are dimmed.

Step 4 In the Rule State area, select one of the **Define the State of this Rule** radio buttons.

- **Enable reporting and active actions**
- **Disable reporting and active actions**



Note You can enable or disable a rule at any time (see [“How to Edit Rules”](#) section on page 9-68).

Step 5 (Optional) Set behavior per traffic flow for this rule, continue with the instructions in the [“How to Define Per-Flow Actions for a Rule”](#) section on page 9-66.

Step 6 Click **OK**.

The Add New Rule to Package dialog box closes.

The new rule is added to the list of rules displayed in the right (Rule) pane.

What to Do Next

Usage limits and breach handling are part of quota management (see [“Managing Quotas”](#) section on page 9-83):

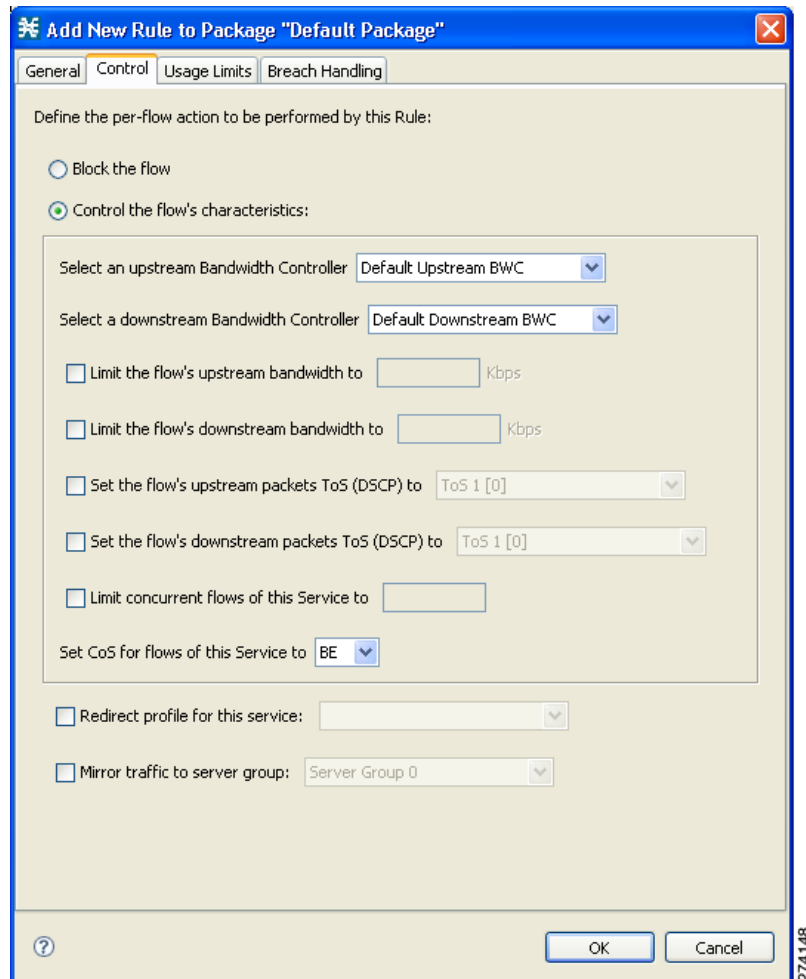
- To configure parameters in the Usage Limits tab, see [“How to Select Quota Buckets for Rules”](#) section on page 9-93.
- To configure parameters in the Breach Handling tab, see [“How to Edit Breach-Handling Parameters for a Rule”](#) section on page 9-94.

How to Define Per-Flow Actions for a Rule

The Control tab of the Add New Rule to Package dialog box allows you to set behavior per traffic flow for sessions that are mapped to the current service.

- Step 1** In the Add New Rule to Package dialog box, click the **Control** tab.
The Control tab opens (Figure 9-47).

Figure 9-47 Control Tab



To control flows that are mapped to the service of this rule, continue at [Step 3](#).

- Step 2** To block flows that are mapped to the service of this rule, select the **Block the flow** radio button and continue at [Step 12](#).
- Step 3** Select the **Control the flow's characteristics** radio button.
The options in the Flow Characteristic area are enabled.

- Step 4** From the upstream Bandwidth Controller drop-down list, select an upstream BWC. This sets up bandwidth metering of all concurrent flows mapped to this rule, based on the characteristics of the selected BWC.

The BWCs in this drop-down list are defined when creating or editing the package.



Caution

For time-based rules: If you need different global controller settings for different time frames, define maximum bandwidths per time frame for one global controller. Do not create a separate global controller for each time frame.

When the mouse is placed over the drop-down list, a tooltip appears (Figure 9-48). The tool tip contains the properties of the selected BWC, such as Peak Information Rate [PIR], Committed Information Rate [CIR], Global Controller, and Assurance Level.

Figure 9-48 Drop-Down List Tips



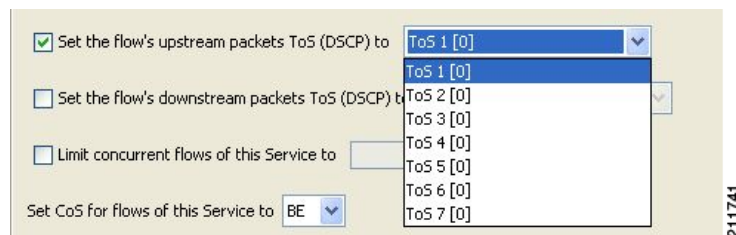
- Step 5** From the downstream Bandwidth Controller drop-down list, choose a downstream BWC.
- Step 6** (Optional) To set a per-flow upstream bandwidth limit, check the **Limit the flow's upstream bandwidth** check box and enter a value in the Kbps field.



Note Per-flow bandwidth has a granularity of 1 Kbps up to 57 Mbps.

- Step 7** (Optional) To set a per-flow downstream bandwidth limit, check the **Limit the flow's downstream bandwidth** check box and enter a value in the Kbps field.
- Step 8** (Optional) To change the DSCP ToS marker of all packets in upstream flows, check the **Set the flow's upstream packets ToS (DSCP) to** check box and select a value from the drop-down list (Figure 9-49).

Figure 9-49 Drop Down List Values



- Step 9** (Optional) To change the DSCP ToS marker of all packets in downstream flows, check the **Set the flow's downstream packets ToS (DSCP) to** check box and select a value from the drop-down list.
- Step 10** (Optional) To set the maximum number of concurrent flows (mapped to this rule) permitted to a subscriber, check the **Limit concurrent flows of this Service** check box and enter a value in the associated field.

- Step 11** From the Set CoS for flows of this Service drop-down list, select a class-of-service.
- Step 12** (Optional) To enable subscriber redirection, check the **Redirect profile for this service** check box and choose a redirect profile from the drop-down list.
- Step 13** (Optional) To enable traffic mirroring, check the **Mirror traffic to server group** check box and choose a server group from the drop-down list.



Note The Mirror traffic to server group check box is only enabled when Traffic Mirroring is enabled in the VAS Settings dialog box.

- Step 14** Click **OK**.
- The Add New Rule to Package dialog box closes.
- The new rule is added to the list of rules displayed in the right (Rule) pane.

How to Edit Rules

You can edit any rule, including the default service rule.



Note You cannot disable the default service rule.



Note The tabs of the Edit Rule for Service dialog box are the same as the tabs of the Add New Rule to Package dialog box, except for the General tab—you cannot change the service to which the rule applies.

- Step 1** In the Policies tab, select a package from the package tree.
- Step 2** In the right (Rule) pane, select a rule.


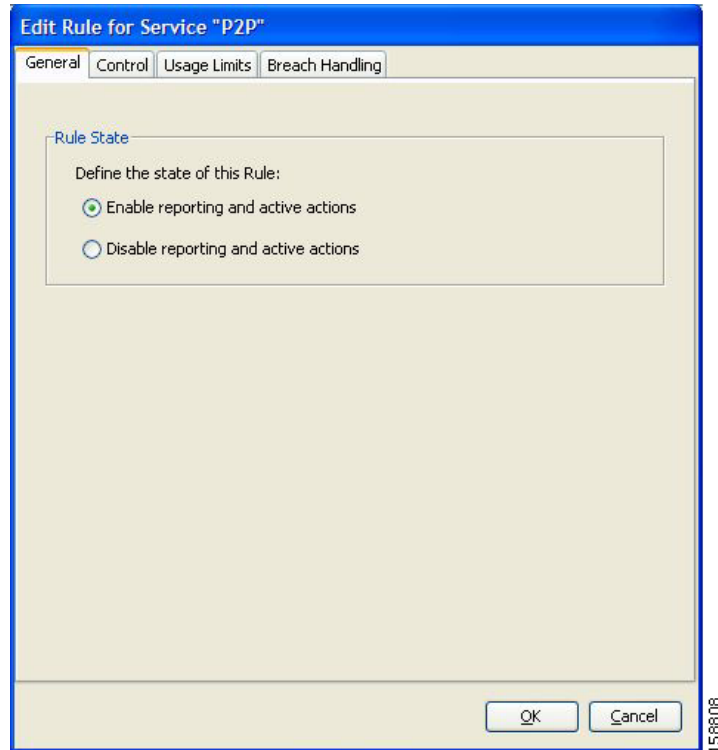
- Step 3** Click  (**Edit Rule**).
- The Edit Rule for Service dialog box appears ([Figure 9-50](#)).

Figure 9-50 *Edit Rule for Service*



- Step 4** In the Rule State area, select one of the **Define the State of this Rule** radio buttons.
- **Enable reporting and active actions**
 - **Disable reporting and active actions**
- Step 5** Change behavior per traffic flow.
- a. Click the **Control** tab.
The Control tab opens.
 - b. Follow the instructions in [How to Define Per-Flow Actions for a Rule](#), page 9-66.
- Step 6** Change usage limits.
- a. Click the **Usage Limits** tab.
The Usage Limits tab opens.
 - b. Follow the instructions in [How to Select Quota Buckets for Rules](#), page 9-93.
- Step 7** Define behavior when a quota is breached.
- a. Click the **Breach Handling** tab.
The Breach Handling tab opens.
 - b. Follow the instructions in [How to Edit Breach-Handling Parameters for a Rule](#), page 9-94.

- Step 8** Click **OK**.
The Edit Rule for Service dialog box closes.
All changes to the rule are saved.

How to Delete Rules

You can delete any user-defined rule. The default service rule cannot be deleted.



Note

You can *disable* a rule without losing its profile. For details, see Step 4 of “[How to Edit Rules](#)” section on page 9-68. This feature allows you to enable the rule again later, without having to reset all its parameters. You cannot disable the default service rule.


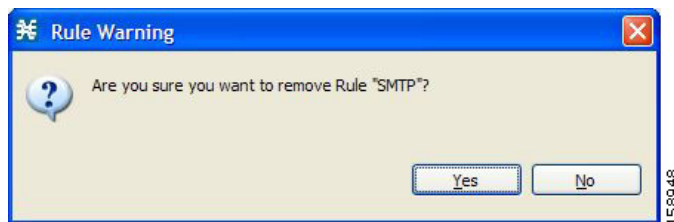
- Step 1** In the Policies tab, select a package from the package tree.
Step 2 In the right (Rule) pane, select a rule.
Step 3 In the Rule pane, click the **Delete Rule** () icon.
A Rule Warning message appears ([Figure 9-51](#)).

Figure 9-51 Rule Warning






- Step 4** Click **Yes**.
The selected rule is deleted.

How to Display the Services Affected by a Rule

You can define a service as the child of another service (the parent service is a service group). Until you define a separate rule for a child service, the rule of the parent service applies to the child service. A rule that affects any of child services of a service is indicated in the rules list by a different icon, as illustrated for the P2P rule and the FTP rule in [Figure 9-52](#).

Figure 9-52 Rules


Rule	Action
 Default Rule	controlled ; unlimited quota
 FTP	controlled ; unlimited quota
 P2P	controlled ; unlimited quota

You can display all (child) services that are affected by a rule.



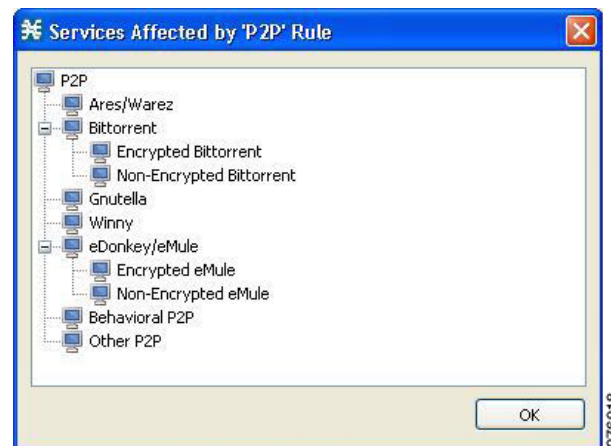
Note

The default service rule applies to all services for which a specific rule is *not* defined.

- Step 1** In the right (Rule) pane of the Policies tab, select a rule and click the **Show All Services Affected By This Rule** ().

The Services Affected dialog box appears ([Figure 9-53](#)).

Figure 9-53 Services Affected



- Step 2** Click **OK**.

The Services Affected dialog box closes.

Managing Time-Based Rules

The Console allows you to divide the week into four time frames (see [“Managing Calendars”](#) section on [page 9-76](#)). A time-based rule is a rule that applies to one time frame.

You can add time-based rules to any rule. If a time-based rule is not defined for a time frame, the parent rule is enforced.

Often, you want the rules for the different time frames to be similar. When you add a time-based rule, the settings of the parent rule are copied to the new time-based rule; you can make any needed changes. Subsequent changes to the parent rule do not affect the time-based rule.

You must define the calendar before defining the related time-based rules.

How to Add Time-Based Rules to a Rule

Adding a time-based rule to a rule allows you to specify alternate rule parameters applicable only for a specific time frame. If a time-based rule is not defined for a time frame, the parent rule is enforced.

- When you add a time-based rule, all parameters are initially set to the values defined for the parent rule. Subsequent changes to the parent rule do not change the time-base rule.
- The tabs of the Add New Time-Based Rule dialog box are the same as the tabs of the Add New Rule to Package dialog box, except for the General tab. In the Add New Rule to Package dialog box, you select a service; in the Add New Time-Based Rule dialog box, you select a time frame.

A service whose time-based rule affects any of its child services is indicated in the rules list by a modified icon, as illustrated for the Weekend time-based rule of the P2P rule in [Figure 9-54](#).

Figure 9-54 P2P Weekend Based Time Rule

Rule	Action
Default Rule	controlled [Default Upstream BWC; Default Downstream BWC; unlimited quota
P2P	controlled [Default Upstream BWC; Default Downstream BWC; quota replenished ...
Weekend	controlled [Default Upstream BWC; Default Downstream BWC; quota replenished ...
Yahoo Messenger VoIP	controlled [Default Upstream BWC; Default Downstream BWC; unlimited quota
Nintendo Wii	controlled [Default Upstream BWC; Default Downstream BWC; unlimited quota
Weekend	controlled [Default Upstream BWC; Default Downstream BWC; unlimited quota
MGCP	controlled [Default Upstream BWC; Default Downstream BWC; unlimited quota

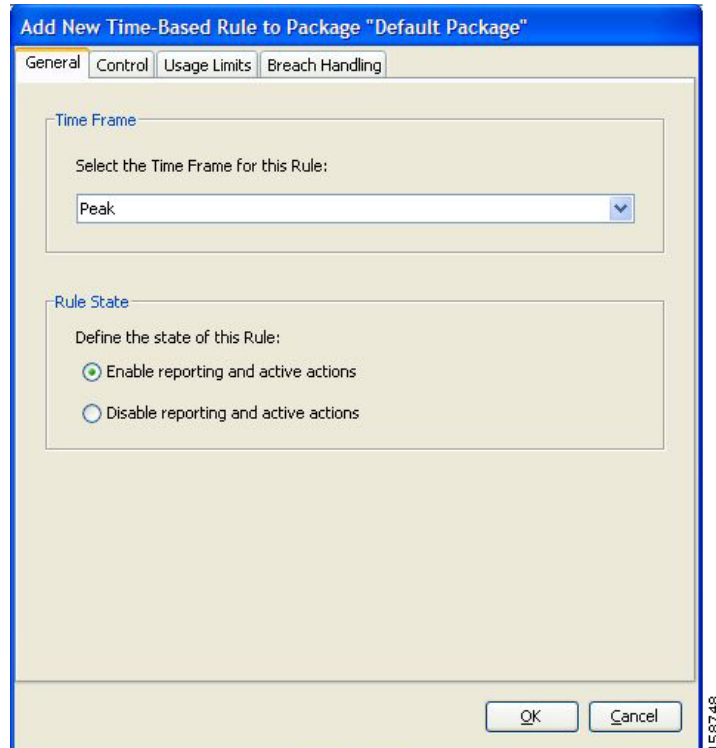
27/131

Step 1 In the Policies tab, select a package from the package tree.

Step 2 In the right (Rule) pane, select a rule.

- Step 3** Click the **Add Time-Based Rule** () icon.
The Add New Time-Based Rule dialog box appears (Figure 9-55).

Figure 9-55 Add New Time-Based Rule



- Step 4** In the Time Frame area, from the Select the Time Frame for this Rule drop-down list, select one of the four time frames.
- Step 5** In the Rule State area, select one of the **Define the State of this Rule** radio buttons.
- **Enable reporting and active actions**
 - **Disable reporting and active actions**
- Step 6** Define behavior per traffic flow.
- a. Click the **Control** tab.
The Control tab opens.
 - b. Follow the instructions in [How to Define Per-Flow Actions for a Rule](#), page 9-66.
- Step 7** Change usage limits.
- a. Click the **Usage Limits** tab.
The Usage Limits tab opens.
 - b. Follow the instructions in [How to Select Quota Buckets for Rules](#), page 9-93.
- Step 8** Define behavior when a quota is breached.
- a. Click the **Breach Handling** tab.
The Breach Handling tab opens.
 - b. Follow the instructions in [How to Edit Breach-Handling Parameters for a Rule](#), page 9-94.

Step 9 Click **OK**.

The Add New Time-Based Rule dialog box closes.

The new time-based rule is displayed as a child of the rule in the Rule pane.

How to Edit Time-Based Rules

You can edit time-based rules.



Note

The tabs of the Edit Time-Based Rule for Service dialog box are the same as the tabs of the Add New Time-Based Rule dialog box, except for the General tab. You cannot change the time frame to which the rule applies.

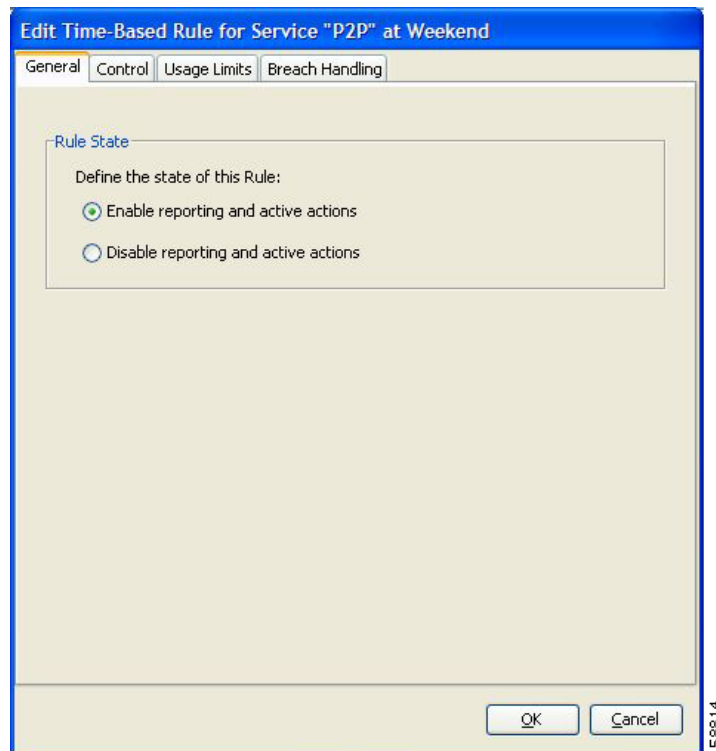
Step 1 In the Policies tab, select a package from the package tree.

Step 2 In the right (Rule) pane, select a time-based rule.

Step 3 Click the **Edit Rule** () icon.

The Edit Time-Based Rule for Service dialog box appears ([Figure 9-56](#)).

Figure 9-56 *Edit Time-Based Rule for Service*



Step 4 In the Rule State area, select one of the **Define the State of this Rule** radio buttons.

- **Enable reporting and active actions**
- **Disable reporting and active actions**

- Step 5** Define behavior per traffic flow.
- Click the **Control** tab.
The Control tab opens.
 - Follow the instructions in [How to Define Per-Flow Actions for a Rule](#), page 9-66.
- Step 6** Change usage limits.
- Click the **Usage Limits** tab.
The Usage Limits tab opens.
 - Follow the instructions in [How to Select Quota Buckets for Rules](#), page 9-93.
- Step 7** Define behavior when a quota is breached.
- Click the **Breach Handling** tab.
The Breach Handling tab opens.
 - Follow the instructions in [How to Edit Breach-Handling Parameters for a Rule](#), page 9-94.
- Step 8** Click **OK**.
The Edit Time-Based Rule for Service dialog box closes.
All changes to the time-based rule are saved.

How to Delete Time-Based Rules

You can delete any time-based rule.



Note

You can *disable* a rule without losing its profile (see “[How to Edit Time-Based Rules](#)” section on page 9-74). This allows you to enable the rule again later, without having to reset all its parameters.


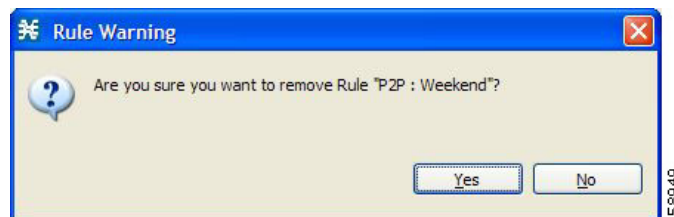
- Step 1** In the Policies tab, select a package from the package tree.
- Step 2** In the right (Rule) pane, select a time-based rule.
- Step 3** In the Rule pane, click the **Delete Rule** () icon.
A Rule Warning message appears ([Figure 9-57](#)).

Figure 9-57 Rule Warning



- Step 4** Click **Yes**.
The selected rule is deleted.

Managing Calendars

Calendars are used to divide the hours of the week into four time frames.

After you have configured a calendar, you can add time-based rules to a package that uses the calendar. A time-based rule is a rule that applies to only one time frame. Time-based rules allow you to set rule parameters that apply only at specific times. You might, for example, want to define different rules for peak, off-peak, nighttime, and weekend usage.

Each service configuration includes one default calendar. You can add nine more calendars, each with a different time-frame configuration. You can use different calendars for different packages. You can also use different calendars where a service provider has customers in more than one time zone by configuring calendars with a one-hour offset from each other.

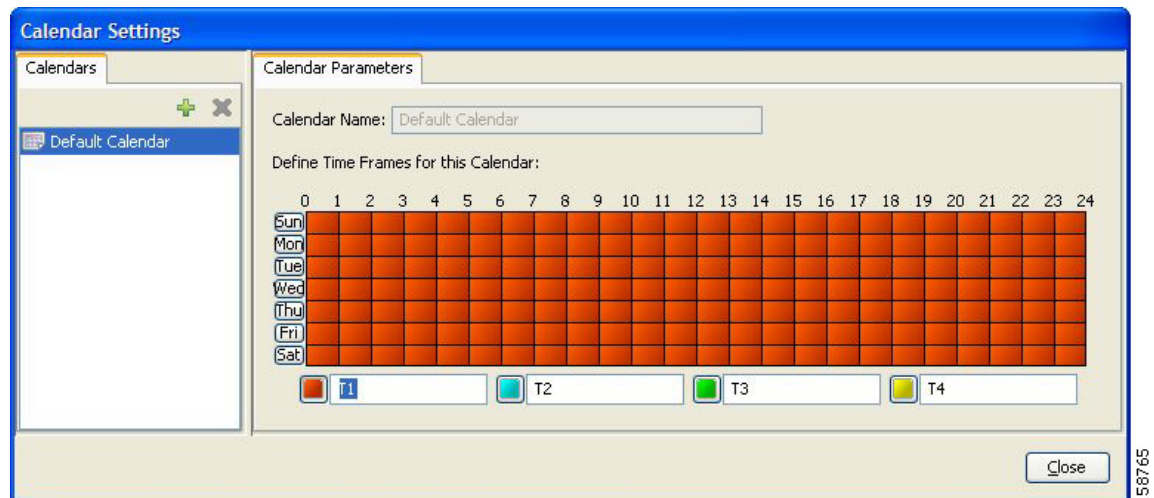
- [How to View Calendars, page 9-76](#)
- [How to Add Calendars, page 9-77](#)
- [How to Rename the Time Frames, page 9-77](#)
- [How to Delete Calendars, page 9-78](#)
- [How to Configure the Time Frames, page 9-79](#)

How to View Calendars

You can view a list of existing calendars and their time frames.

- Step 1** From the Policies tab of the left pane, choose **Configuration > Policies > Weekly Calendars**. The Calendar Settings dialog box appears ([Figure 9-58](#)).

Figure 9-58 *Calendar Settings*



The Calendars tab displays a list of existing calendars. Click a calendar in the list to display its time-frame settings.

The time frames for the selected calendar are displayed and configured in the Calendar Parameters tab.

- Step 2** Click **Close**.
The Calendar Settings dialog box closes.

How to Add Calendars

Each service configuration includes one default calendar. You can add up to nine more calendars.


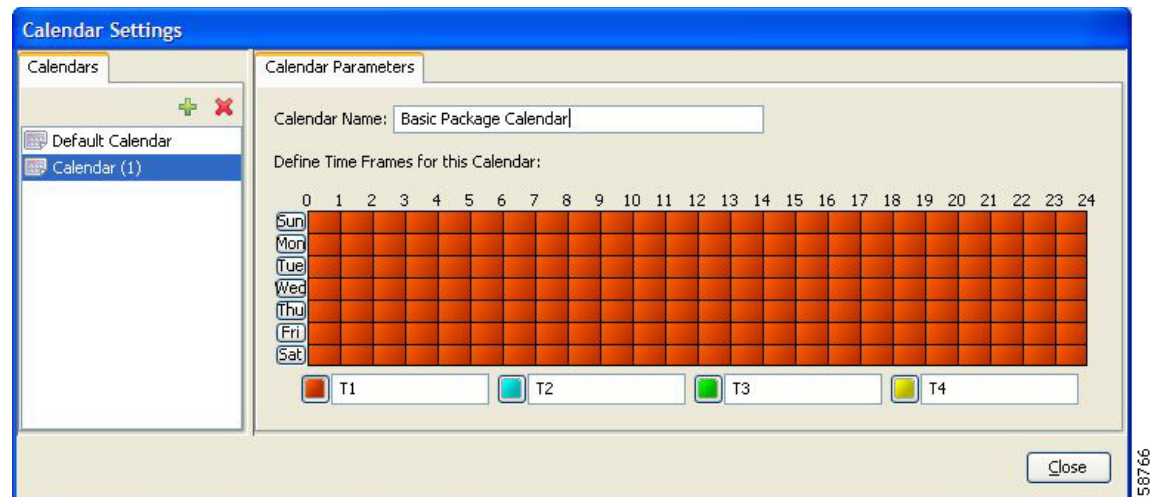
- Step 1** From the Policies tab of the left pane, choose **Configuration > Policies > Weekly Calendars**.
The Calendar Settings dialog box appears.
- Step 2** In the Calendar tab, click the **Add** () icon.
A new calendar is added with the name Calendar (1).
- Step 3** In the Calendar Parameters tab (Figure 9-59), click in the Calendar Name field and enter the name for this calendar.

Figure 9-59 *Calendar Parameters Tab*



- Step 4** Click **Close**.
The Calendar Settings dialog box closes, and the new calendar name is saved.

How to Rename the Time Frames

By default, the time frames are named T1, T2, T3, and T4. You can change these names at any time; for example, you may want to name the time frames Peak, Off Peak, Night, and Weekend.



Note

Although you can configure the time frames differently in each calendar, the names of the time frames are the same in all of the calendars. If you change the name when configuring one calendar, the names are also changed for all other calendars.

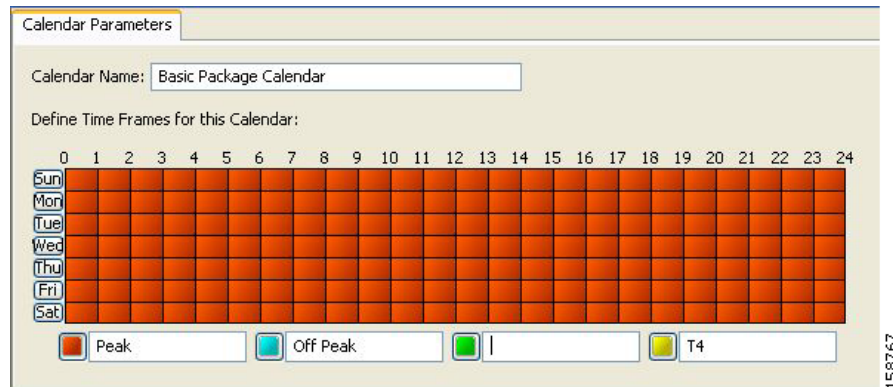
Step 1 From the Policies tab of the left pane, choose **Configuration > Policies > Weekly Calendars**.

The Calendar Settings dialog box appears.

In the Calendar Parameters tab (Figure 9-60), below the grid, each of the four time frames is listed in a field next to a colored square.

Step 2 Click in a Time Frame Name field, and enter a new name for the time frame.

Figure 9-60 Calendar Parameters Tab



Step 3 Repeat Step 2 for the other three time frames.

Step 4 Click **Close**.

The Calendar Settings dialog box closes, and the changes to the names of the time frames are saved.

How to Delete Calendars

You can delete any user-added calendar. The default calendar cannot be deleted.



Note

A calendar used by a package cannot be deleted. (When you select the calendar, the Delete icon is dimmed.) To delete the calendar, you must first select a different calendar for each package using the calendar that is deleted.

See “[How to Set Advanced Package Options](#)” section on page 9-57 for information about changing the calendar associated with a package.


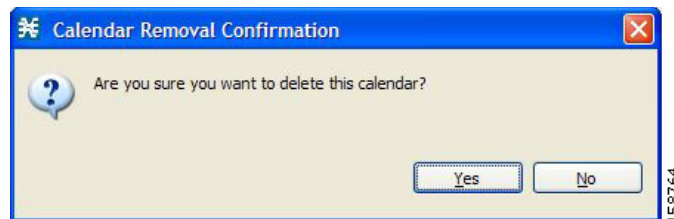
-
- Step 1** From the Policies tab of the left pane, choose **Configuration > Policies > Weekly Calendars**.
The Calendar Settings dialog box appears.
- Step 2** In the Calendar tab, select a calendar and click the **Delete** () icon.
A Calendar Removal Confirmation message appears ([Figure 9-61](#)).

Figure 9-61 *Calendar Removal Confirmation*



- Step 3** Click **Yes**.
The calendar is deleted.
- Step 4** Click **Close**.
The Calendar Settings dialog box closes.
-

How to Configure the Time Frames

By default, all the hours of the week belong to one time frame. The Console allows you to assign each of the 168 (24x7) hours of the week to one of four separate time frames. These time frames allow you to supply time-dependent differentiated services and to impose constraints on any service.

You might want, for example, to divide the week as follows:

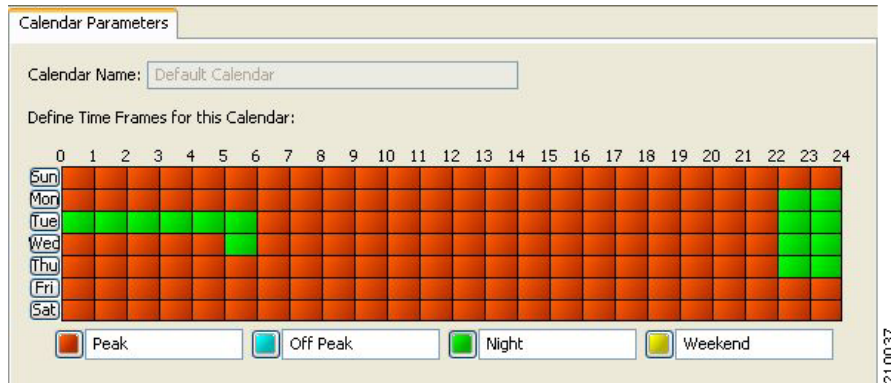
- Peak
- Off Peak
- Night
- Weekend

You can define different time frames for each calendar.

- Step 1** From the Policies tab of the left pane, choose **Configuration > Policies > Weekly Calendars**.
The Calendar Settings dialog box appears.
- Step 2** In the Calendars tab, select a calendar to configure.
In the Calendar Parameters tab, the selected calendar's **Define Time Frames for this Calendar** grid is displayed. The grid, representing one week, is laid out in a format of 24 hours x 7 days. Each cell represents one hour.
Below the grid, the name of each time frame appears next to a colored button.
- Step 3** Click one of the colored buttons.

- Step 4** Select all the cells in the grid that represent hours that are part of the selected time frame. You can select a group of cells by holding down the mouse button and dragging across the cells (Figure 9-62).

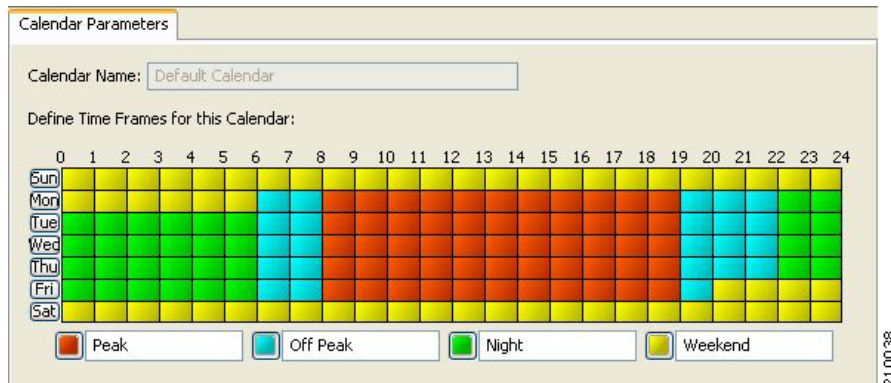
Figure 9-62 *Calendar Parameters Tab*



The changes are written to the service configuration as you make them.

- Step 5** Repeat Steps 3 and 4 for the other time frames until you have mapped the entire grid. You have now mapped the week into four different time frames. Figure 9-63 illustrates a possible time partition plan.

Figure 9-63 *Time Partition Plan Example*



- Step 6** Click **Close**. The Calendar Settings dialog box closes.

How to Manage DSCP ToS Marker Values

Cisco SCA BB can change the value of the DSCP ToS marker of packets of flows that match a filter rule or a service rule.

For details on how to change the value of the DSCP ToS marker, see the following steps:

- For Filter Rule—see Step 11 of [“How to Add Filter Rules”](#) section on page 10-27
- For Service Rule—see Steps 10 and 11 of [“How to Define Per-Flow Actions for a Rule”](#) section on page 9-66 and Step 9 of [“How to Edit Breach-Handling Parameters for a Rule”](#) section on page 9-94

Cisco SCA BB supports seven ToS Marker Classes. You assign each class a specific value to apply to the packets of a flow.

**Note**

If you have used DSCP marking on a Cisco SCA BB release before 3.1.5 and you are converting your old service configurations, you must reconfigure the service configurations to obtain the same network behavior as in the former release.

DSCP ToS Marking

DSCP ToS marking is used in IP networks as a means to signal the type and priority of a flow between network elements.

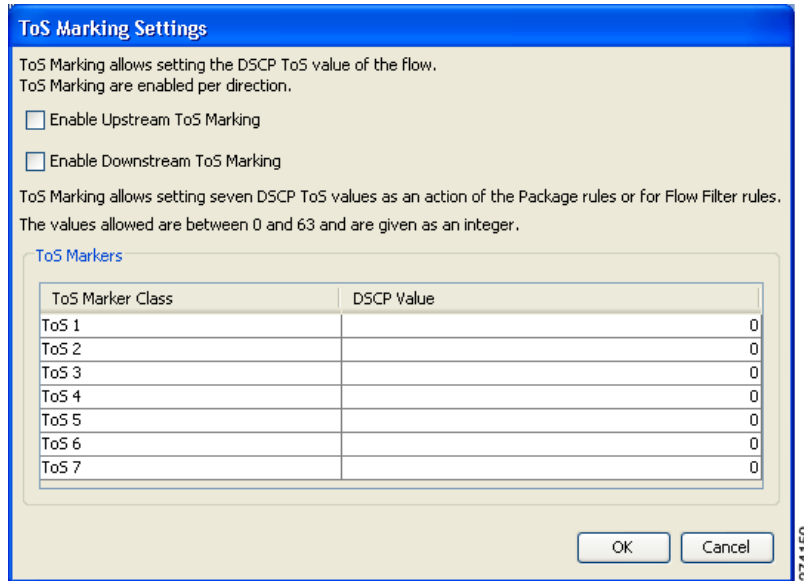
The default marking option is not to mark the packet. The classification may take a few packets to finalize. So after the ToS marking is enabled, the first few packets may still be processed under the default option and therefore may not be marked.

**Caution**

In an MPLS environment, the Cisco SCE platform does not map the DSCP bits to the EXP bits of the MPLS header.

- Step 1** From the Policies tab of the left pane, choose **Configuration > Policies > ToS Marking Settings**.
The ToS Marking Settings dialog box appears (Figure 9-64).

Figure 9-64 ToS Marking Settings



- Step 2** (Optional) To enable DSCP ToS marking on upstream flows, check the **Enable Upstream ToS Marking** check box.

If Upstream ToS Marking is disabled, it overrides filter rule and service rule settings.

- Step 3** (Optional) To enable DSCP ToS marking on downstream flows, check the **Enable Downstream ToS Marking** check box.

If Downstream ToS Marking is disabled, it overrides filter rule and service rule settings.

- Step 4** Give unique names to the ToS Marker Classes.



Note You can use the default names for the ToS Marker Classes, but it is recommended that you provide meaningful names.

- Step 5** Assign values to the ToS Marker Classes.

Values must be in the range from 0 to 63.



Note When defining filter rules and service rules, the names and values of ToS Marker Classes are displayed in drop-down lists in the format “name [value]”. For example, “ToS 1 [23]” or “My P2P ToS [1]”

- Step 6** Click **OK**.

Your changes are saved.

The ToS Marking Settings dialog box closes.

Managing Quotas

- [How to Add Quota Profiles, page 9-83](#)
- [How to Edit Quota Profiles, page 9-86](#)
- [How to Delete Quota Profiles, page 9-91](#)
- [How to Edit Quota Management Settings for Packages, page 9-91](#)
- [How to Select Quota Buckets for Rules, page 9-93](#)
- [How to Edit Breach-Handling Parameters for a Rule, page 9-94](#)

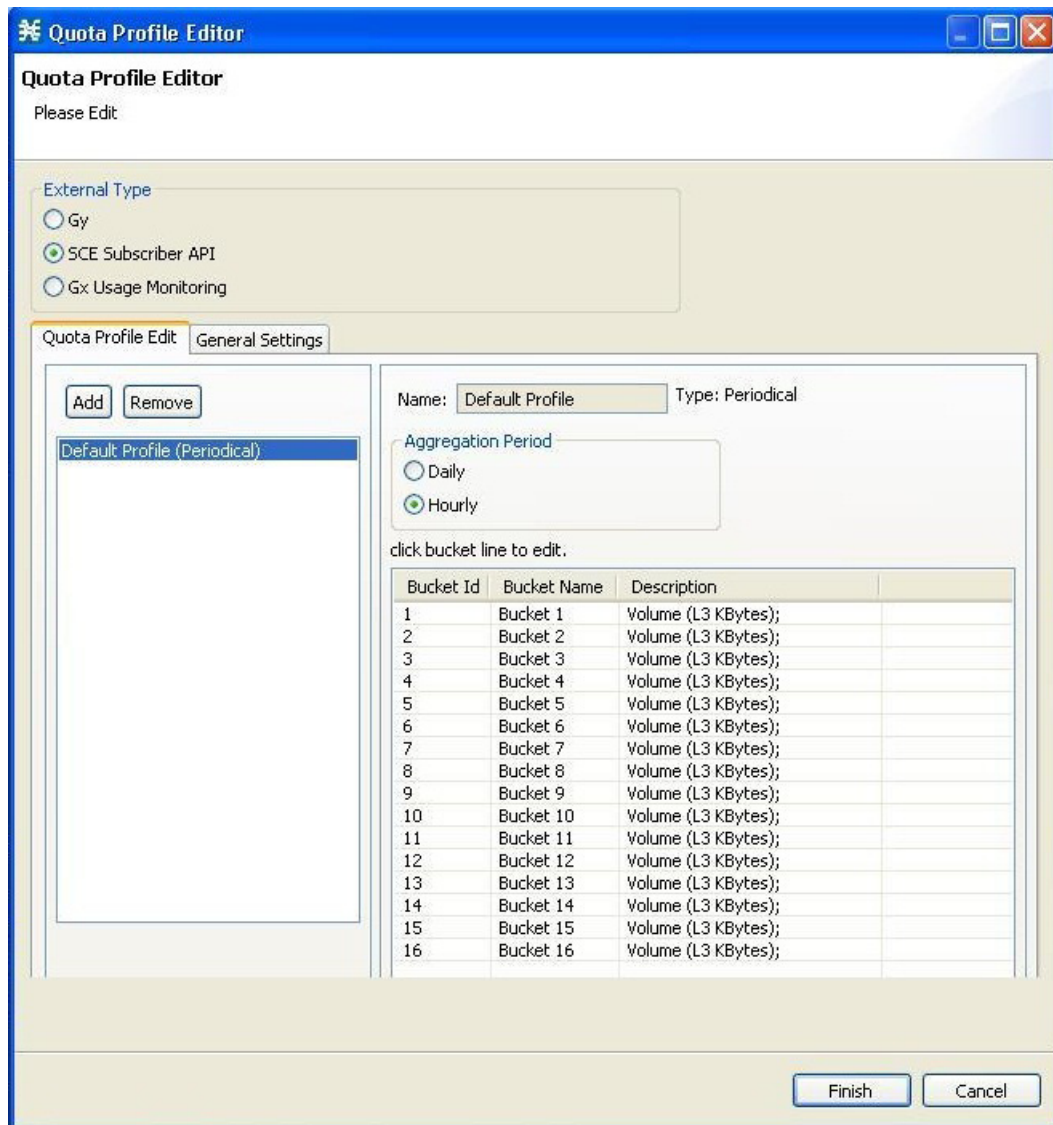
How to Add Quota Profiles

You can add and define new profiles and edit existing profiles. Additionally, you can add up to 16 new buckets.

You also define the quota buckets associated with the package. Rules can use quota buckets to set limits to the consumption of particular service groups (see [“How to Select Quota Buckets for Rules” section on page 9-93](#)).

- Step 1** From the Policies tab in the left pane, choose **Configuration > Policies > Quota Settings**.
The Quota Profile Editor dialog box appears (Figure 9-65).

Figure 9-65 Quota Profile Editor



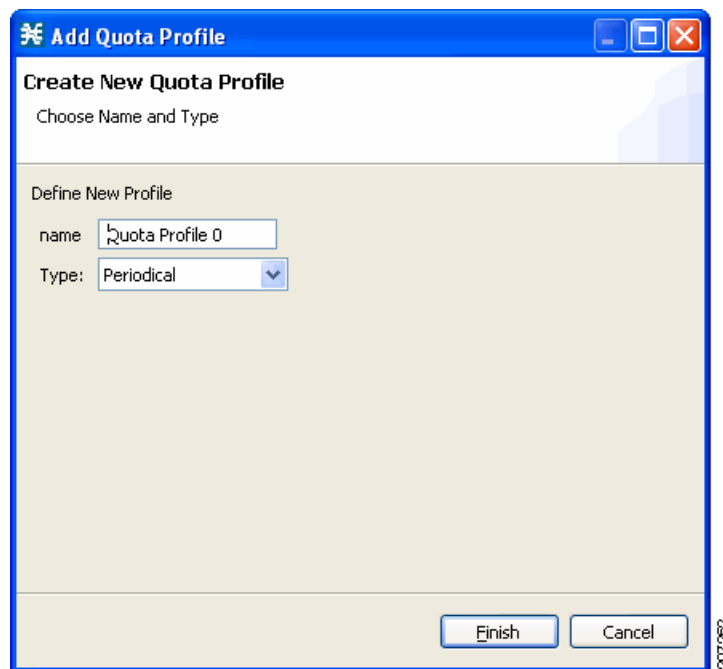
- Step 2** Select one of the **External Type** radio buttons.
- Gy—The Gy quota model enables the Gy interface adapter to be used for the external quota management. For more information, see the *Cisco Service Control Mobile Solution Guide*.
 - SCE Subscriber API—The Subscriber API enables the external applications (policy servers) to connect directly to the Cisco SCE for subscriber provisioning. For more information, see the *Cisco SCMS SCE Subscriber API Programmer Guide*.
 - Gx Usage Monitoring—Gx Usage Monitoring enables the Gx interface to generate usage monitoring reports. For more information, see the *Cisco Service Control Mobile Solution Guide*.

**Note**

Using periodical quota management, you can scatter quota replenishment so that the quota of all subscribers is not replenished at the same time. (See “[Quota Replenish Scatter](#)” section on page 9-91.)

- Step 3** For Periodical quota profile, select one of the Aggregation Period radio buttons to specify when the quota is renewed for the package:
- Hourly—Replenishes quota at each hour change
 - Daily—Replenishes quota at midnight
- Step 4** In the **Quota Profile Edit** tab, click **Add**.
The Add Quota Profile dialog box appears ().

Figure 9-66 Add Quota Profile



- Step 5** In the Name field, enter a unique name for the new quota profile.
- Step 6** Select the Type from the drop-down list.
- Periodical
 - Subscriber SCE API
- Step 7** Click **Finish**.

The Add Quota Profile window closes.

The new profile is added to the list of profiles displayed in the left (Quota Profile Edit) pane.

How to Edit Quota Profiles

You can edit the profiles to update the bucket profile.

**Note**

You cannot edit or remove the default profile.

Step 1 From the Policies tab in the left pane, choose **Configuration > Policies > Quota Settings**.

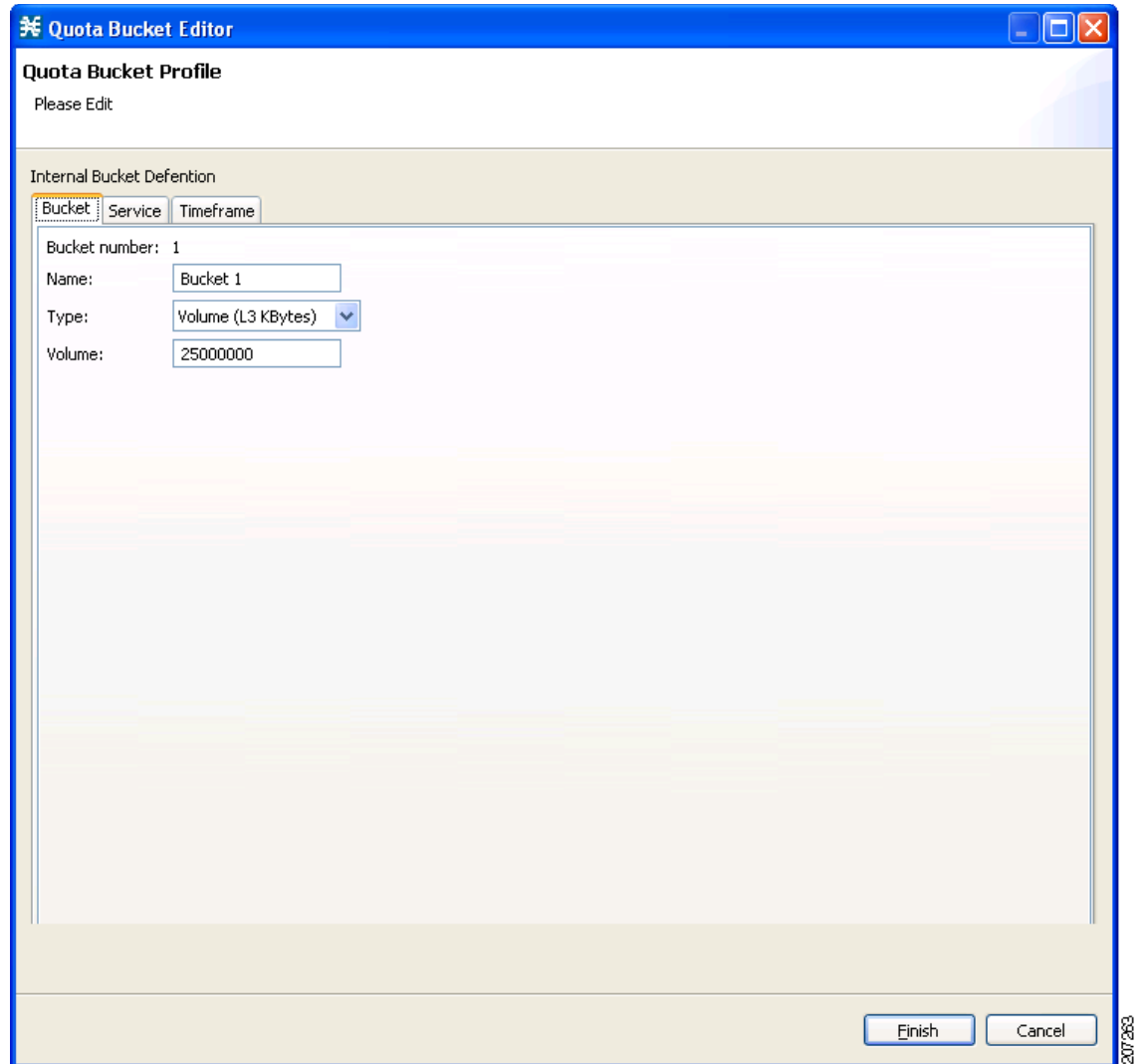
The Quota Profile Editor dialog box appears ([Figure 9-71](#)).

Step 2 Select a quota profile from the profile tree.

All the buckets defined for the selected profile are listed on the right pane.

- Step 3** Double-click a bucket line in the right pane.
The Quota Bucket Editor window appears (Figure 9-67).

Figure 9-67 Quota Bucket Editor



- Step 4** Change the Name, Type, and Volume.

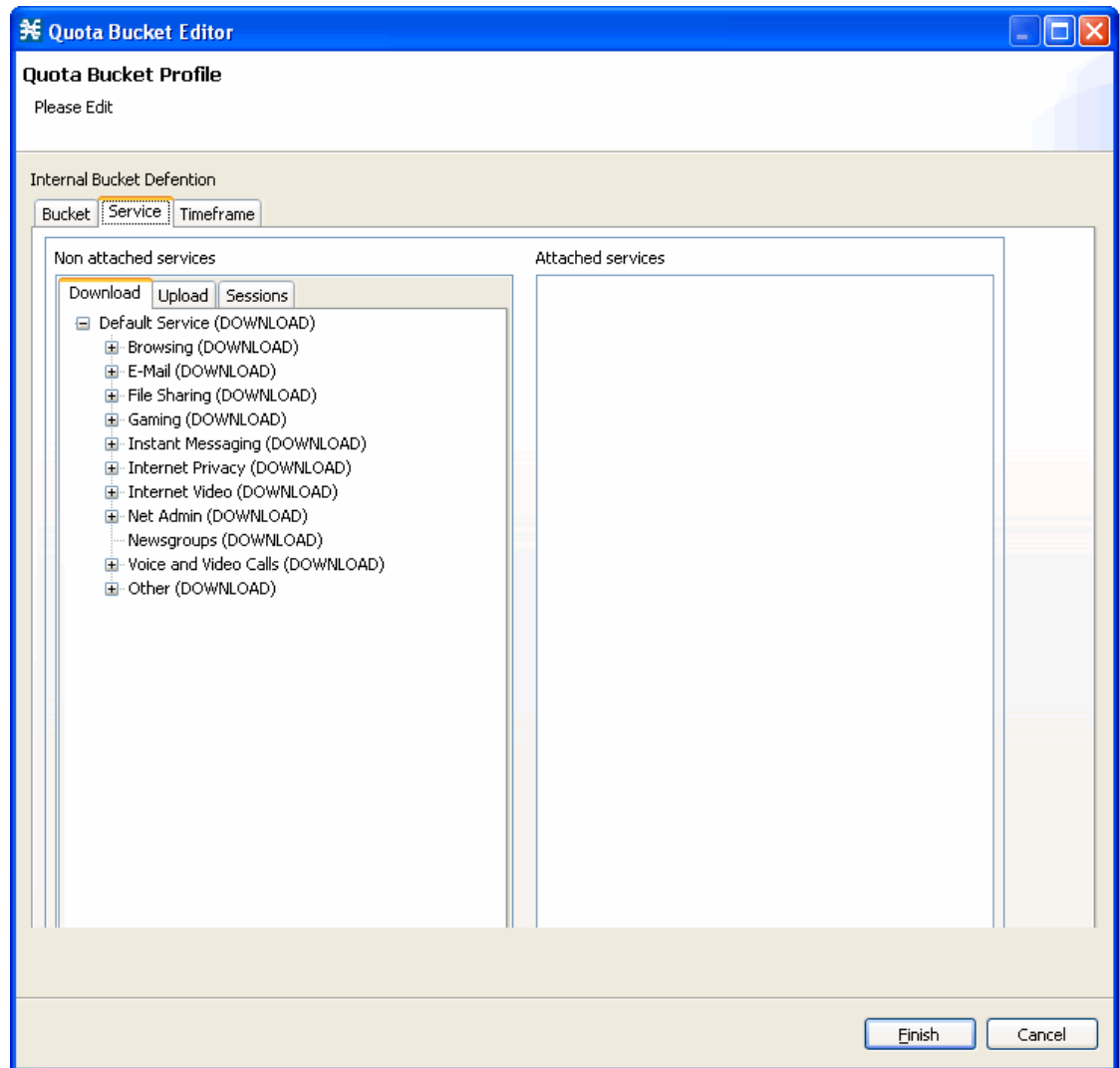


Note

You can use the default name for the bucket. It is recommended that you enter a meaningful name.

Step 5 Click on the Service tab, to associate the services to the quota profile (Figure 9-68).

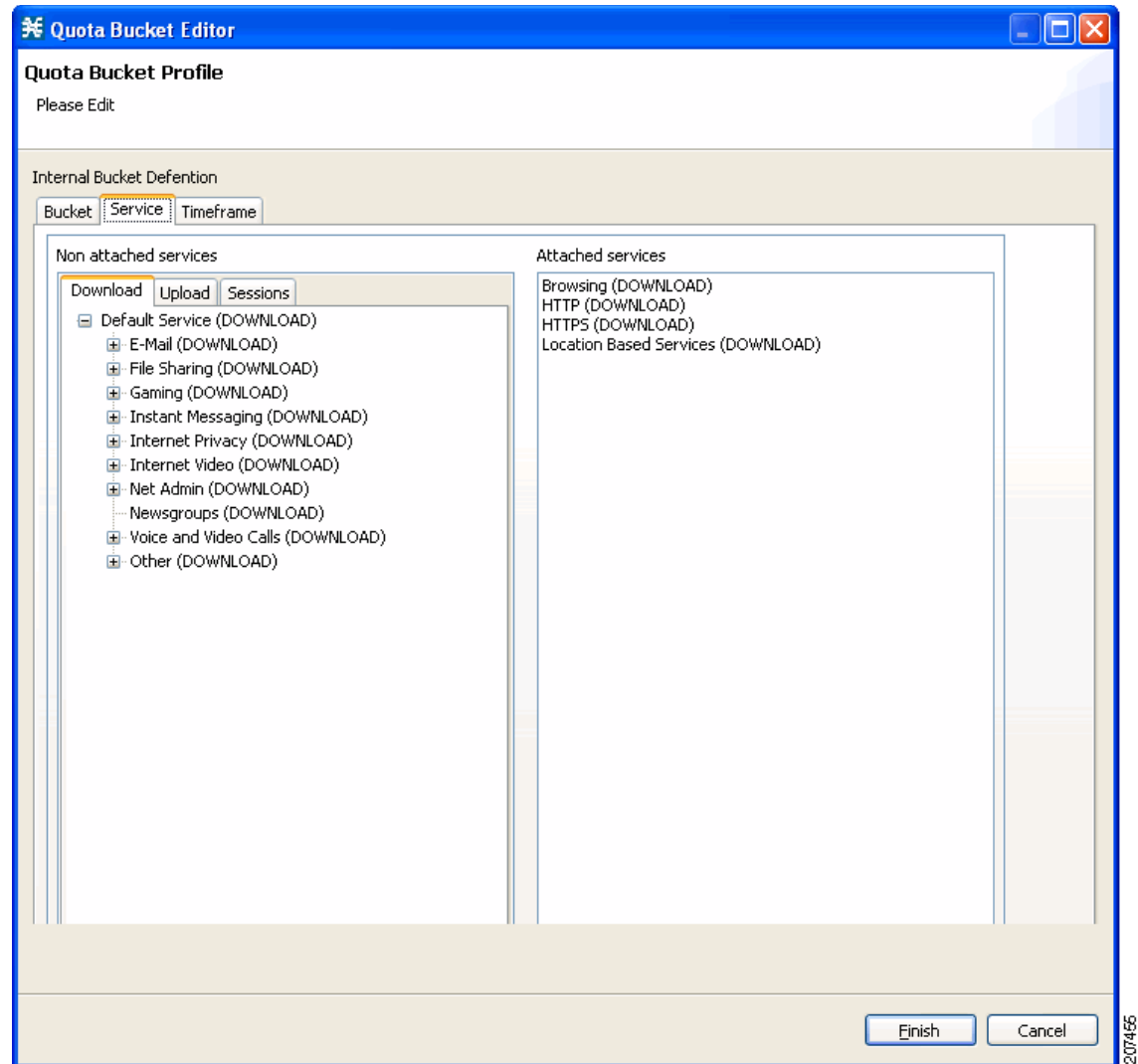
Figure 9-68 Quota Bucket Editor - Service



Step 6 Select a service from the Non Attached Service pane and move it to the Attached Service pane on the right.

The selected service is moved along with its sub services (Figure 9-69).

Figure 9-69 Quota Bucket Editor - Attached Service

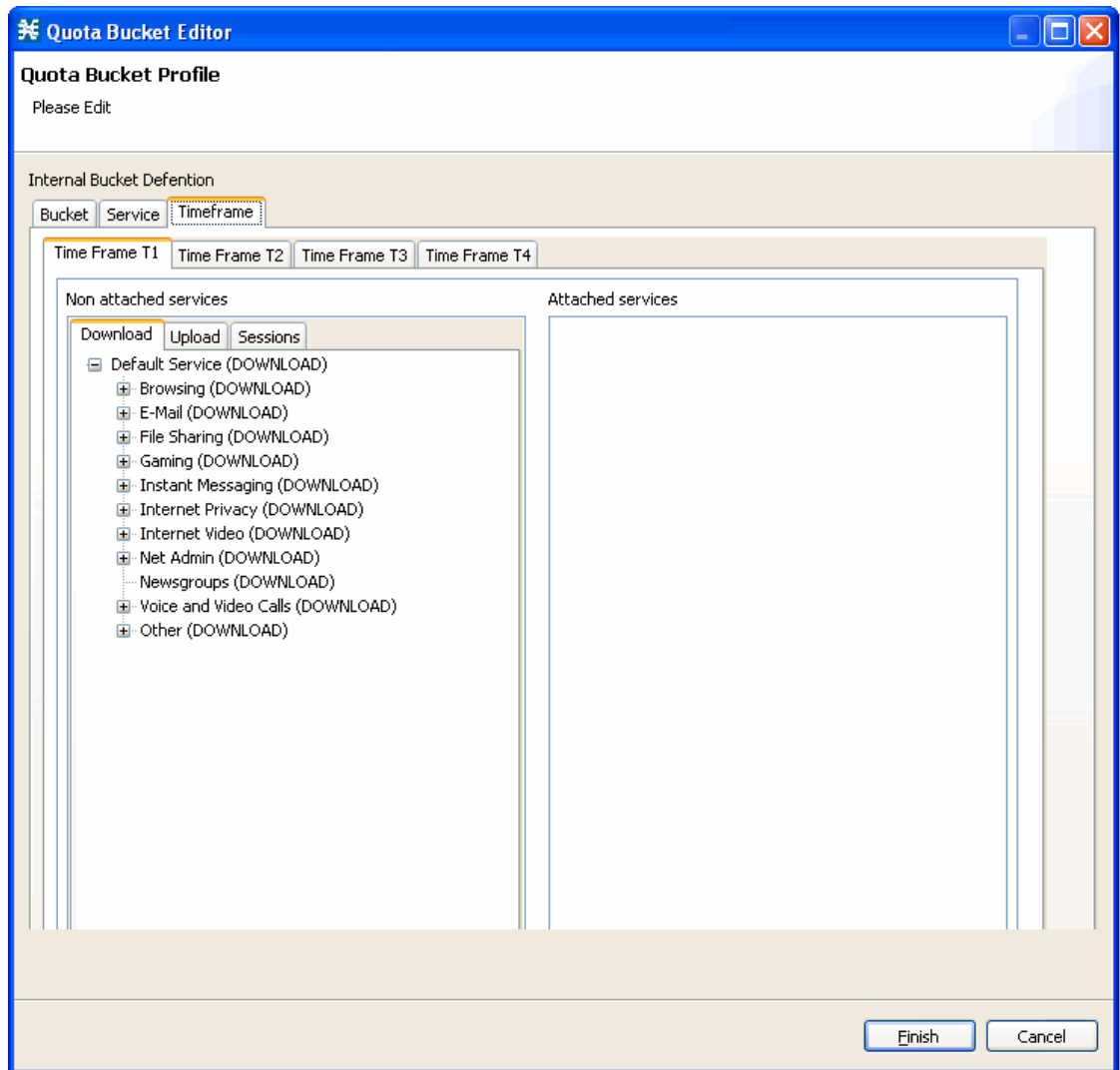


Based on the bucket type, you can select services from the following tabs:

- Download
- Upload
- Session

Step 7 Click on the Timeframe tab, to associate different timeframes to the quota profile (Figure 9-70).

Figure 9-70 Quota Bucket Editor - Timeframe



Step 8 Select a service from the Non Attached Service pane and move it to the Attached Service pane on the right.

The selected service is moved along with its sub services.

Based on the bucket type, you can select services from the following tabs:

- Download
- Upload
- Session

- Step 9** Click **Finish**.
The Quota Bucket Editor closes.
- Step 10** Click **Finish**. The Quota Profile Editor closes.
-

What to Do Next

To select a service to which the rule relates to, see [“How to Add Rules to a Package”](#) section on page 9-63.

How to Delete Quota Profiles



Note The default profile cannot be deleted.

- Step 1** From the Policies tab in the left pane, choose **Configuration > Policies > Quota Settings**.
The Quota Profile Editor dialog box appears ([Figure 9-71](#)).
- Step 2** Select a quota profile from the profile tree.
- Step 3** Click **Remove**.
- Step 4** Click **Finish**.
The Quota Profile Editor dialog box closes.
-

How to Edit Quota Management Settings for Packages

You can define whether an external quota manager or the Cisco SCA BB performs the quota management for a package.

Quota Replenish Scatter

By default, if subscriber quota is replenished using periodical quota management, the quota of all subscribers is replenished at the same time. To smooth quota replenishment, you can scatter the time of quota replenishment.

To activate this feature, enter a non-zero value for the Length of the time frame for quota replenish scatter (minutes) property of the Advanced Options tab of the Systems Settings dialog box (see [“Managing Advanced Service Configuration Options”](#) section on page 10-58). By default, this property has a value of zero, that is, all quota is replenished at the same time.

Quota for each subscriber is replenished at a random time within the quota replenish scatter time frame, with replenish events split evenly before and after the quota aggregation time.

Best results are obtained if the scatter time frame is the same length as the quota aggregation period, which should completely smooth replenish events. Do not enter a value larger than the quota replenish period. Therefore, for an hourly quota replenish period, set the scatter to 60 minutes.

The quota replenish scatter function is independent of all other quota management parameters.


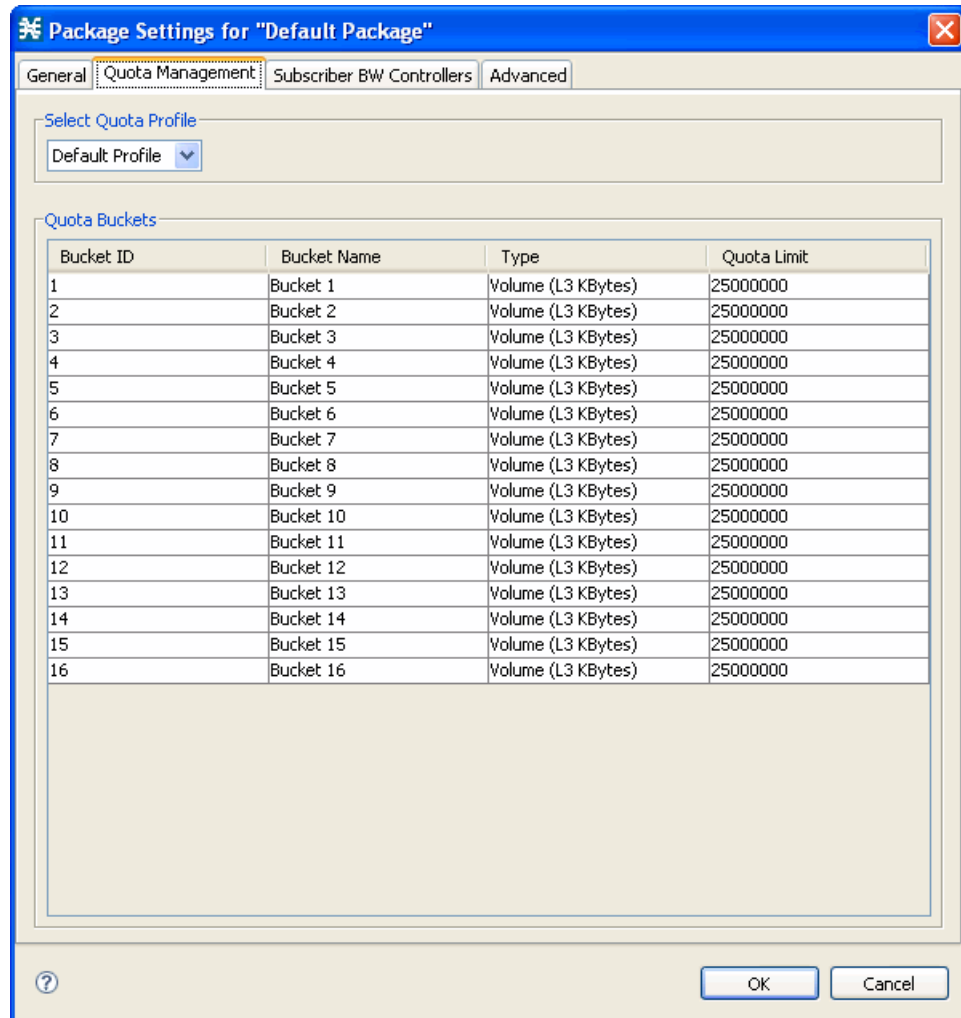
- Step 1** In the Policies tab, select a package from the package tree, and click the **Edit Package** () icon. The Package Settings dialog box appears.
- Step 2** In the Package Settings dialog box, click the **Quota Management** tab. The Quota Management tab opens ([Figure 9-71](#)).

Figure 9-71 Quota Management Tab



- Step 3** Select the Select quota profile from the drop-down list.

- Step 4** Click **OK**.

The Package Settings dialog box closes.

All changes to the quota management settings are saved.

How to Select Quota Buckets for Rules

Select the quota buckets that the flows mapped to a rule uses. The quota buckets are defined during package setup (see “[How to Edit Quota Management Settings for Packages](#)” section on page 9-91). If no quota bucket is appropriate for the rule, add a new quota bucket to the package or edit an existing bucket.


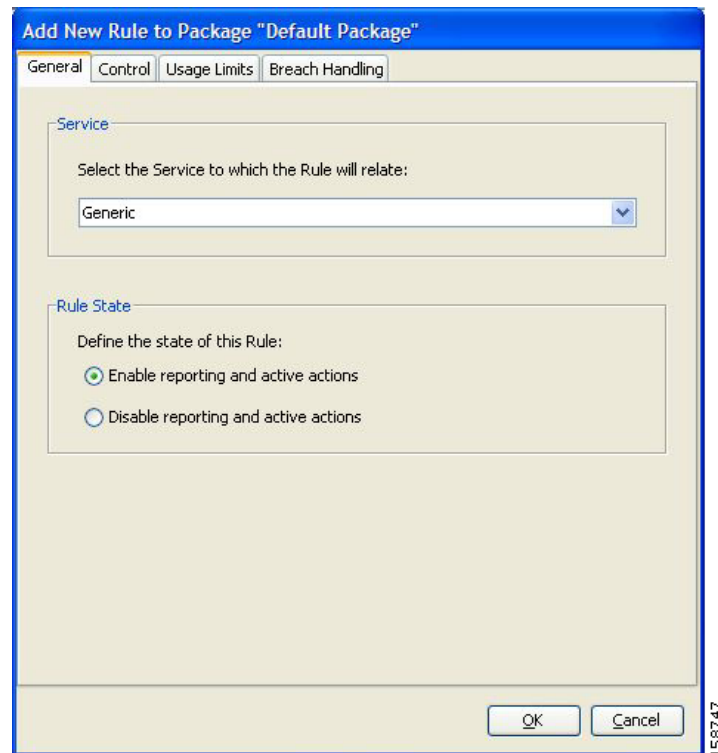
- Step 1** In the Network Traffic tab, select a package from the package tree.
- Step 2** In the right (Rule) pane, click the **Add Rule** () icon.
- The Add New Rule to Package dialog box appears ([Figure 9-72](#)).

Figure 9-72 Add New Rule to Package



- Step 3** In the Service area, select a service from the Select the Service to Which the Rule Relates drop-down list.

Step 4 Click the **Usage Limits** tab (Figure 9-73).

Figure 9-73 Usage Limits Tab



Step 5 The Usage Limits tab displays the package profile details.

The quota bucket selected for the rule is displayed. For more information on adding services to quota profile, see [Step 5](#) of the “[How to Edit Quota Profiles](#)” section on page 9-86 section.

Step 6 Click **OK**.

The Edit Rule for Services dialog box closes.

How to Edit Breach-Handling Parameters for a Rule

You can define the Cisco SCE platform behavior when an aggregated volume limit or the total number-of-sessions limit is exceeded. You can also notify subscribers when they exceed their quotas.

Breach-Handling Parameters

The following are the configuration parameters in the Breach Handling tab of the Edit Rule for Service Settings dialog box.

- You determine what happens to flows identified as belonging to this rule when a quota is breached:
 - No changes to active control—Flows mapped to this rule are not affected when quota is breached. Cisco SCA BB can generate Quota Breach RDRs even when this option is selected (see [“How to Manage Quota RDRs”](#) section on page 8-8).
 - Block the flow—Flows mapped to this rule are blocked when quota is breached.
 - Redirect to—Redirect the flow to a specified, protocol-dependent URL, where a posted web page explains the reason for the redirection. URL redirection sets are defined in the System Settings dialog box. (See [“How to Add a Set of Redirection URLs”](#) section on page 10-52.) Only three protocol types support redirection: HTTP, HTTP Streaming, and RTSP. Redirection is not supported when unidirectional classification is enabled.
 - Control the flow characteristics—The behaviors of flows mapped to this rule change when quota is breached:
 - Select an upstream Bandwidth Controller—Map the traffic flow of this rule to a specific upstream BW controller (BWC). This sets up bandwidth metering of all concurrent flows mapped to this rule, based on the characteristics of the selected BWC.
 - Select a downstream Bandwidth Controller—The same functionality as the previous option, but for downstream flow.
 - Limit the flow’s upstream bandwidth—Set a per-flow upstream bandwidth limit (for flows mapped to the service of this rule).
 - Limit the flow’s downstream bandwidth—Set a per-flow downstream bandwidth limit.
 - Set the flow's upstream packets ToS—Set the DSCP ToS marker of all packets of upstream flows.
 - Set the flow's downstream packets ToS—Set the DSCP ToS marker of all packets of downstream flows.
 - Limit concurrent flows of this Service—Set the maximum number of concurrent flows (mapped to this rule) permitted to a subscriber.
- Activate a Subscriber Redirect—Activate a Subscriber Redirect when subscribers exceed their quota limit.
- Activate a Subscriber Notification—Activate a Subscriber Notification when subscribers exceed their quota limit. This notification can, for example, convey the quota breach situation to the subscriber and explain how to obtain additional quota.



Note

Subscriber notification is not supported when unidirectional classification is enabled.

To define Subscriber Notifications, see [“Managing Subscriber Notifications”](#) section on page 10-41.

- Activate Traffic Mirroring—Activate traffic mirroring when subscribers exceed their quota limit

Step 1 In the Policies tab, select a package from the package tree.

Step 2 In the right (Rule) pane, select a rule.


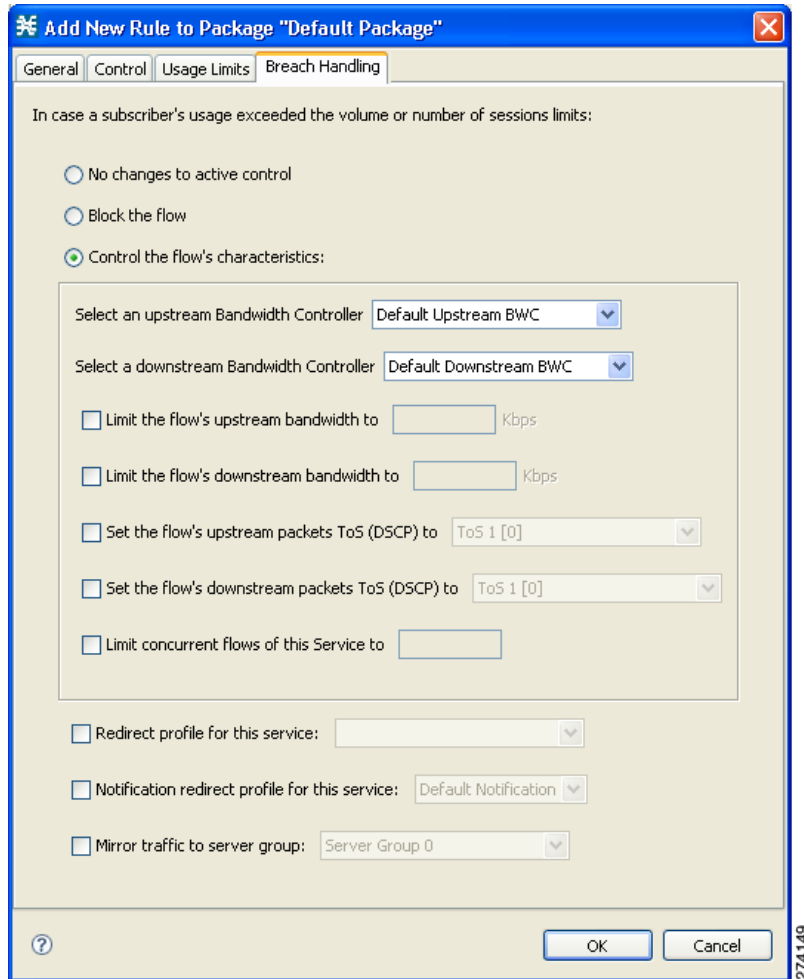
- Step 3** Click the **Edit Rule** () icon.
The Edit Rule for Service dialog box appears.
- Step 4** Click the Breach Handling tab.
The Breach Handling tab opens (Figure 9-74).

Figure 9-74 Breach Handling Tab



- Step 5** Set the behavior of the flow when quota is breached.
- To block the flow when quota is breached, continue at [Step 6](#).
 - To change the characteristics of the flow when quota is breached, continue at [Step 10](#).
 - To leave the flow unchanged when quota is breached, select the **No changes to active control** radio button and continue at [Step 11](#).
- Step 6** To block the flow, select the **Block the flow** radio button.
- Step 7** Continue at [Step 10, page 350](#).

Step 8 Change the characteristics of the flow.

Select the **Control the flow's characteristics** radio button.

The options in the Flow Characteristic area are enabled:

- From the upstream Bandwidth Controller drop-down list, select an upstream BWC

The BWCs in this drop-down list are defined when creating or editing the package.

When the mouse is placed over the drop-down list, a tooltip appears. The tooltip contains the properties of the selected BWC, such as PIR, CIR, AL, and Global Controller.

- From the downstream Bandwidth Controller drop-down list, select a downstream BWC.
- (Optional) Check the **Limit the flow's upstream bandwidth** check box and enter a value in the Kbps field.
- (Optional) Check the **Limit the flow's downstream bandwidth** check box and enter a value in the Kbps field.
- (Optional) Check the **Set the flow's upstream packets ToS (DSCP) to** check box and select a value from the drop-down list.
- (Optional) Check the **Set the flow's downstream packets ToS (DSCP) to** check box and select a value from the drop-down list.
- (Optional) Check the Limit concurrent flows of this Service check box and enter a value in the associated field. (Optional) To enable subscriber

Step 9 (Optional) To enable subscriber redirect, check the check box, and select a redirect profile from the drop-down list.

Step 10 (Optional) To enable subscriber notification, check the Notification redirect profile for this service check box and select a notification redirect profile from the drop-down list.



Note A subscriber notification can be activated in addition to any of the three breach-handling options.



Note Subscriber notification is not supported when unidirectional classification is enabled. If you try to check the Activate a Subscriber Notification check box when unidirectional classification is enabled, a Rule Error message appears.

Step 11 Click **OK** to continue.

Step 12 (Optional) To enable mirror traffic to a server group, check Mirror traffic to server group and choose a server group to send the mirror traffic to.



Note The Mirror traffic to server group check box is only enabled when Traffic Mirroring is enabled in the VAS Settings dialog box.

Step 13 Click **OK**.

The Edit Rule for Service dialog box closes.

All changes to the rule are saved.

Example: Creating Tiered Subscriber Services

Tiered subscriber services can be implemented using the Cisco SCA BB Console. Because the definition of such services is open ended, this section describes how to define two of the tiers outlined in the value proposition description. The two tiers are defined as follows:

- Silver
 - Weekly bandwidth limited to 4.2 GB (corresponds to a daily limit of 600 MB)
 - Email and browsing services are limited to 256 kbps
 - Audio and video streaming services are limited to 64 kbps
 - P2P services are limited to 28 kbps
- Gold
 - Weekly bandwidth limited to 5.6 GB (corresponds to a daily limit of 800 MB)
 - Email and browsing services are not bandwidth limited
 - Audio and video streaming services are limited to 128 kbps
 - P2P services are limited to 28 kbps

The following steps are applicable to both the 'Silver' and 'Gold' packages.

Step 1 Create a new package as described in [“How to Add Packages” section on page 9-55](#).

Step 2 Enable periodical (internal) quota management.

- a. Set the aggregation period to Daily
- b. Set the quota limit to the desired value and give the quota bucket a meaningful name

For further information, see [“How to Edit Quota Management Settings for Packages” section on page 9-91](#).

Step 3 Add the bandwidth controllers for the required services and set the PIR to the desired rate.



Note Each service that is bandwidth limited requires a sub bandwidth controller that is a child of the primary bandwidth controller, not an extra bandwidth controller.

For further information, see [“How to Edit Package Subscriber BWCs” section on page 9-30](#).

Step 4 Add a rule to the package for each bandwidth limited service.

For further information, see [“How to Add Rules to a Package” section on page 9-63](#).

Step 5 Configure the rule to control the characteristics of the flow with the bandwidth controller for the relevant service.

For further information, see [“How to Define Per-Flow Actions for a Rule” section on page 9-66](#).

Step 6 Set the usage limit for the package to use the quota bucket defined in [Step 2](#).

For further information, see the [“How to Select Quota Buckets for Rules” section on page 9-93](#) section.

Unknown Subscriber Traffic

Cisco SCE platform processes a traffic flow that does not match any filter rule (see [“Filtering the Traffic Flows” section on page 10-23](#)). Cisco SCE platform tries to identify the subscriber responsible for the traffic flow. The platform checks its internal database for a subscriber identified by the IP address or VLAN tag of the traffic flow. If no such subscriber exists, the traffic flow is mapped to the Unknown Subscriber Traffic category.

The Unknown Subscriber Traffic category is included in the tree in the Network Traffic tab but is not part of the package hierarchy. The Unknown Subscriber Traffic category cannot be deleted.

**Note**

Traffic of one unknown subscriber cannot be distinguished from traffic of other unknown subscribers. Therefore, you cannot set either per-subscriber usage limits or subscriber-level metering with subscriber BWCs. You can use subscriber BWCs only to link a selected service to a global controller.

The Unknown Subscriber Traffic category behaves like a package with the following parameters:

- Package Name = Unknown Subscriber Traffic
- Package Index = 4999
- One package usage counter:
 - Counter Name = Unknown Subscriber Traffic Counter
 - Counter Index = 1023

You can:

- Edit the Unknown Subscriber Traffic package settings:
 - Add extra BWCs (see [“How to Edit Package Subscriber BWCs” section on page 9-30](#)).
 - Select a calendar (see [“How to Set Advanced Package Options” section on page 9-57](#)).
- Edit the default service rule for the Unknown Subscriber Traffic category:
 - Change the Rule State (see [“How to Edit Rules” section on page 9-68](#)).
 - Change per-flow actions for the rule (see [“How to Define Per-Flow Actions for a Rule” section on page 9-66](#)).
- Add rules to the Unknown Subscriber Traffic package:
 - Add rules (see [“How to Add Rules to a Package” section on page 9-63](#)); edit (see [“How to Edit Rules” section on page 9-68](#)) and delete (see [“How to Delete Rules” section on page 9-70](#)) these rules.
 - Add time-based rules (see [“How to Add Time-Based Rules to a Rule” section on page 9-72](#)); edit (see [“How to Edit Time-Based Rules” section on page 9-74](#)) and delete (see [“How to Delete Time-Based Rules” section on page 9-75](#)) these rules.

