CHAPTER 9

Using the Service Configuration Editor: Traffic Control

Revised: December 14, 2011, OL-7205-19

Introduction

The Traffic Control capabilities of the Service Control Engine (SC platform and the Cisco Service Control Application for Broadband (SCA BB) are used to limit and prioritize traffic flows. Control of traffic is based on parameters such as the service of the flow, the subscriber's package, and the subscriber's quota state.

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 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—2048 upstream and 2048 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.

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

The upstream and downstream interfaces are each assigned one default global controller that, by default, controls the total link traffic. Depending on the Cisco SCE hardware, you can add up to 1024 or 2048, more global controllers for each interface, and assign a maximum bandwidth of the total link limit to each global controller separately.

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

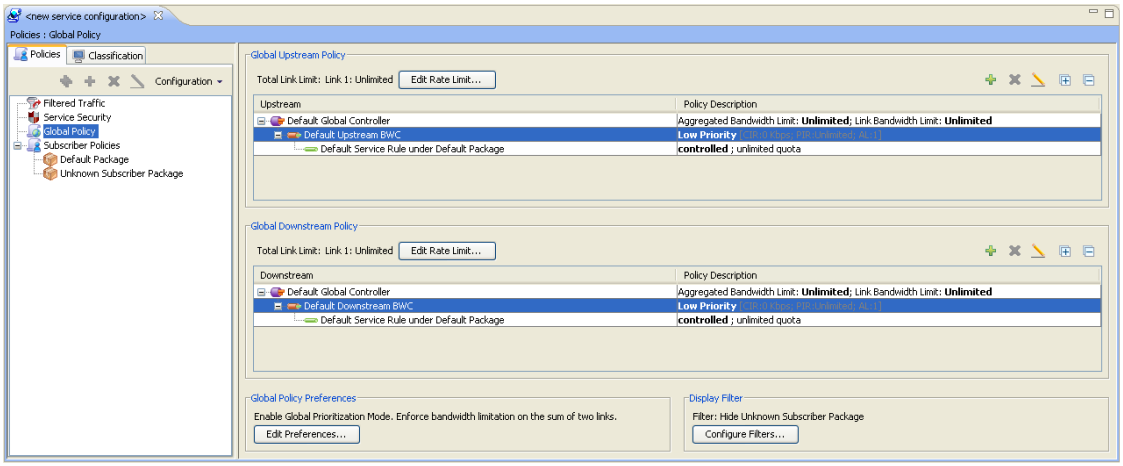
How to View Global Controller Settings

Note Global controller bandwidth is based on Layer 1 volume.
(Accounting, reporting, and subscriber bandwidth control in 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, 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 (see Managing Calendars, page 9-68):

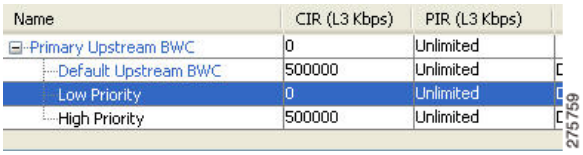
  – A single value in this field indicates that the maximum bandwidth for this global controller is constant.

  – 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

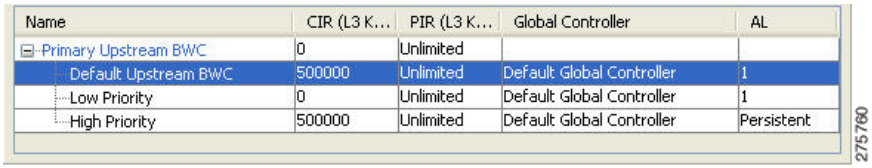
– If two time frames have the same maximum bandwidth, the value is not repeated (Figure 9-3). (So **40,,,100** means that the first three time frames have a maximum bandwidth of 40 percent of the total link limit, and the fourth time frame has a maximum bandwidth equal to the total link limit.)

Figure 9-3 Time Frame Details



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

Figure 9-4 Total Link Time



How to Filter Global Controllers

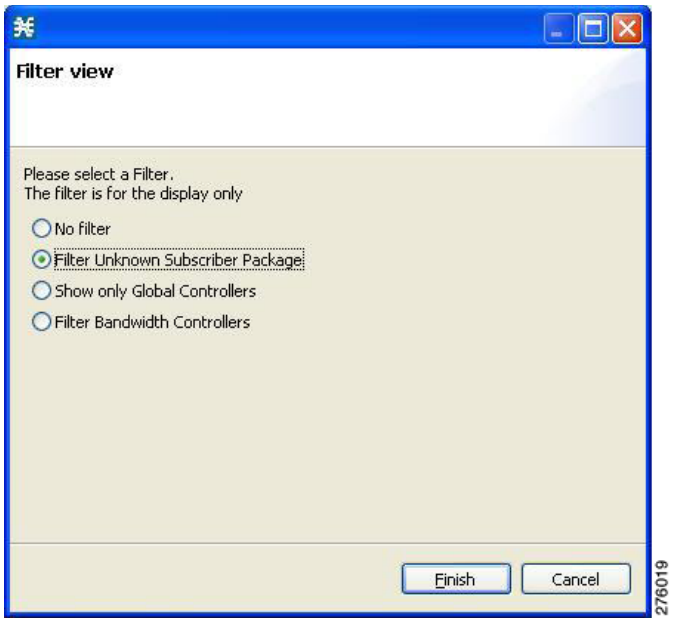
Step 1 In the Policies tab, click **Global Policy**.

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 SCE link passing through the SCE platform.

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

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

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

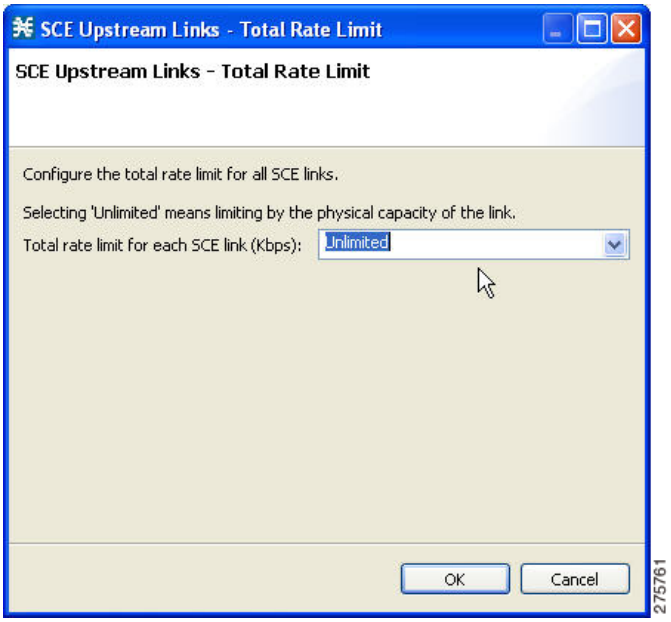
Step 1 In the Policies tab, click **Global Policy**.

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 SCE link (Kbps) field.

Step 4 Click **OK**.

Your changes are saved.

The Global Controller Settings dialog box closes.

How to Add Global Controllers

Depending on the Cisco SCE hardware, you can add up to 1024 or 2048 upstream global controllers and 1024 or 2048 downstream global controllers to a service configuration.

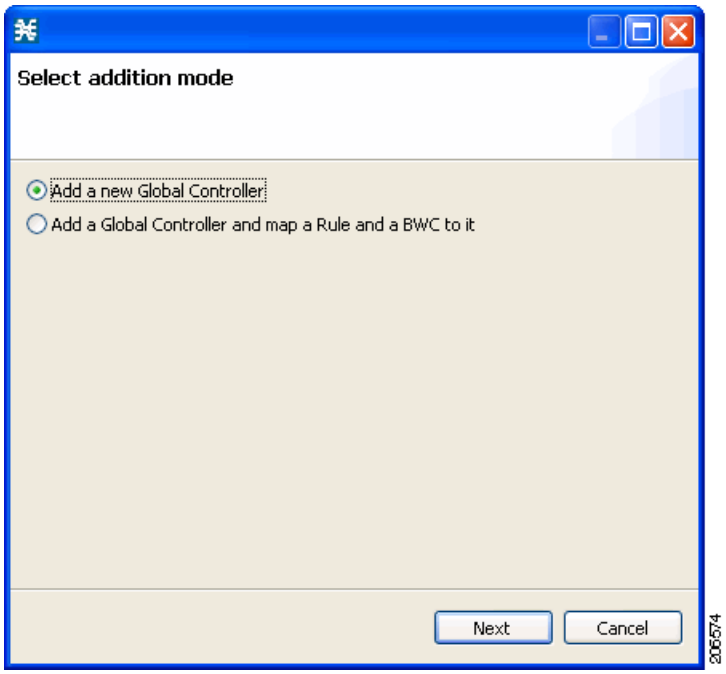
Step 1 In the Policies tab, click **Global Policy**.

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 (**Add**).

The Select Addition mode dialog box appears (Figure 9-7).

Figure 9-7 Select Addition Mode



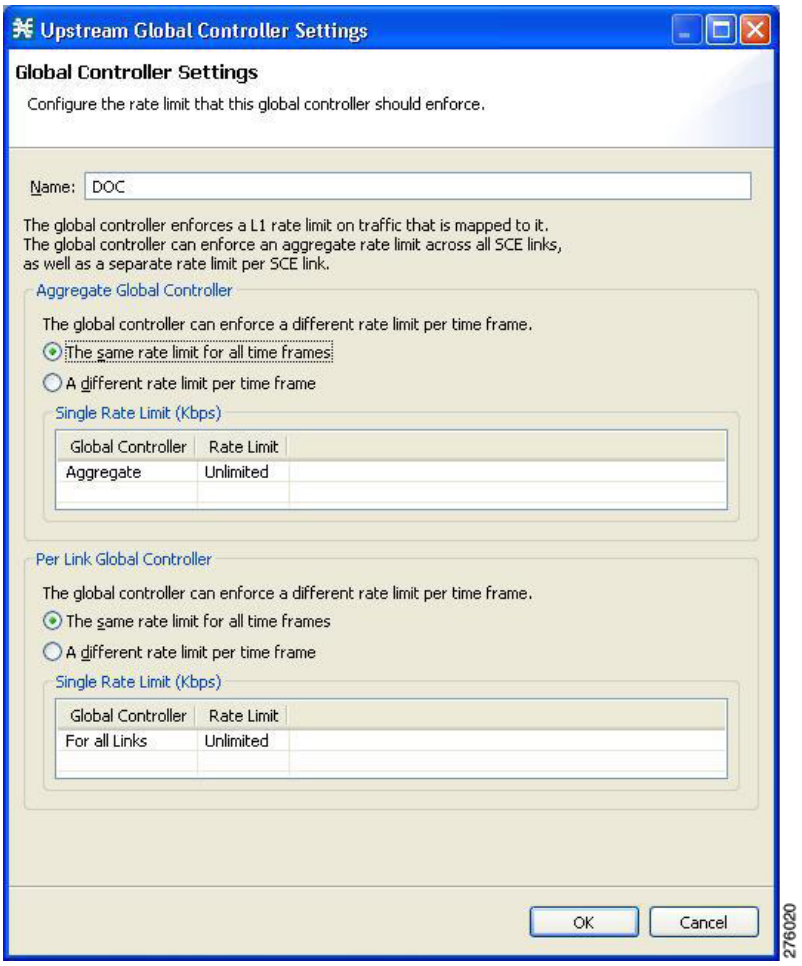
Step 3 Choose the **Add a new Global Controller** radio button.

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



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.

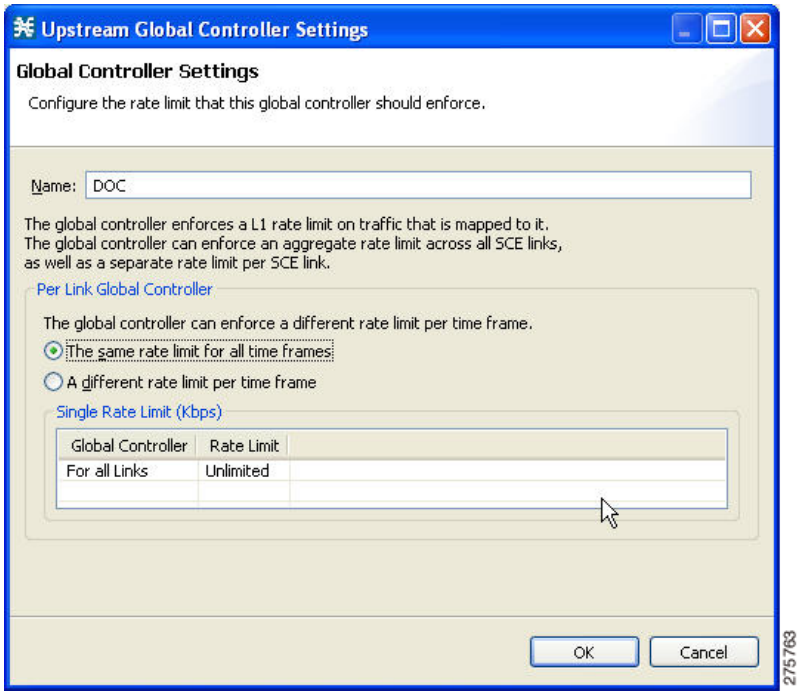
Step 2 Select a global controller.

Step 3 Click (**Edit**).

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



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

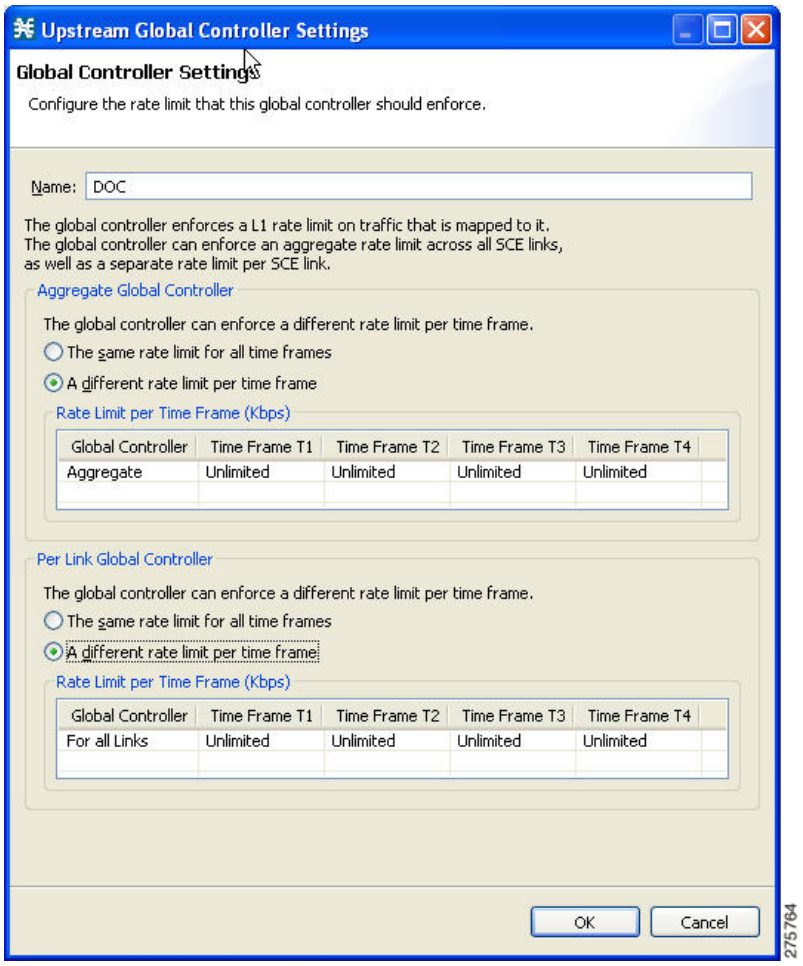
- Choose the **The same rate limit for all time frames r**adio button, and in the Single Rate Limit (Kbps) field, enter the desired value in Kbps for the maximum bandwidth.

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



Note These values will be 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  (**Delete**).

Note If a subscriber BWC is using the specified global controller (see How to Edit Package Subscriber BWCs, page 9-29), 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 will result in an error message during apply policy, similar to the following:

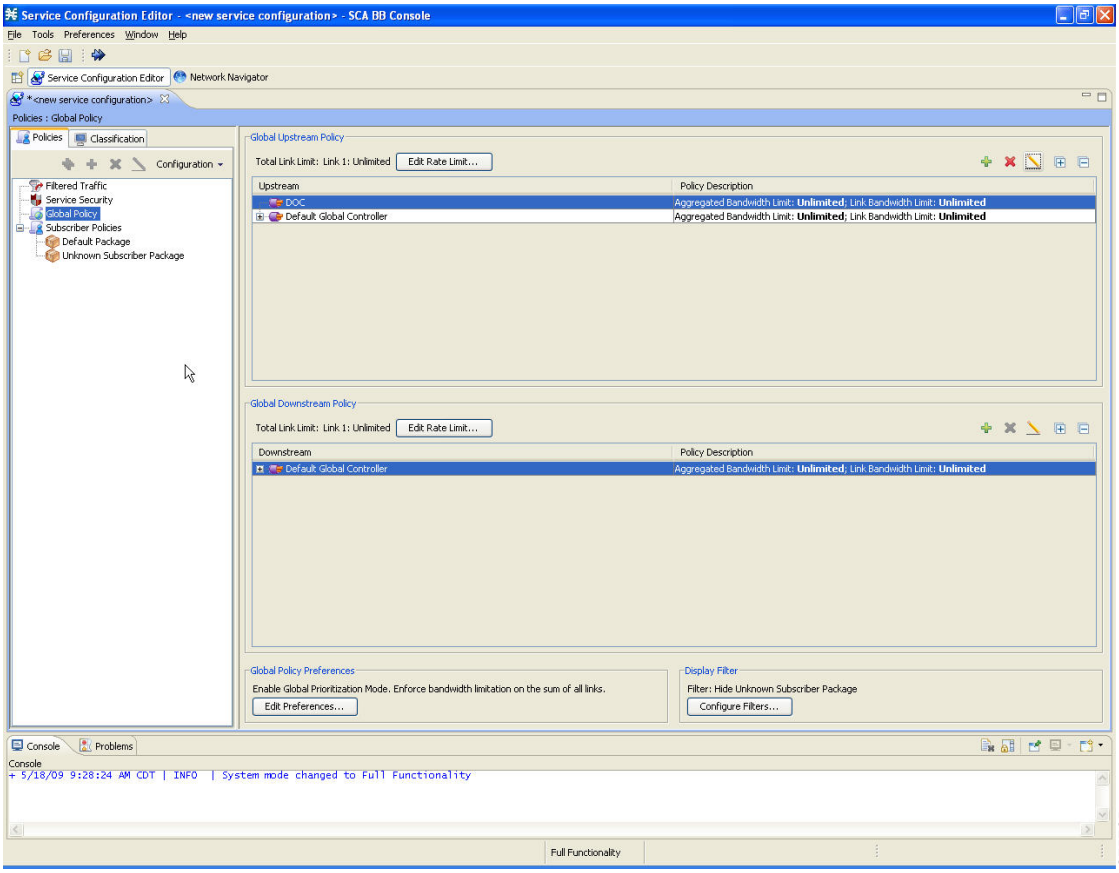
"Invalid value set on Link ID 6 for upstream GC 'Default Global Controller '. Link ID 6 does not exist. Available Link IDs: 1, 2, 3, 4"

The respective edit dialog of the Global Controller settings can be activated by (Figure 9-11):

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

Note The behavioral is the same whether configure upstream or downstream GC.

Figure 9-11 Global Controller Settings Activation



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 9-25

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**.

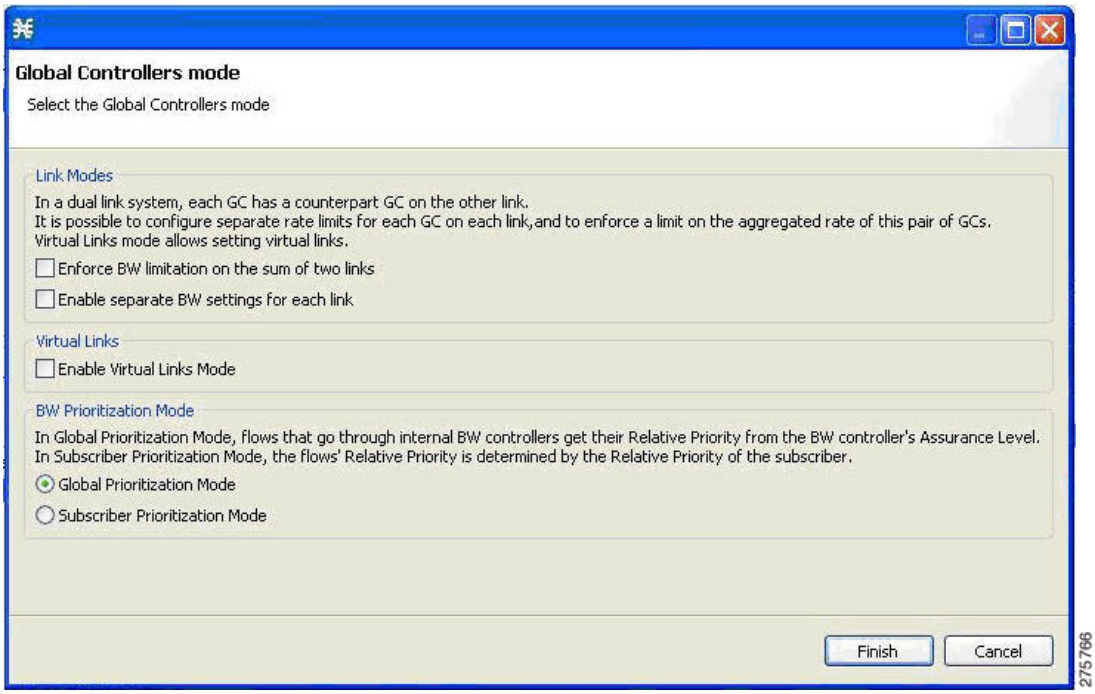
The Global Bandwidth Settings dialog box in the right (Rule) pane.

Step 2 Add global controllers, as described in How to Add Global Controllers, page 9-6.

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**.

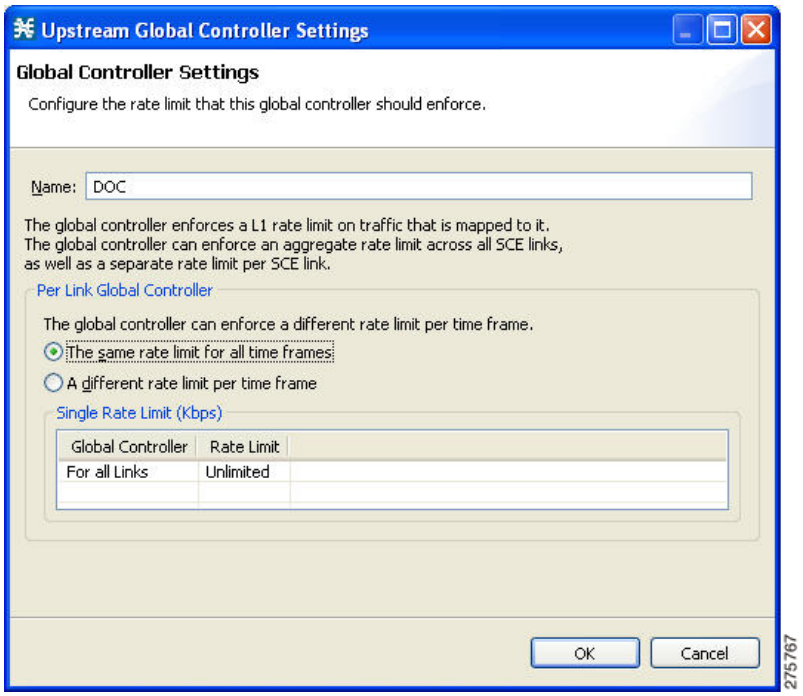
The Global Bandwidth Settings dialog box is displayed in the right (Rule) pane.

Step 7 Select a global controller.

Step 8 Click (**Edit**).

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 r**adio button.

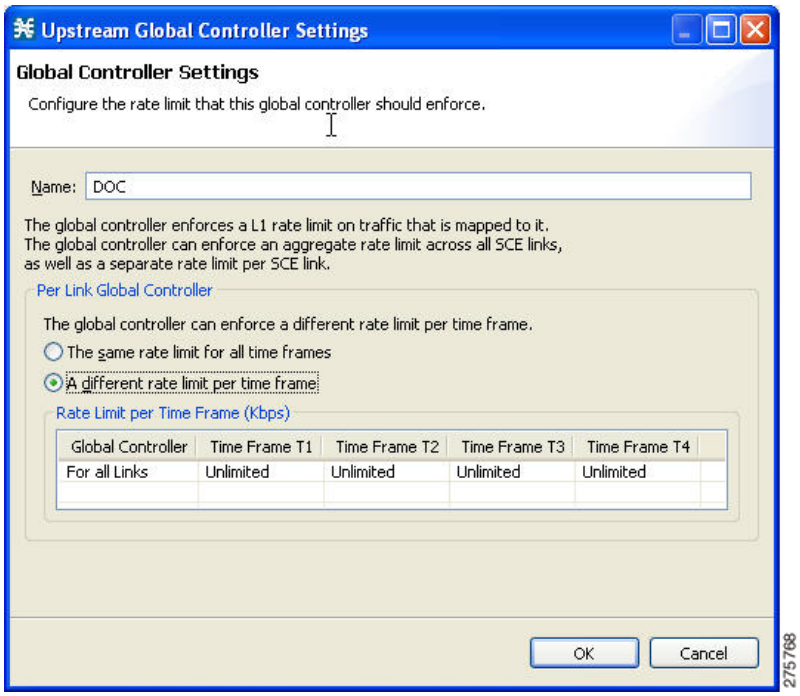
b. Enter the desired value in Kbps for the maximum bandwidth in the Rate limit for the Per Link Global Controller (in Kbps) field.

Step 10 Set the maximum limit that this global controller carries to vary according to time frame.

a. Choose the **A different rate limit per time frame** radio button.

b. Enter the desired value for each time frame (Figure 9-14).

Figure 9-14 Upstream Global Controller Settings



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**.

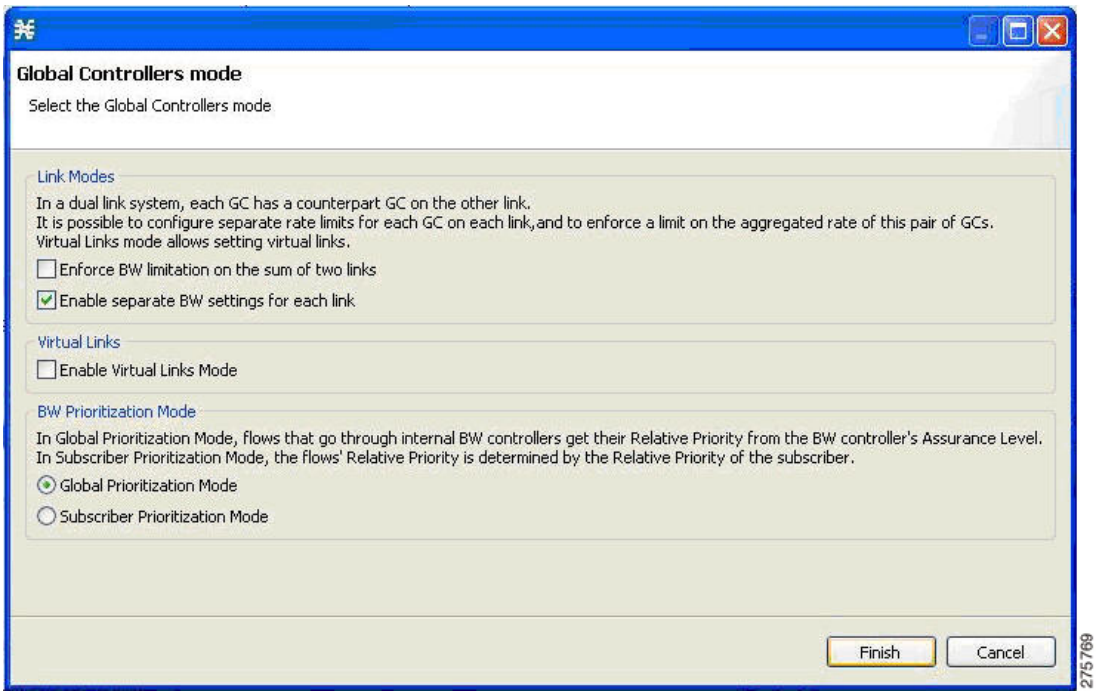
The Global Bandwidth Settings dialog box in the right (Rule) pane.

Step 2 Add global controllers, as described in How to Add Global Controllers, page 9-6.

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**.

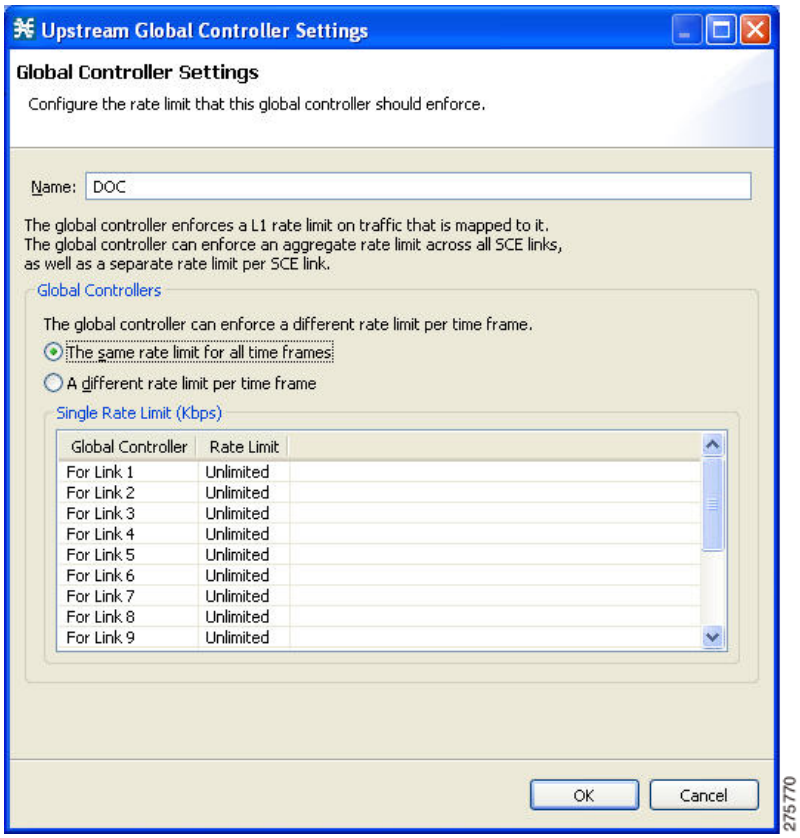
The Global Bandwidth Settings dialog box is displayed in the right (Rule) pane.

Step 7 Select a global controller.

Step 8 Click (**Edit**).

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 r**adio button

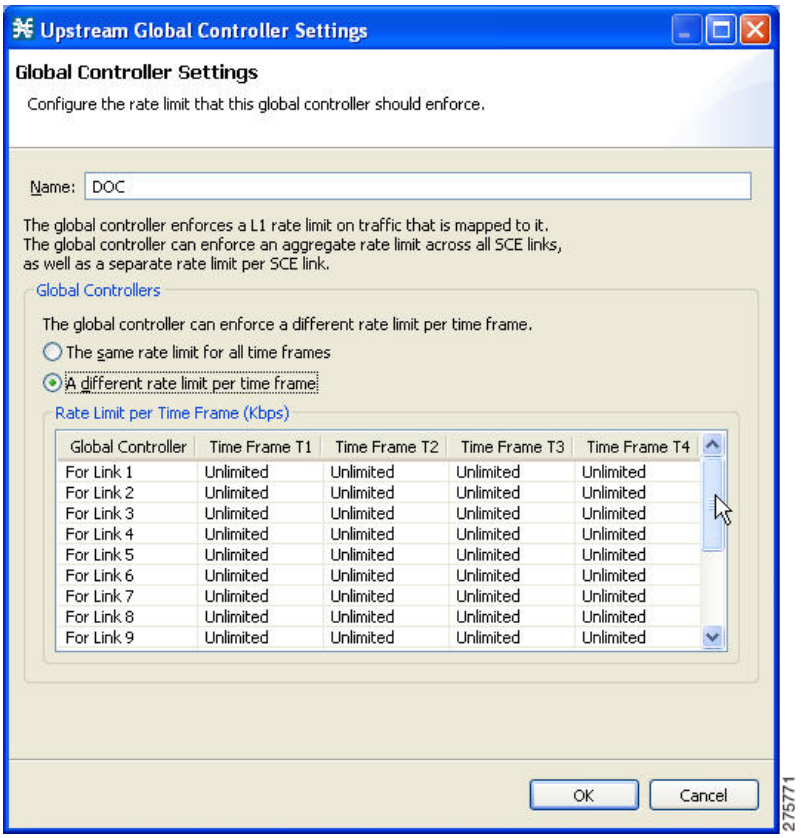
b. Enter the desired value in Kbps for the maximum bandwidth in the Rate limit for the Per Link Global Controller (in Kbps) field.

Step 10 Set the maximum limit that this global controller carries to vary according to time frame for each link.

a. Choose the **A different rate limit per time frame** radio button.

b. 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 in addition you can 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**.

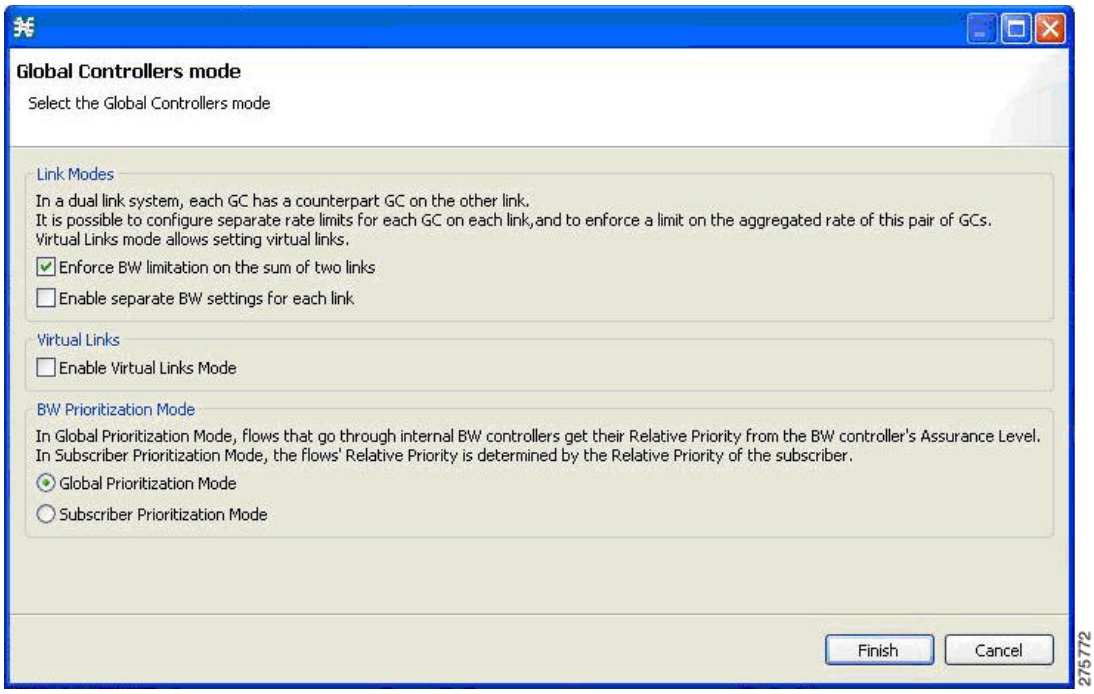
The Global Bandwidth Settings dialog box in the right (Rule) pane.

Step 2 Add global controllers, as described in How to Add Global Controllers, page 9-6.

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**.

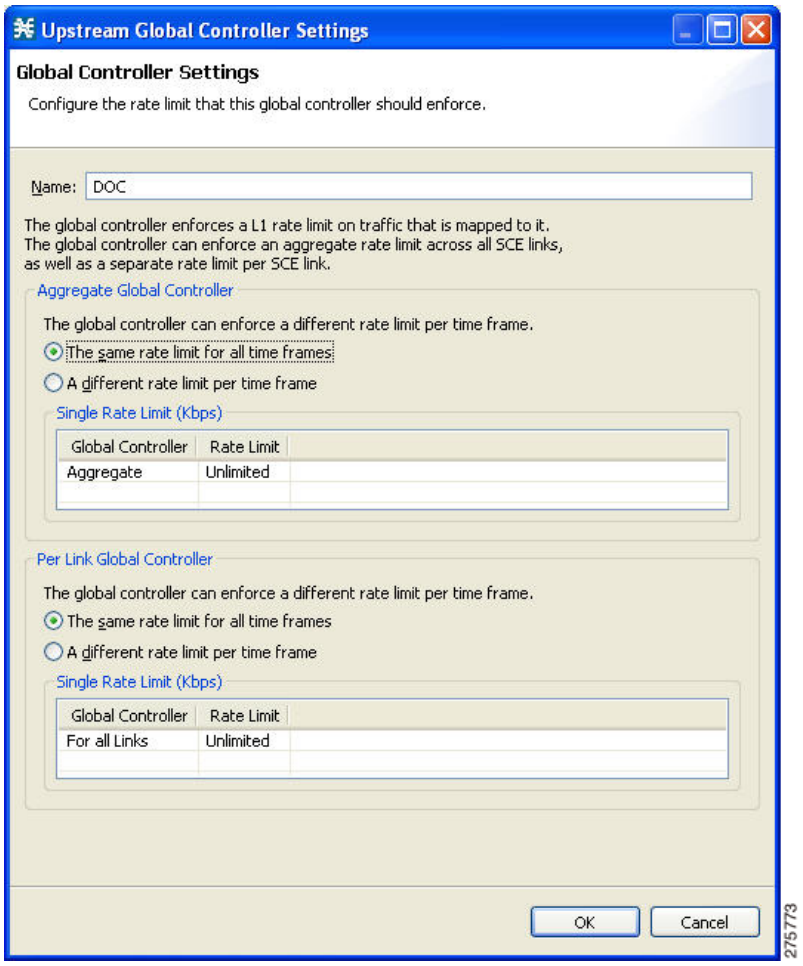
The Global Bandwidth Settings dialog box is displayed in the right (Rule) pane.

Step 7 Select a global controller.

Step 8 Click (**Edit**).

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

Figure 9-19 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 r**adio button on the Aggregate Global Controller tab.

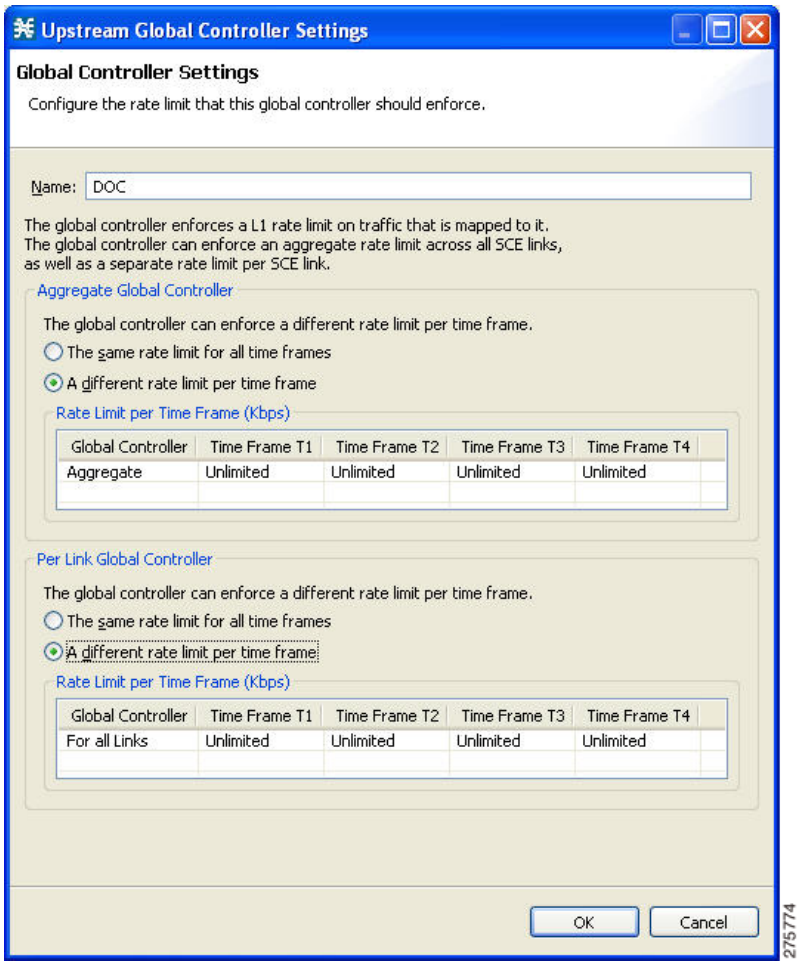
b. Enter the desired value in Kbps for the maximum bandwidth in the Rate limit for the Per Link Global Controller (in Kbps) field.

Step 10 Set the maximum limit that this global controller carries to vary according to time frame.

a. Choose the **A different rate limit per time frame** radio button the Aggregate Global Controller tab.

b. Enter the desired value for each time frame (Figure 9-20).

Figure 9-20 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 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 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 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**.

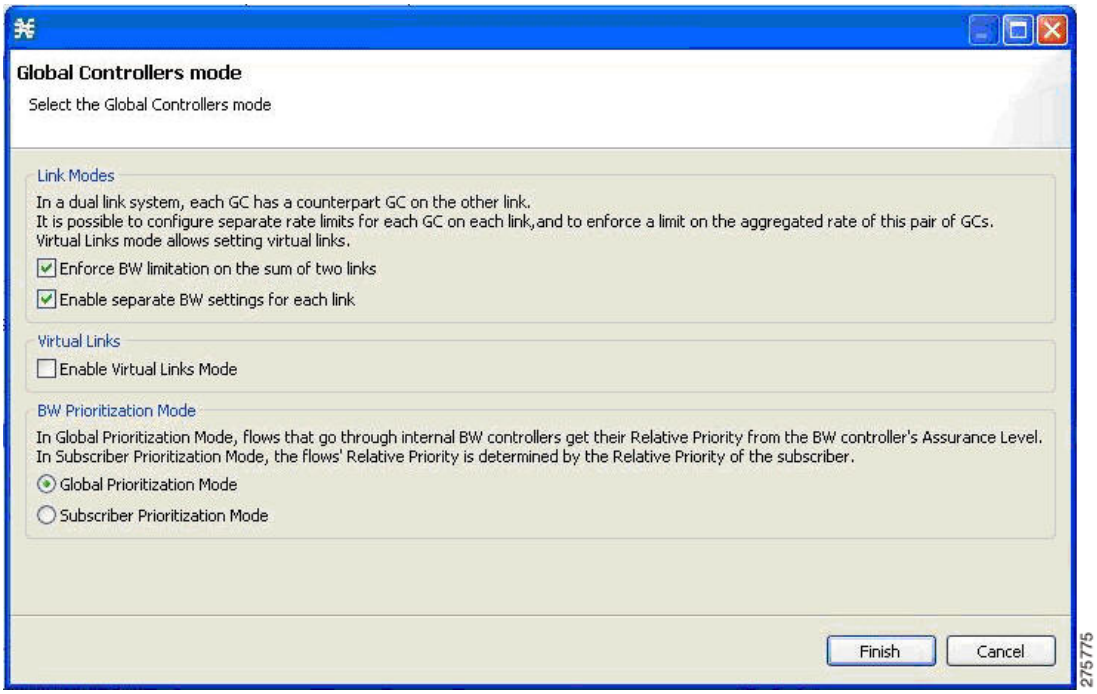
The Global Bandwidth Settings dialog box in the right (Rule) pane.

Step 2 Add global controllers, as described in How to Add Global Controllers, page 9-6.

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**.

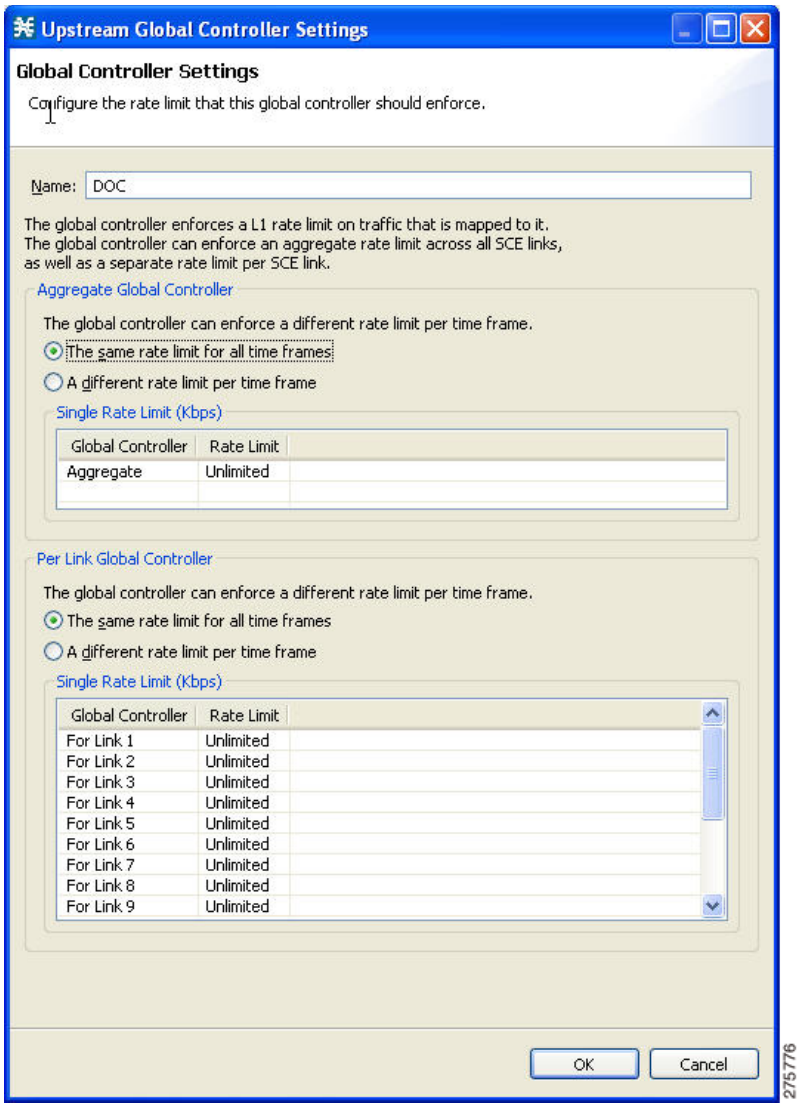
The Global Bandwidth Settings dialog box is displayed in the right (Rule) pane.

Step 7 Select a global controller.

Step 8 Click (**Edit**).

The Global Controller Settings dialog box appears (Figure 9-22).

Figure 9-22 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 r**adio button on the Per Link Global Controller tab.

b. Enter the desired value in Kbps for the maximum bandwidth in the Rate limit for the Link 1 (in Kbps) field.

c. Repeat Step 9b for each link.

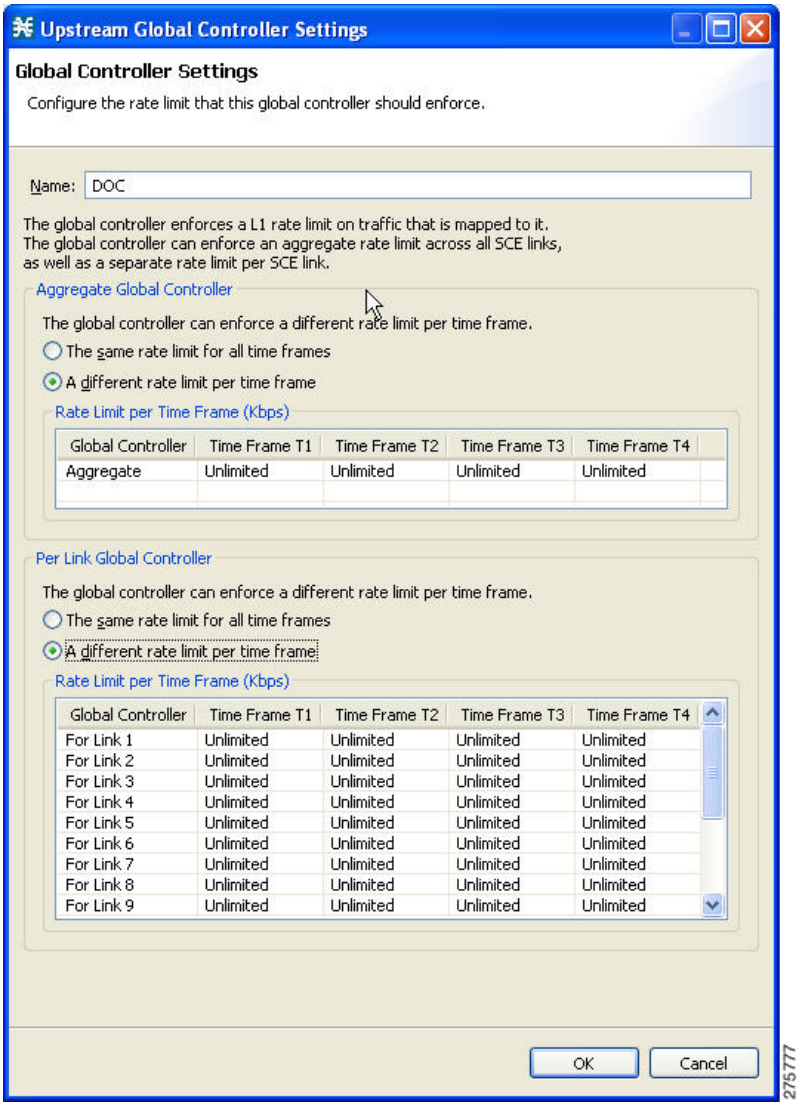
Step 10 Set the maximum limit that this global controller carries to vary according to time frame.

a. Choose the **A different rate limit per time frame** radio button the Per Link Global Controller tab.

b. Enter the desired value for each time frame.

c. Repeat Step 10b for each link (Figure 9-23).

Figure 9-23 Downstream Global Controller Settings



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**.

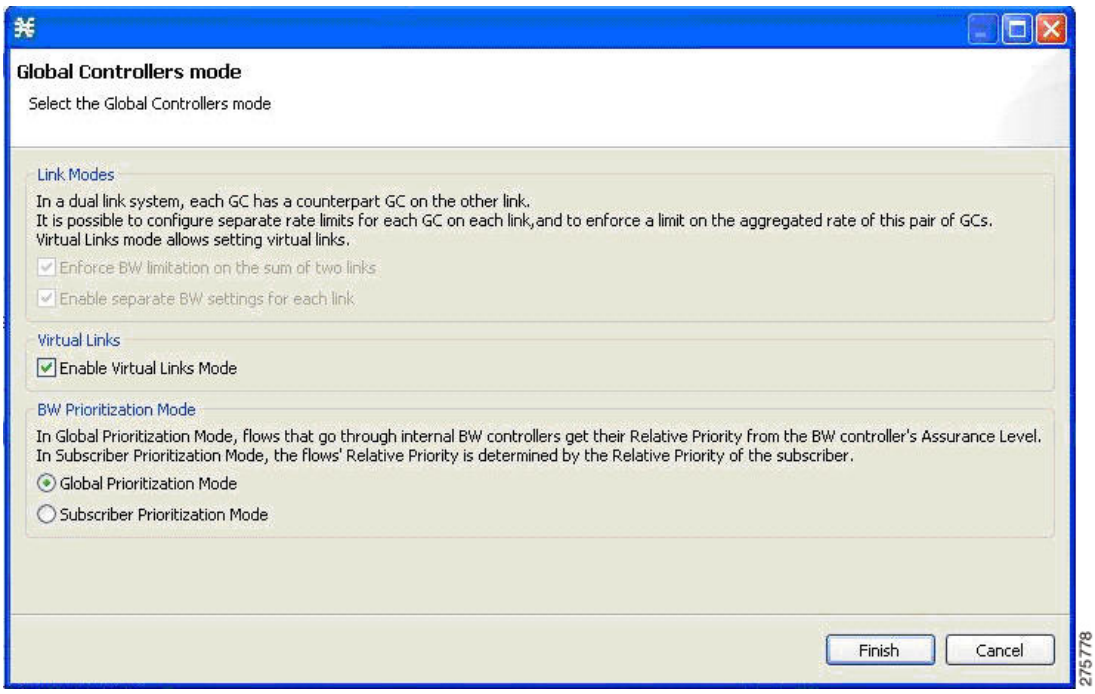
The Global Bandwidth Settings dialog box in the right (Rule) pane.

Step 2 Add global controllers, as described in How to Add Global Controllers, page 9-6.

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.

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

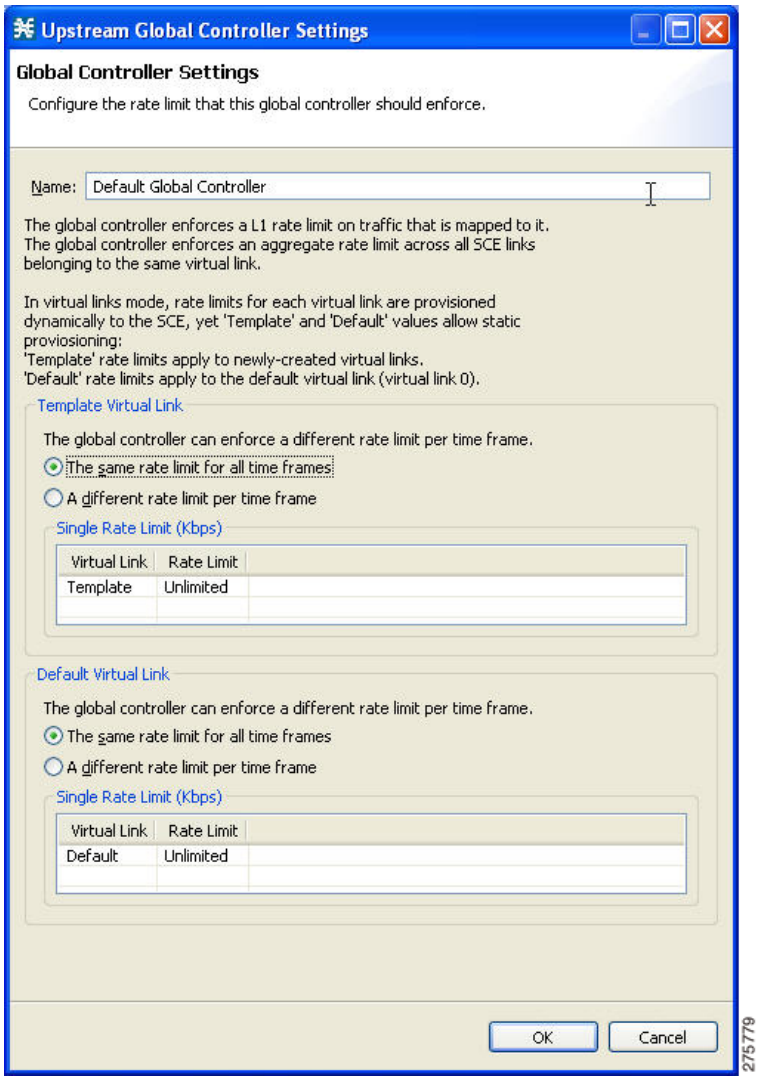
The Global Bandwidth Settings dialog box is displayed in the right (Rule) pane.

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



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 r**adio 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 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 r**adio button on the Default Virtual Link tab.

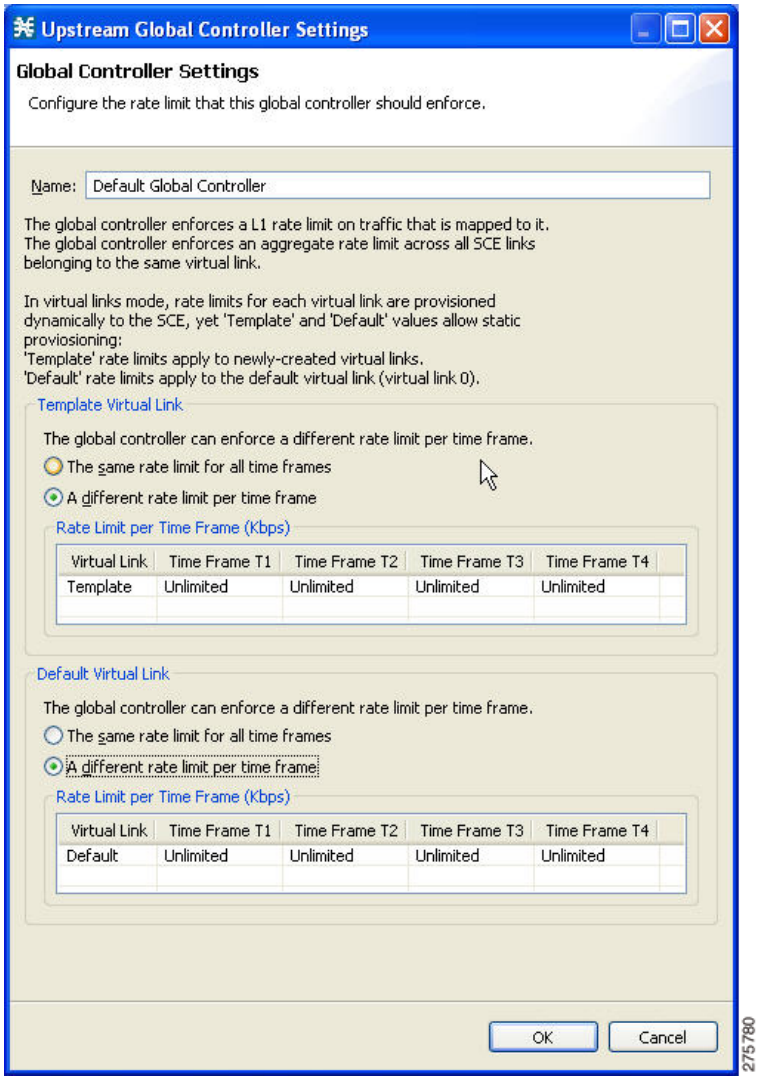
b. Enter the desired value in Kbps for the maximum bandwidth in the Rate limit for the Link 1 (in Kbps) field.

Step 12 Set the maximum limit that this global controller carries to vary according to time frame.

a. Choose the **A different rate limit per time frame** radio button the Default Virtual Link tab.

b. Enter the desired value for each time frame (Figure 9-26).

Figure 9-26 Upstream Global Controller Settings



Step 13 Click **OK**

Your changes are saved.

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, depending upon 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 each subscriber's service, based upon the CIR, PIR, global controller and Assurance Level (AL) set for the BWC. Each rule defines a link between the service's flows and one of the BWCs (unless the flows are to be blocked). See How to Define Per-Flow Actions for a Rule, page 9-59.
- 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.

The Cisco SCE supports a maximum of 2000 BWCs. You cannot apply a PQB file to an 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.

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.)

- Subscriber BWC Parameters, page 9-29
- How to Edit Package Subscriber BWCs, page 9-29

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.
- AL—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.

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

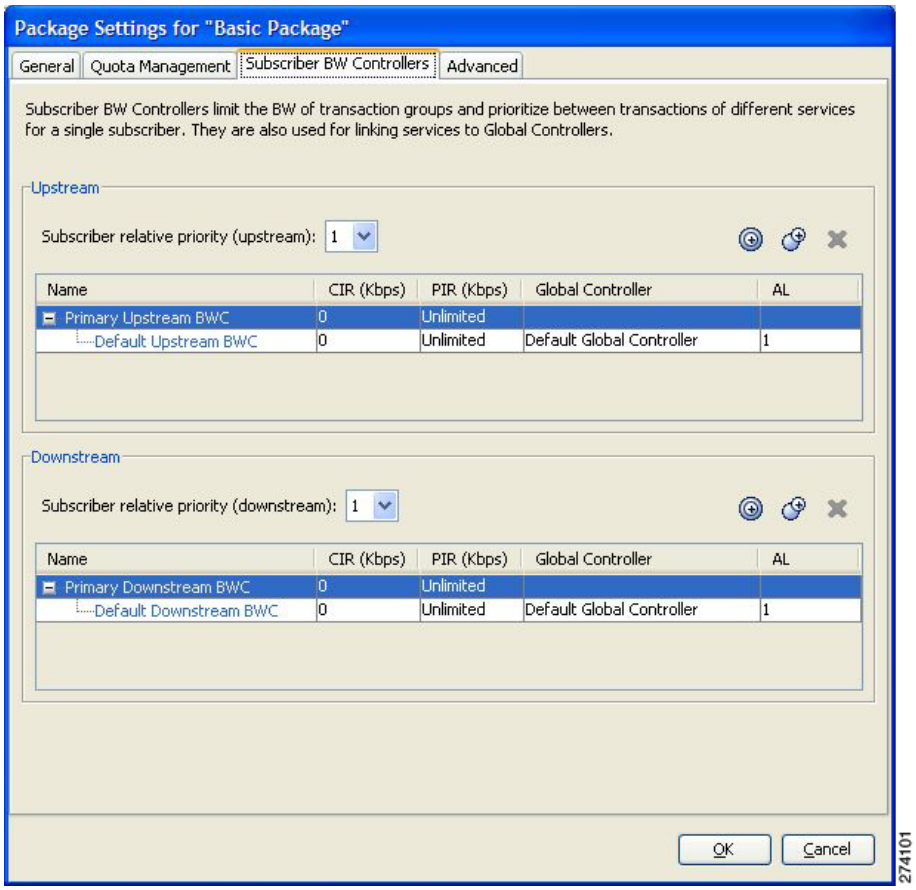
Step 2 In the right (Rule) pane, select a BWC and click (**Edit**).

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.

a. Select a value from the Subscriber relative priority drop-down list.

b. 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.

c. To add BWCs to the package, click (**Add a sub BW Controller)** once for each additional BWC.

d. To add Extra BWCs to the package, click (**Add an extra BW Controller)** once for each additional BWC.

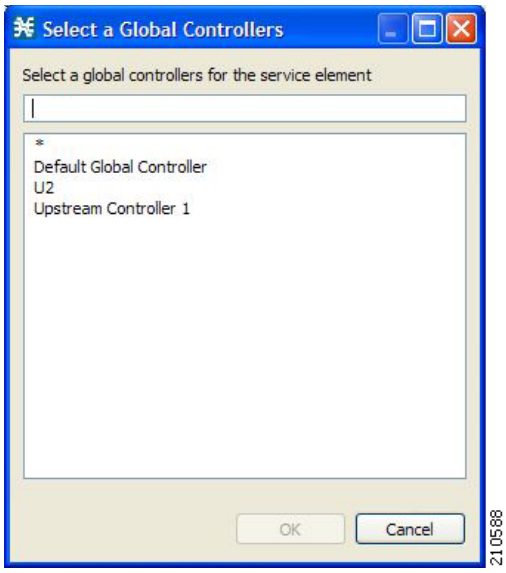
e. Set the parameters for each BWC (including the Primary and Default BWCs).

- (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.

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 9-32
- Example: How to Limit P2P and Streaming Traffic Using the Console, page 9-32

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.

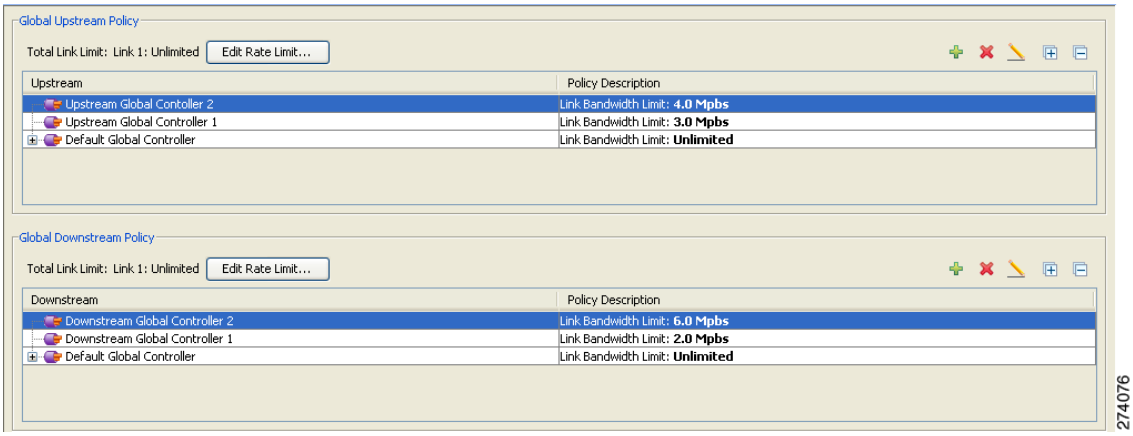
Note The P2P Traffic Optimization wizards allow you to create a simple model of devices, connect to them, and limit P2P traffic to a specified bandwidth. (See How to Use the P2P Traffic Optimization Wizards, page 4-47.)

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).

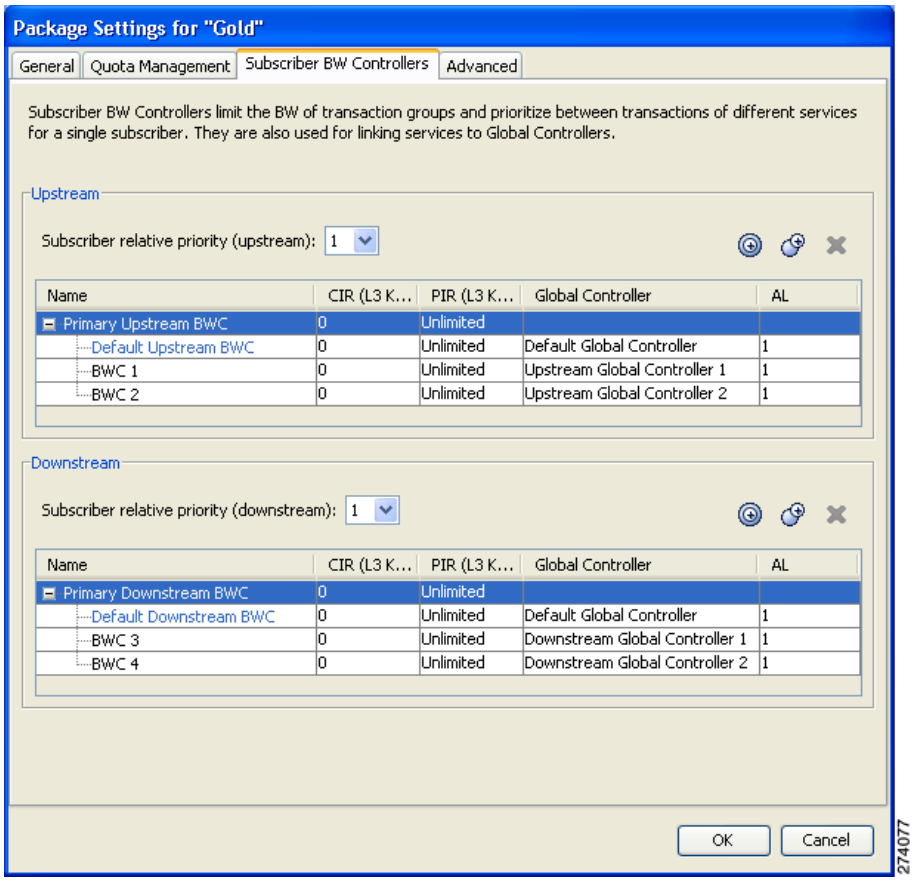
Figure 9-29 Global Bandwidth Settings



(Here, Upstream Controller 1 and Downstream Controller 1 will be used for P2P traffic, and Upstream Controller 2 and Downstream Controller 2 will be 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).

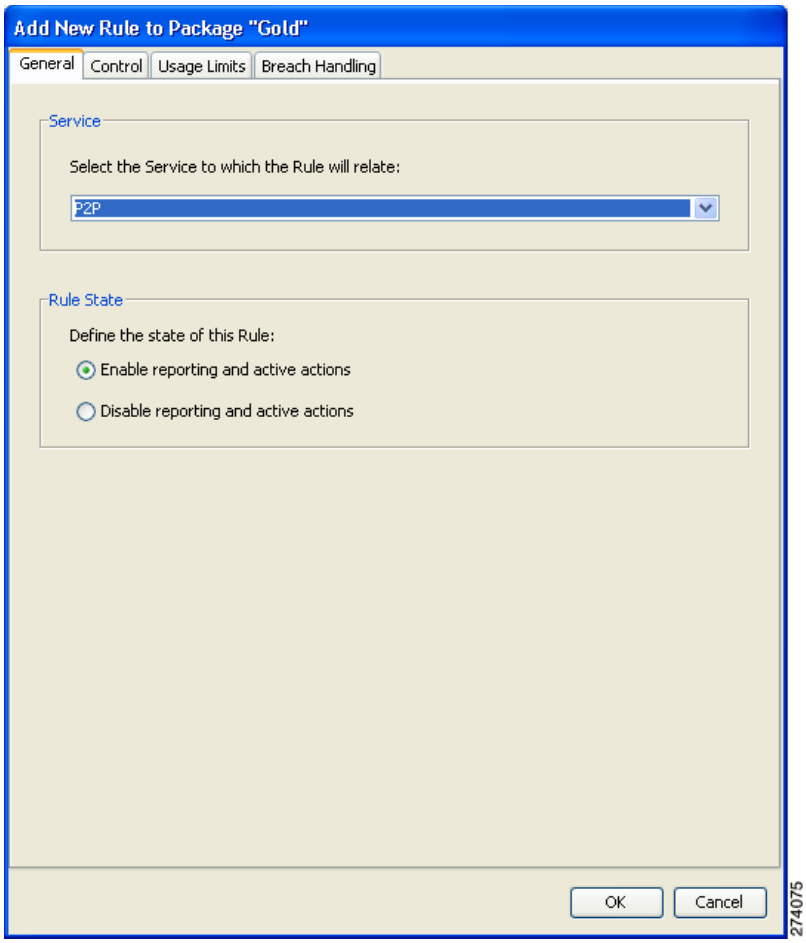
Figure 9-30 Package Settings



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

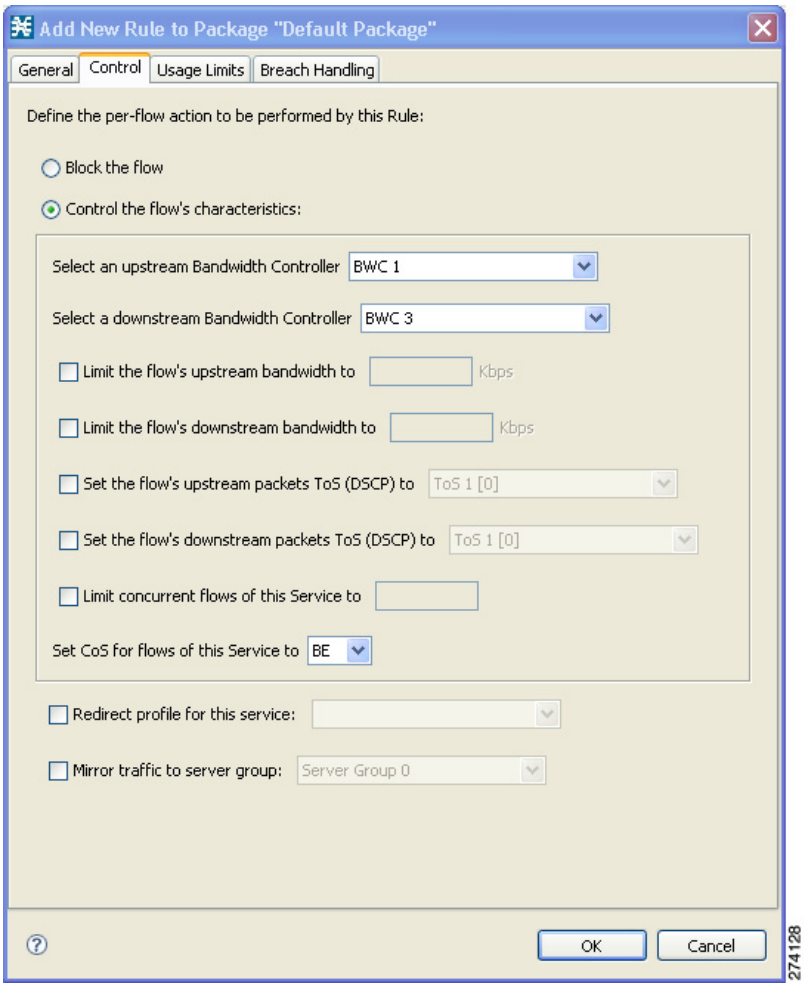
Step 4 Add a rule for the P2P service (Figure 9-31).

Figure 9-31 Add New Rule to Package



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

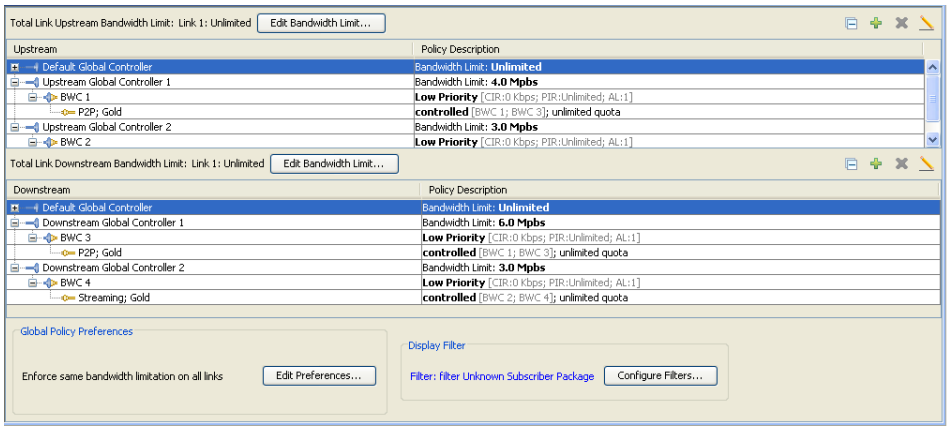


Step 6 Repeat Step 4 and Step 5 for the Streaming service, using BWC 2 as the upstream BWC and BWC 4 as the downstream BWC.

All subscriber traffic using these services will be added to the virtual queue total for these queues. In turn, the bandwidth available to the subscriber for these protocols will 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



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 (**Add**).

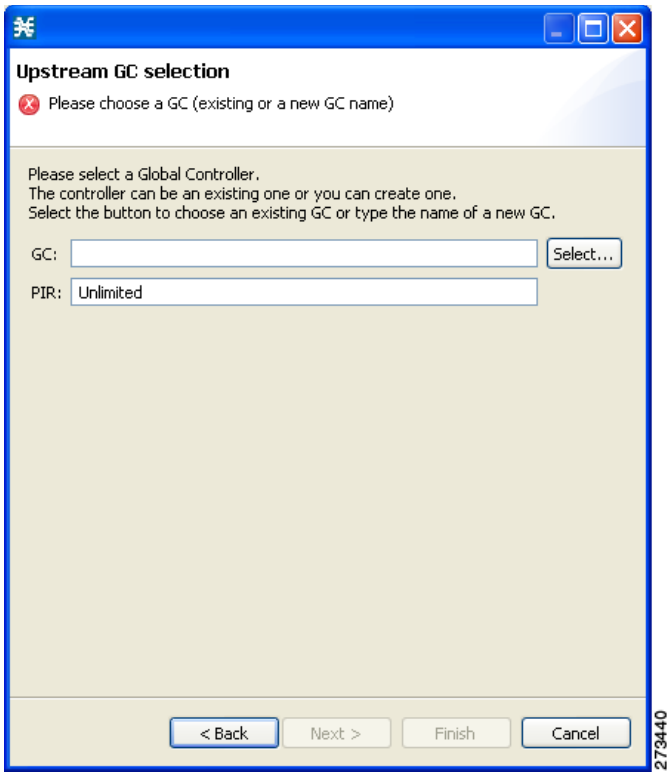
The Select addition mode dialog box appears.

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



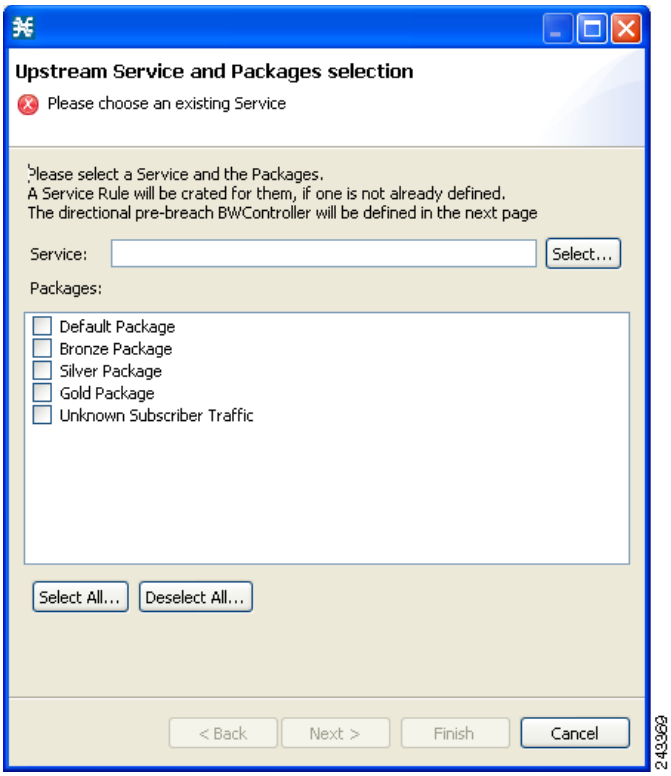
Step 5 In the GC field, enter a new GC name, or click **Select** to choose an existing GC.

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.

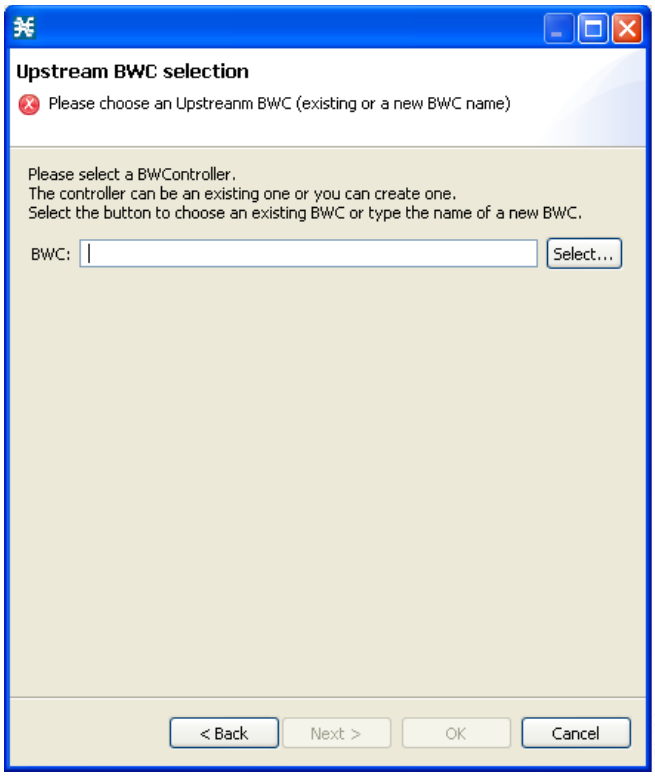
Step 9 In the Packages section, select one or more packages for the rule to apply to.

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 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 the flow that goes through an iBWC is determined by the relative priority of one of:

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

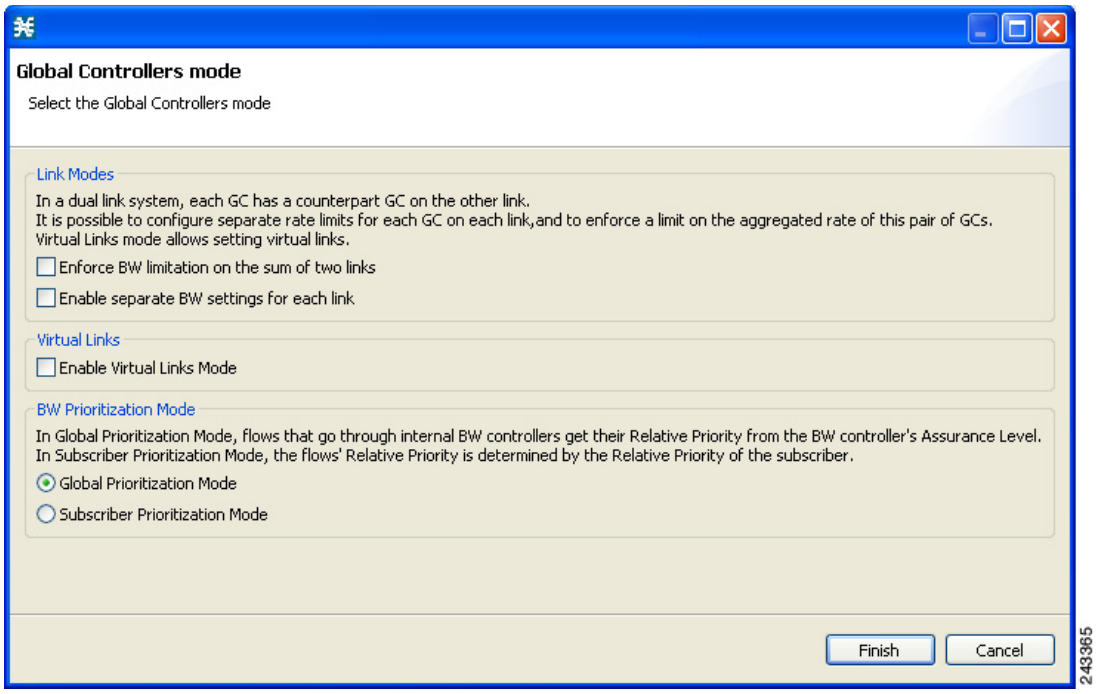
Step 1 In the Policies tab, click **Global Policy**.

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 and depend on the subscriber's package (which defines the template controllers) and the physical link assigned to the subscriber.

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).

Depending on the Cisco SCE harware, a service configuration can contain up to 1024 or 2048 upstream global controllers and 1024 or 2048 downstream global controllers (including the default global controllers). The maximum number of virtual links is limited by the number of directional template global controllers: the number of template global controllers times the number of virtual links cannot exceed 1024 or 2048.

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 will result in en 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 global controllers' PIR values.
7. A subscriber is introduced to the 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 subscriber's package and the virtual links' global controller configuration.

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 the *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.

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 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.

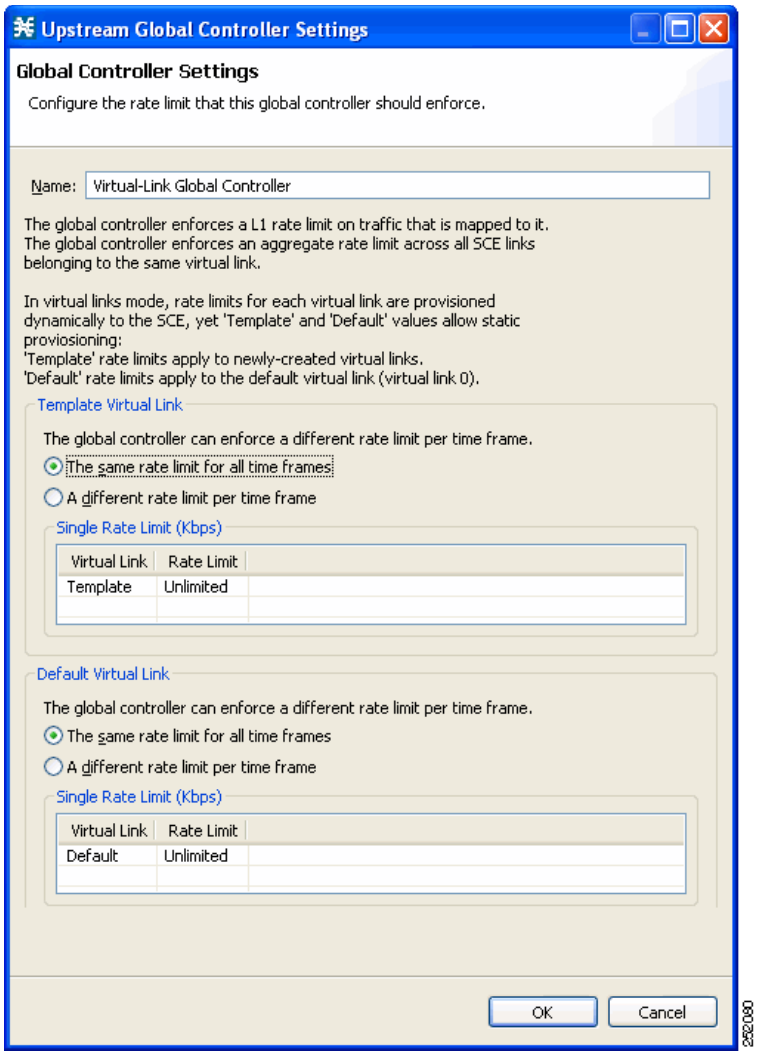
The maximum amount of bandwidth that can be used by any global controller is displayed at the top of the Global Bandwidth Settings:

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

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

The Global Controller Settings dialog box appears (Figure 9-38).

Figure 9-38 Upstream Global Controller Settings



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, refer to the following sections:

- How to Add Global Controllers, page 9-6
- How to Set the Maximum Bandwidth of Global Controllers, page 9-9
- How to Delete Global Controllers, page 9-11
- Managing Subscriber Bandwidth, page 9-28

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 SCE platform capacity that the platform will carry, 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 SCE platform Command-Line Interface (CLI). For more information about the 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, page 9-45.

- 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 commands is a line interface configuration command. To run this command see How to Enter Line Interface Configuration Mode, page 9-45.

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

  ```
  show interface LineCard 0 virtual-links [all | changed]
  ```

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 subscriber's virtual links index
show interface LineCard 0 virtual-links all	Show information about all virtual links
show interface LineCard 0 virtual-links changed	Show information about virtual links whose PIR differs from the value defined in the template global controller

How to Enter Line Interface Configuration Mode

Step 1 At the 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 system's reaction 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, page 7-3) and only then add and define packages.

Every 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 if no other package is specifically assigned to the subscriber, or if a nonexistent package is assigned to the subscriber.

A service configuration can contain up to 5000 packages.

Package Parameters

A package is defined by the following parameters:

- General parameters:
  - Package Name—A unique name for the package
  - Description—(Optional) A description of the package
- Quota Management parameters:
  - Quota Management Mode—Specifies whether subscriber quotas are managed by an external quota manager or replenished periodically by 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 packages. (Changing the package name does not affect SCE platform activity.) A default value of the package index is provided by the system. 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—A default value of the counter index is provided by the system. 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.

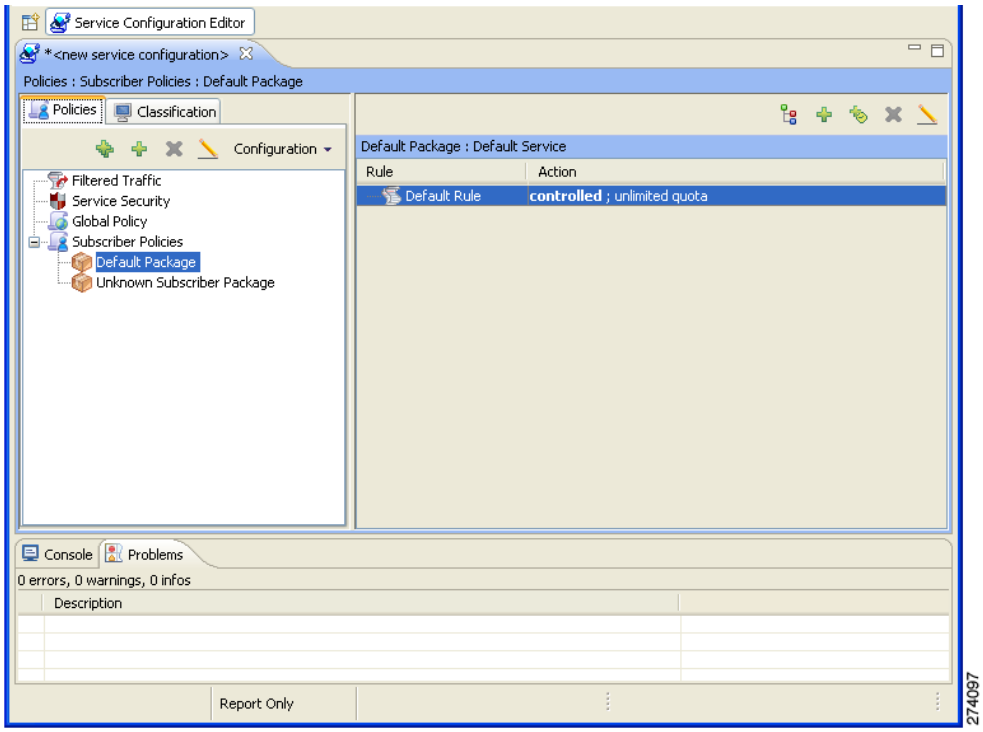
These parameters are defined when you add a new package (see How to Add Packages, page 9-49). You can modify them at any time (see How to Edit Packages, page 9-53).

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 9-39).

Figure 9-39 Policies Tab



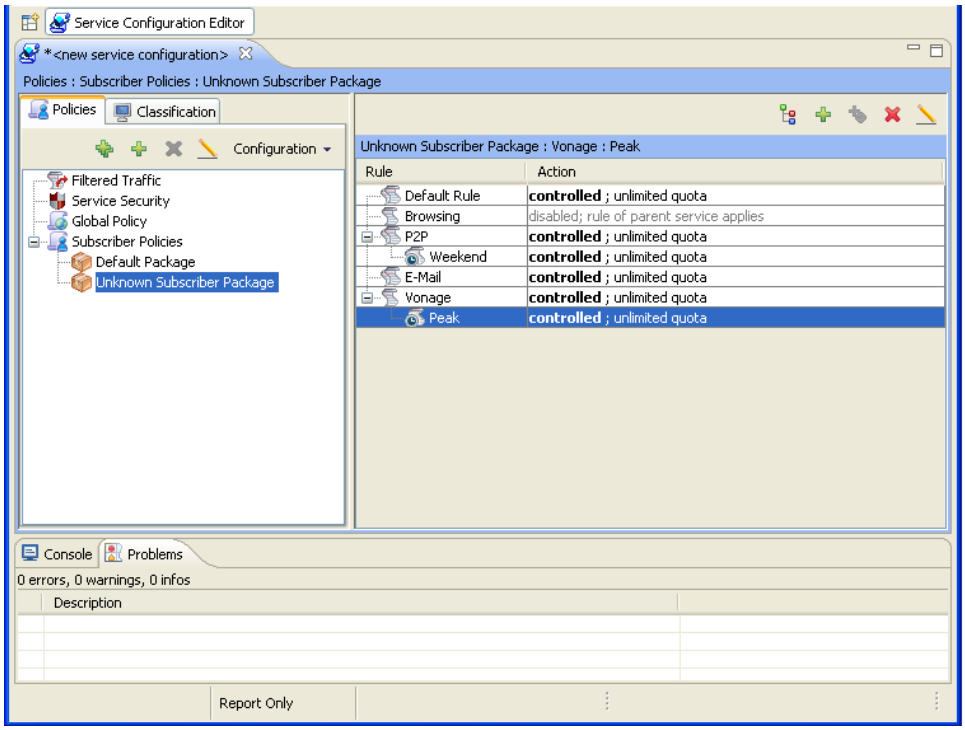
A list of all packages is displayed in the package tree.

Note To view more information about a package, open the Package Settings dialog box (see How to Edit Packages, page 9-53).

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 9-40).

Figure 9-40 Service Configuration Editor



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.

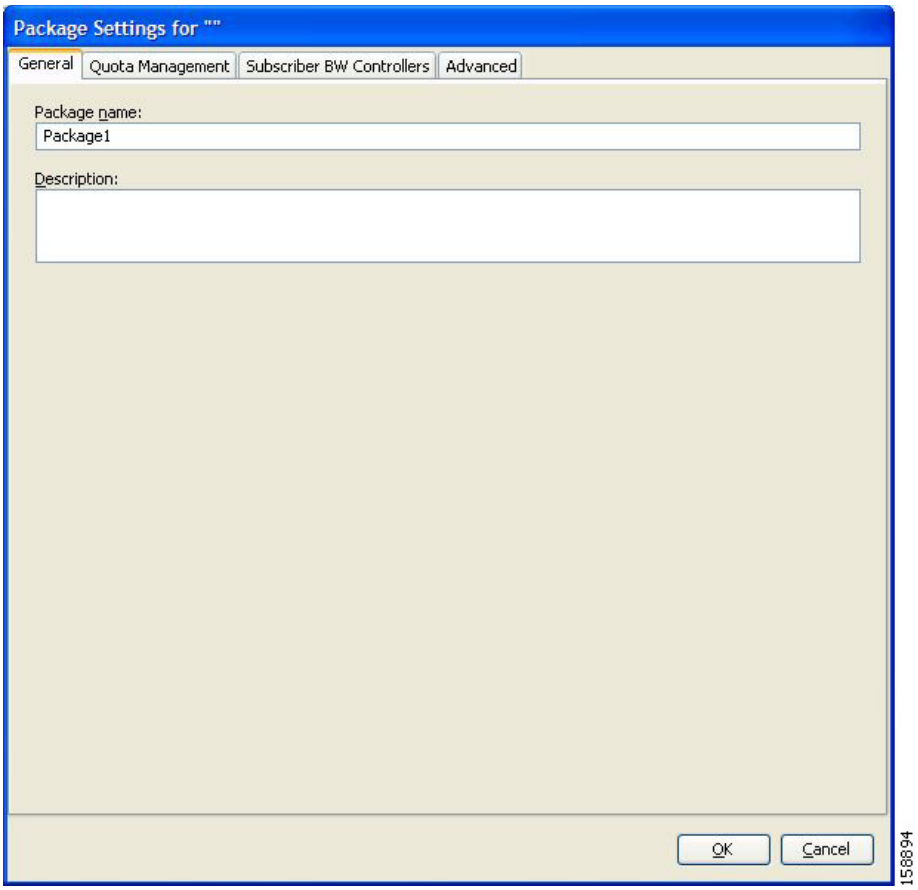
After you have added a new package, you can define rules for the package (see How to Add Rules to a Package, page 9-57).

Step 1 In the Policies tab, select a package from the package tree. This package will be the parent of the package you are adding.

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

The Package Settings dialog box appears (Figure 9-41).

Figure 9-41 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, page 9-55.

What to Do Next

To configure parameters in the Quota Management tab see How to Edit Quota Management Settings for Packages, page 9-75.

To configure parameters in the Subscriber BW Controllers tab, see How to Edit Package Subscriber BWCs, page 9-29.

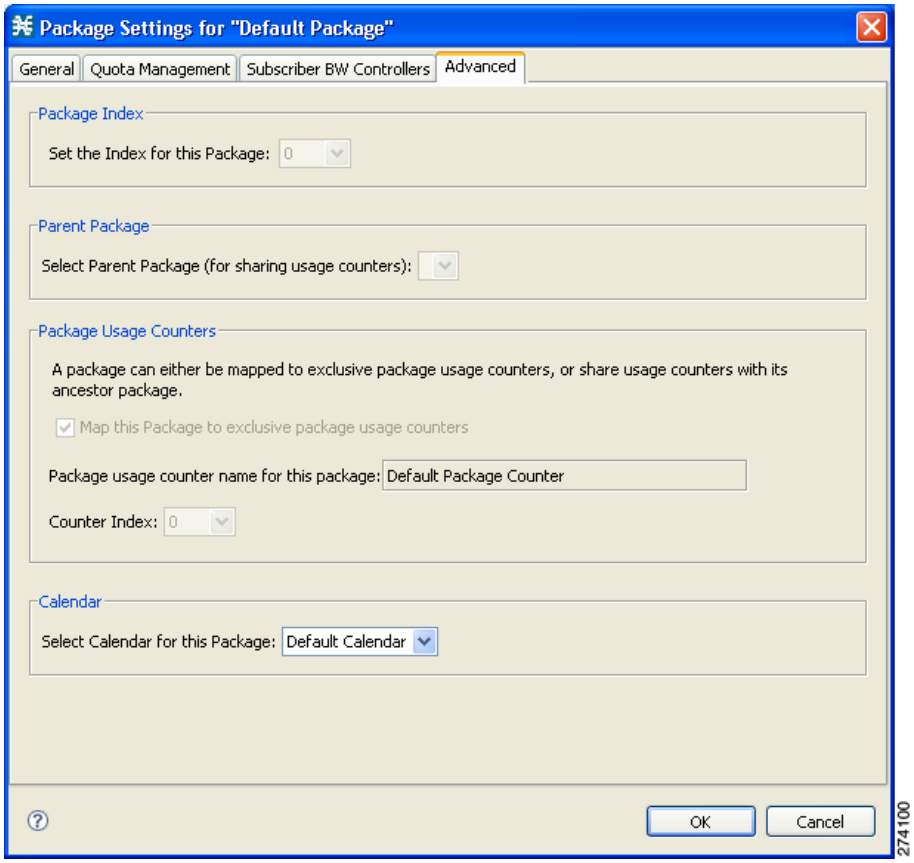
How to Set Advanced Package Options

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 9-42).

Figure 9-42 Advanced Tab



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 A default value of the index is provided by the system. 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 A default value of the index is provided by the system. 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, page 10-54.

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, page 9-55.

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 make changes than to define the package from scratch.

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  (**Duplicate Package**).

A duplicate package is created with all the same attributes as the original package. The name of the new package is the name of the selected package followed by "(1)" (or "(2)", and so on if a package is duplicated many times).

Step 3 Modify the package parameters (see How to Edit Packages, page 9-53).

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  (**Edit Package**).

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, page 9-75.

Step 6 (Optional) Change bandwidth control settings, see How to Edit Package Subscriber BWCs, page 9-29.

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 A default value of the counter index is provided by the system. 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 A default value of the counter index is provided by the system. 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, page 10-54.

Step 8 Click **OK.**

The Package Settings dialog box closes.

All changes to the package parameters are saved.

How to Delete Packages

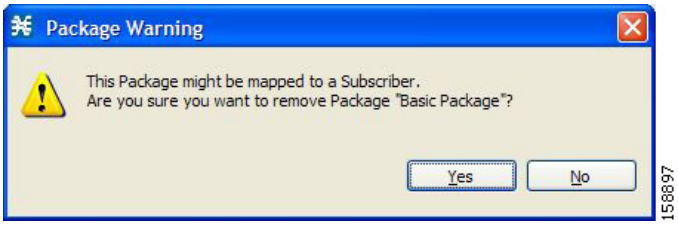
You can delete user-defined packages. The default package cannot be deleted.

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

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

A Package Warning message appears (Figure 9-43).

Figure 9-43 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 a flow's packets
- 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.

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 SCE platform will apply the most specific rule to any flow.

For example, if you define rules for E-Mail and POP3, any flow mapped to the POP3 service will be handled according to the POP3 rule—any flow mapped to the SMTP or IMAP service will be handled according to the E-Mail 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.

Any rule that also applies to child services is indicated by . Rules that do not apply to any child services are shown by .

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, page 9-63.

How to View the Rules of a Package

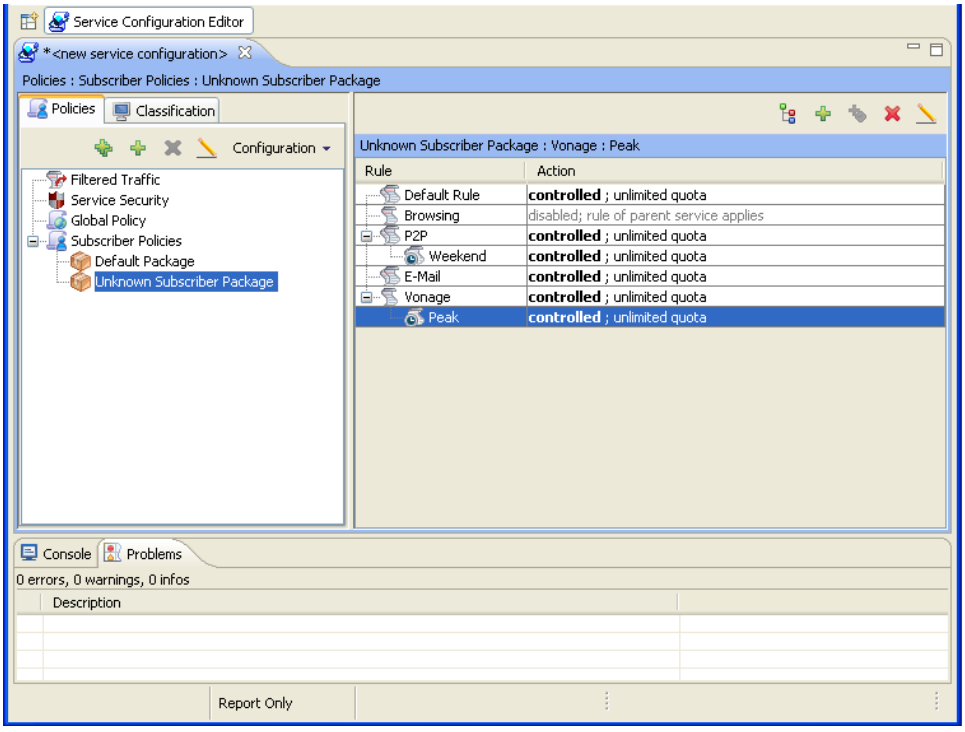
You can view a list of the rules of a package.

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 9-44).

Figure 9-44 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, page 9-61).

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, page 9-66).

How to Add Rules to a Package

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

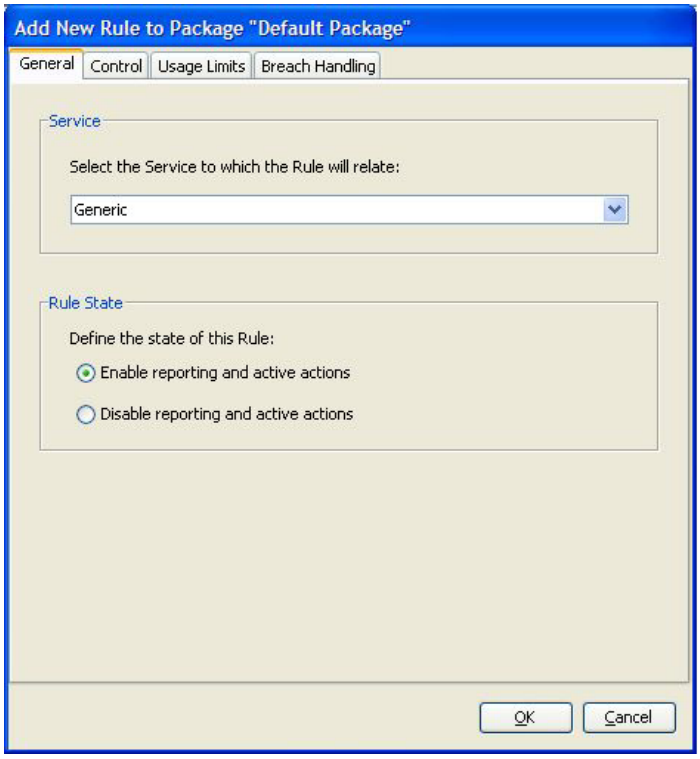
Adding time-based rules is described in the section How to Add Time-Based Rules to a Rule, page 9-64.

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

Step 2 In the right (Rule) pane, click  (**Add Rule**).

The Add New Rule to Package dialog box appears (Figure 9-45).

Figure 9-45 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 will Relate 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, page 9-61).

Step 5 (Optional) Set behavior per traffic flow for this rule, continue with the instructions in the section How to Define Per-Flow Actions for a Rule, page 9-59.

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, page 9-75):

- To configure parameters in the Usage Limits tab see How to Select Quota Buckets for Rules, page 9-77.
- To configure parameters in the Breach Handling tab, see How to Edit Breach-Handling Parameters for a Rule, page 9-78.

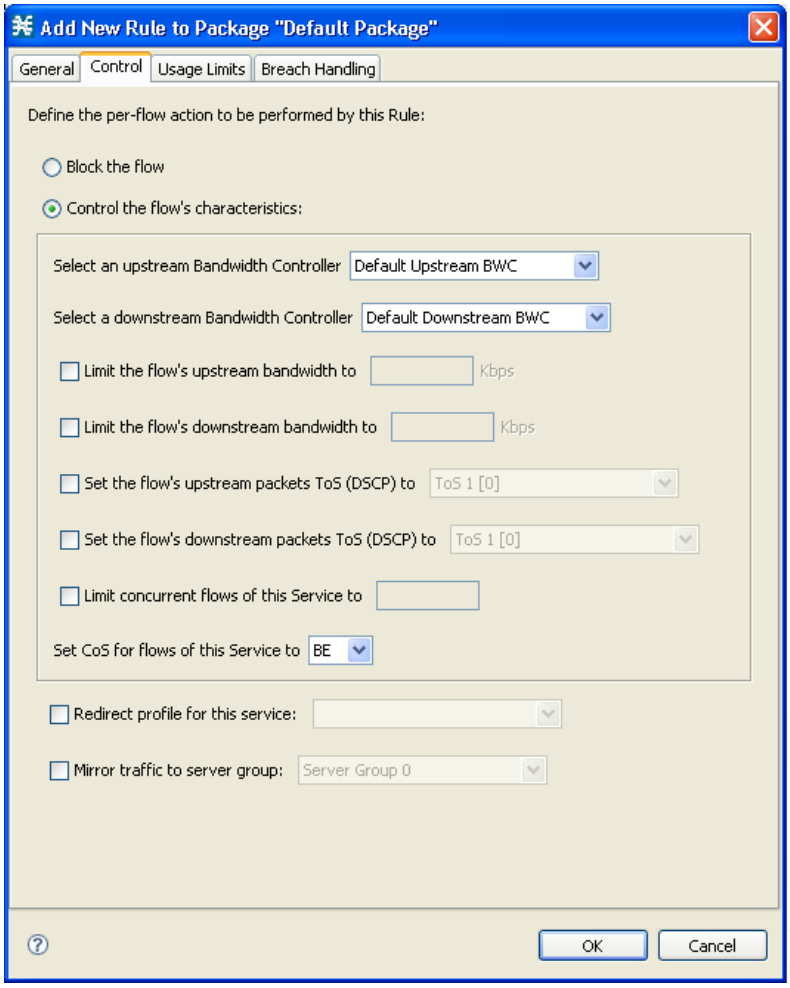
How to Define Per-Flow Actions for a Rule

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 9-46).

Figure 9-46 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.

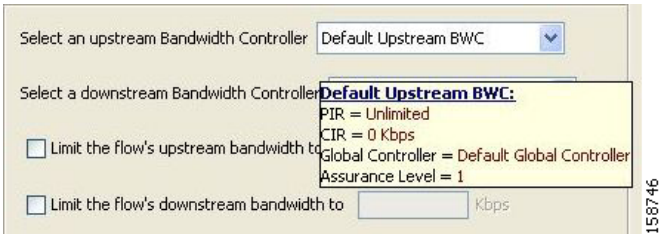
Step 4 From the upstream Bandwidth Controller drop-down list, select an upstream BWC. This sets up bandwidth metering of all concurrent flows mapped to this rule, based on the characteristics of the selected BWC.

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

Note **Important Note 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 9-47) containing the properties of the selected BWC (Peak Information Rate (PIR), Committed Information Rate (CIR), Global Controller, and Assurance Level).

Figure 9-47 Drop-Down List Tips



Step 5 From the downstream Bandwidth Controller drop-down list, choose a downstream BWC.

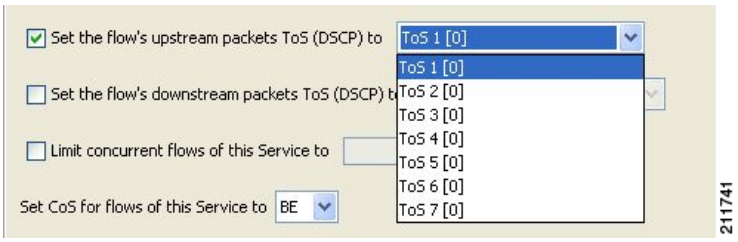
Step 6 (Optional) To set a per-flow upstream bandwidth limit, check the Limit the flow's upstream bandwidth check box and enter a value in the Kbps field.

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 9-48).

Figure 9-48 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.

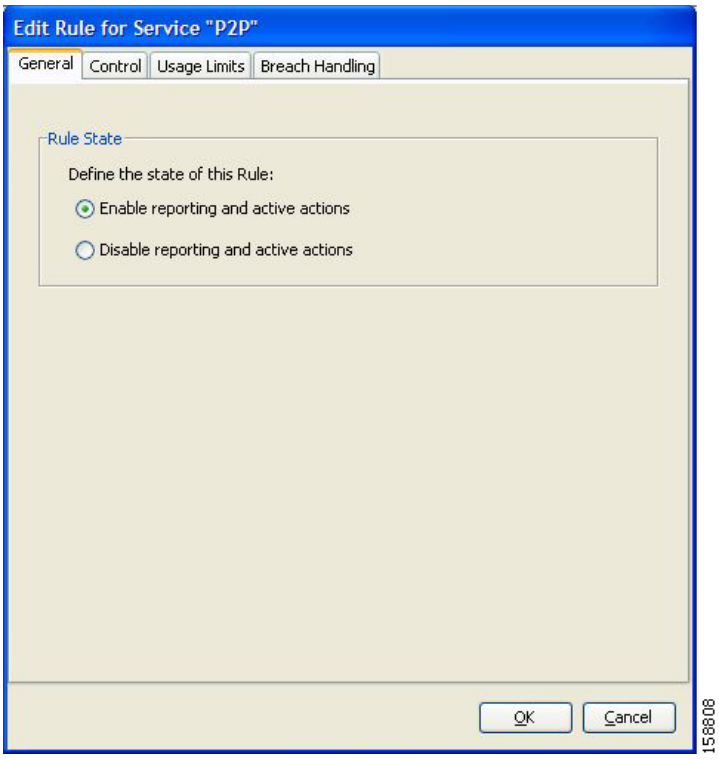
Step 1 In the Policies tab, select a package from the package tree.

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

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

The Edit Rule for Service dialog box appears (Figure 9-49).

Figure 9-49 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 9-59.

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 9-77.

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 9-78.

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 (see Step 4 of How to Edit Rules, page 9-61). This 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 (**Delete Rule**).

A Rule Warning message appears (Figure 9-50).

Figure 9-50 Rule Warning

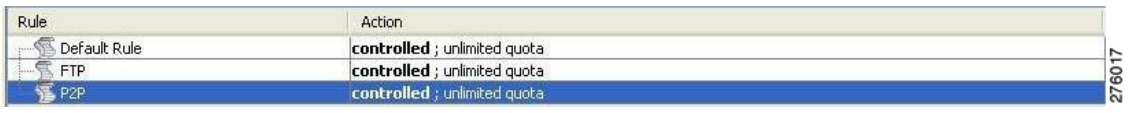
Step 4 Click **Yes.**

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 child service is governed by the rule of the parent service. A rule that affects any of a service's children is indicated in the rules list by a different icon, as illustrated for the P2P rule and the FTP rule in Figure 9-51.

Figure 9-51 Rules



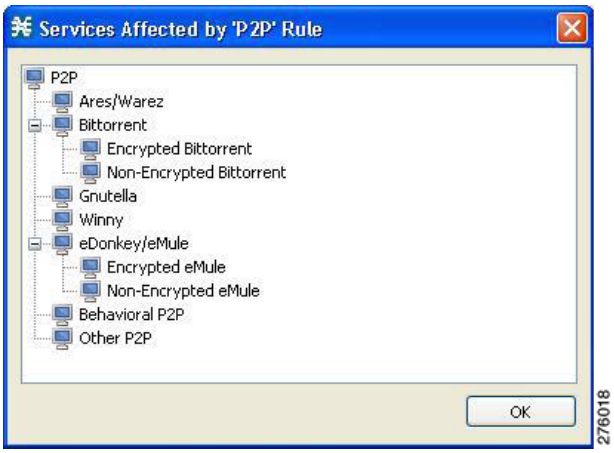
You can display all (child) services that are affected by a rule.

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 (**Show All Services Affected By This Rule**).

The Services Affected dialog box appears (Figure 9-52).

Figure 9-52 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, page 9-68). 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 will 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.

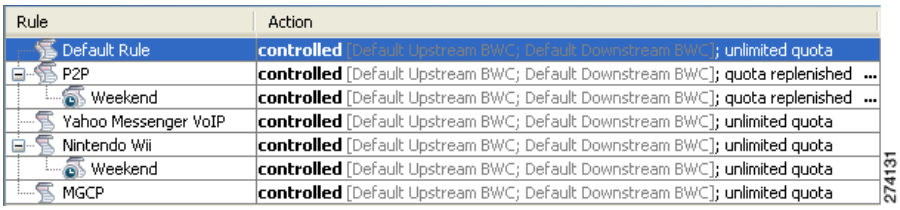
How to Add Time-Based Rules to a Rule

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 9-53.

Figure 9-53 P2P Weekend Based Time Rule



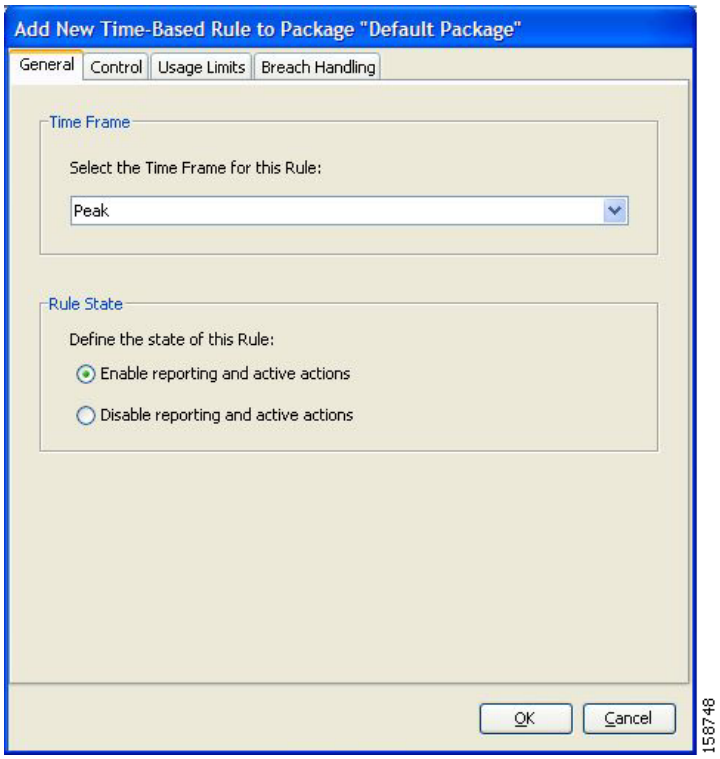
Step 1 In the Policies tab, select a package from the package tree.

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

Step 3 Click (**Add Time-Based Rule**).

The Add New Time-Based Rule dialog box appears (Figure 9-54).

Figure 9-54 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 9-59.

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 9-77.

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 9-78.

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.

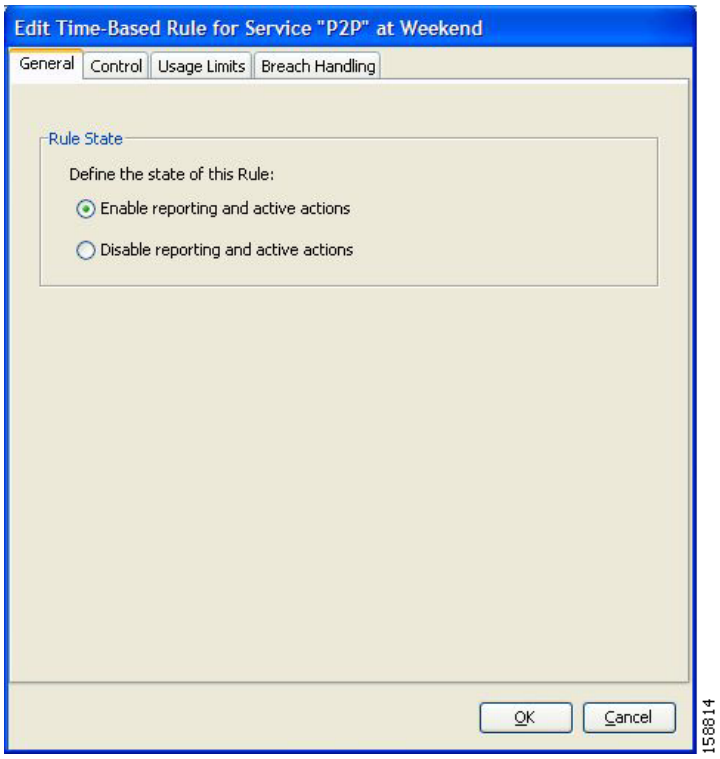
Step 1 In the Policies tab, select a package from the package tree.

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

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

The Edit Time-Based Rule for Service dialog box appears (Figure 9-55).

Figure 9-55 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.

a. Click the **Control** tab.

The Control tab opens.

b. Follow the instructions in How to Define Per-Flow Actions for a Rule, page 9-59.

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 9-77.

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 9-78.

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, page 9-66). This allows you to enable the rule again later, without having to reset all its parameters.

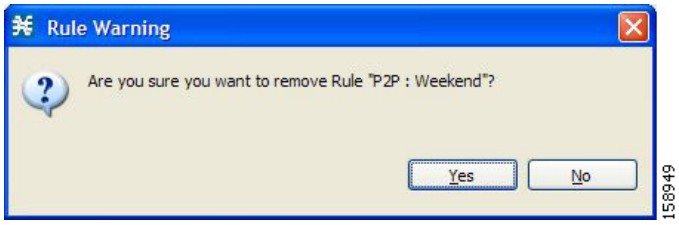
Step 1 In the Policies tab, select a package from the package tree.

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

Step 3 In the Rule pane, click (**Delete Rule**).

A Rule Warning message appears (Figure 9-56).

Figure 9-56 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 will 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 9-69
- How to Add Calendars, page 9-69
- How to Rename the Time Frames, page 9-70
- How to Delete Calendars, page 9-71
- How to Configure the Time Frames, page 9-72

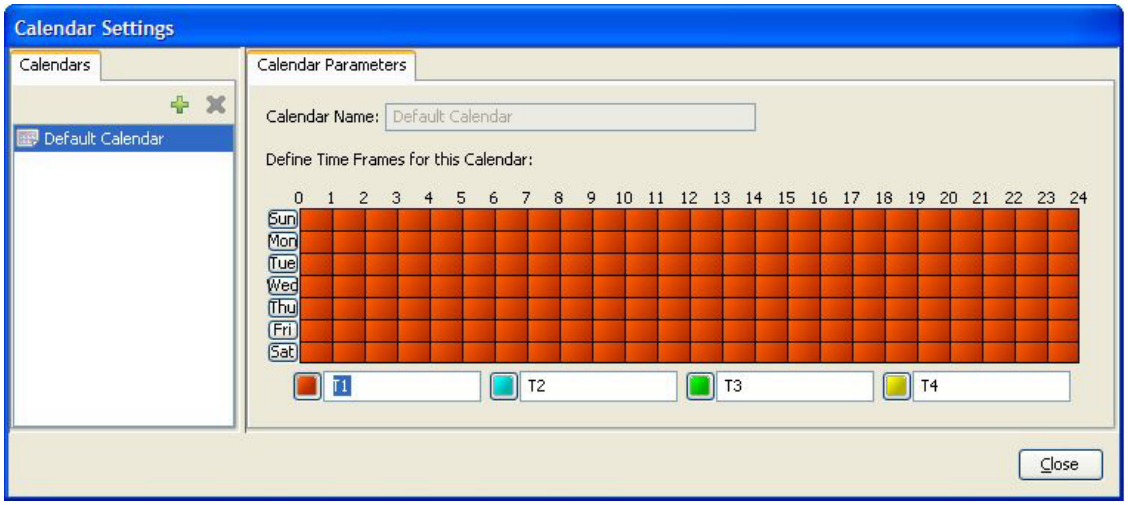
How to View Calendars

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

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

The Calendar Settings dialog box appears (Figure 9-57).

Figure 9-57 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 > Weekly Calendars.**

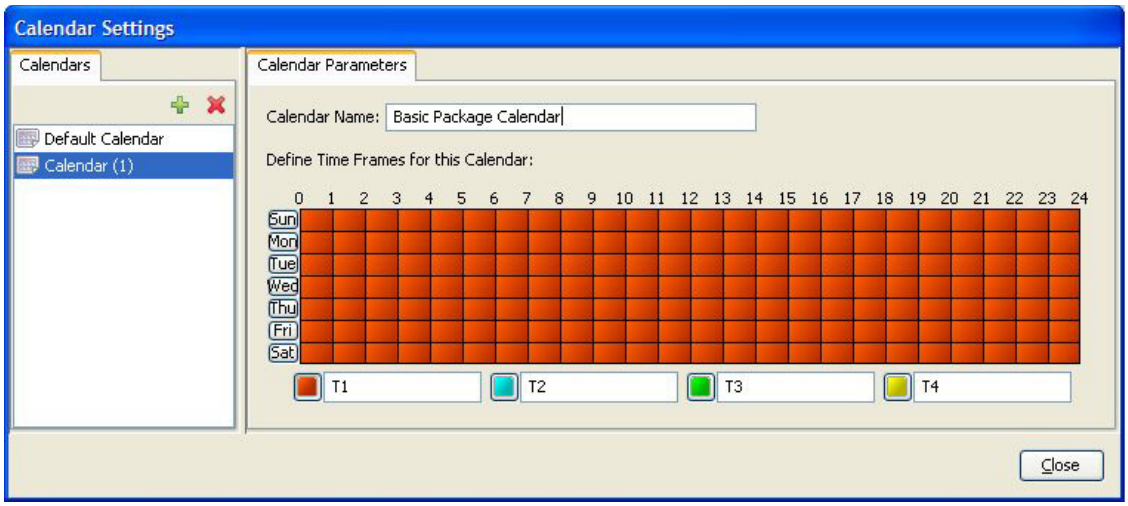
The Calendar Settings dialog box appears.

Step 2 In the Calendar tab, click (**Add**).

A new calendar is added with the name Calendar (1).

Step 3 In the Calendar Parameters tab (Figure 9-58), click in the Calendar Name field and enter the name for this calendar.

Figure 9-58 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.

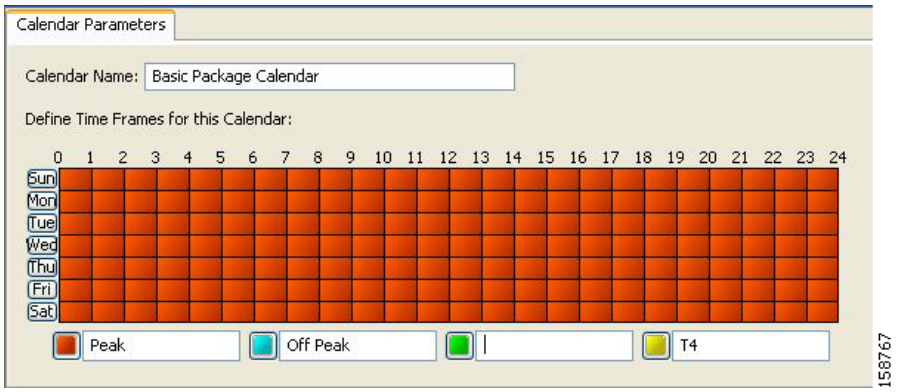
Step 1 From the Policies tab of the left pane, choose **Configuration > Weekly Calendars.**

The Calendar Settings dialog box appears.

In the Calendar Parameters tab (Figure 9-59), 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 9-59 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 will be deleted.
See How to Set Advanced Package Options, page 9-51 for information about changing the calendar associated with a package.

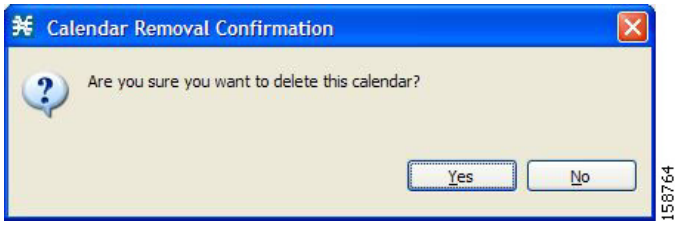
Step 1 From the Policies tab of the left pane, choose **Configuration > Weekly Calendars.**

The Calendar Settings dialog box appears.

Step 2 In the Calendar tab, select a calendar and click (**Delete**).

A Calendar Removal Confirmation message appears (Figure 9-60).

Figure 9-60 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 > 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.

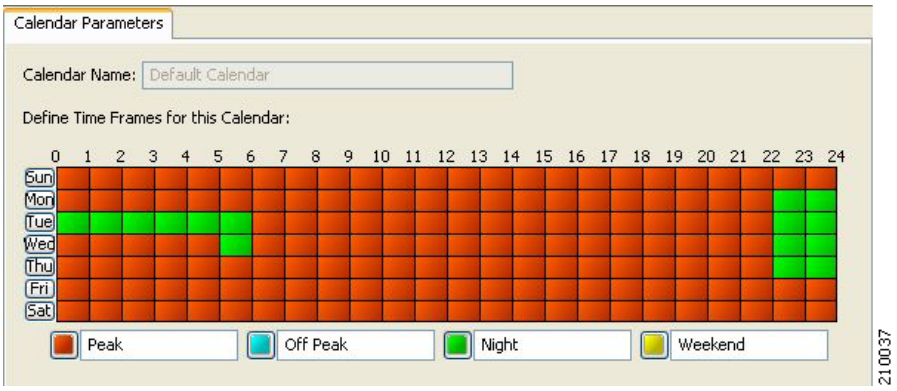
Below the grid, the name of each time frame appears next to a colored button.

Step 3 Click one of the colored buttons.

Step 4 Select all the cells in the grid that represent hours that will be 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 9-61).

Figure 9-61 Calendar Parameters Tab

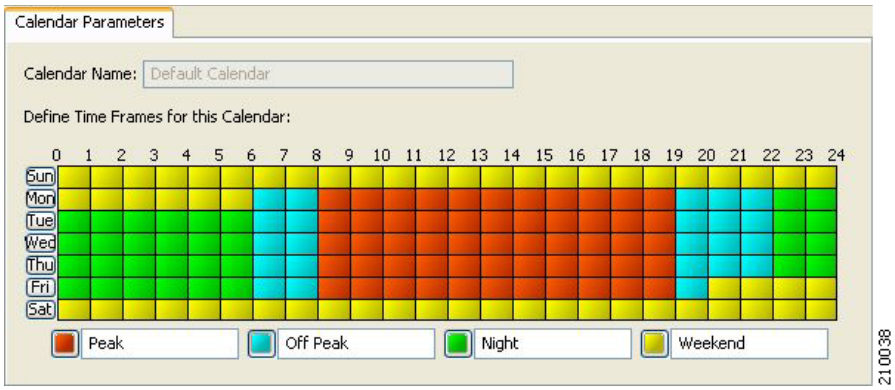


The changes are written to the service configuration as you make them.

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 9-62 illustrates a possible time partition plan.

Figure 9-62 Time Partition Plan Example



Step 6 Click **Close.**

The Calendar Settings dialog box closes.

How to Manage DSCP ToS Marker Values

SCA BB can change the value of the DSCP ToS marker of packets of flows that match a filter rule (see Step 11 of How to Add Filter Rules, page 10-22) or a service rule (see Steps 10 and 11 of How to Define Per-Flow Actions for a Rule, page 9-59 and Step 9 of How to Edit Breach-Handling Parameters for a Rule, page 9-78).

SCA BB supports seven ToS Marker Classes. You assign each class a specific value to apply to a flow's packets.

Note If you have used DSCP marking on a SCA BB release prior to 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.

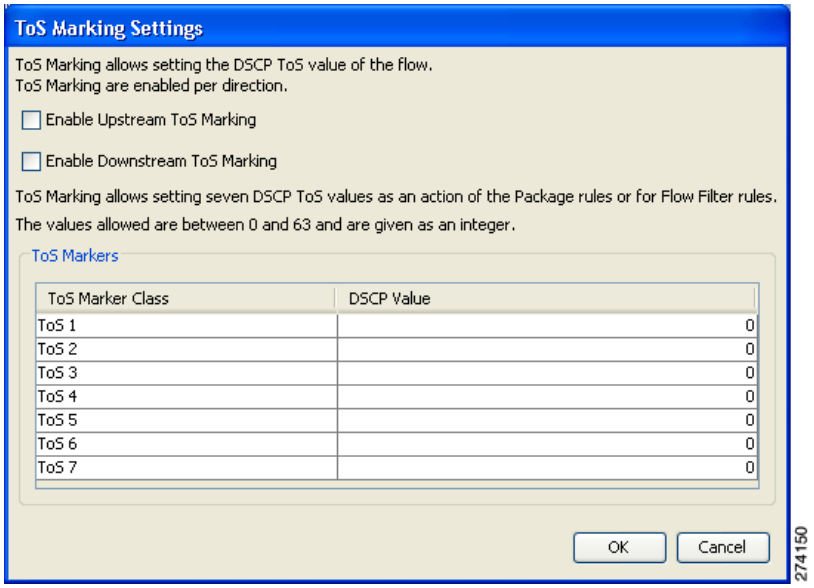
The default marking option is not to mark the packet. Since classification may take a few packets to finalize, it is important to note that if ToS marking is enabled, the first few packets may still be processed under the default option and therefore may not be marked.

Caution In an MPLS environment, the 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 > ToS Marking Settings.**

The ToS Marking Settings dialog box appears (Figure 9-63).

Figure 9-63 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 Edit Quota Management Settings for Packages

You can define whether quota management for a package is performed by an external quota manager or by SCA BB.

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, page 9-77).

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, page 10-47). By default, this property has a value of zero, that is, all quota is replenished at the same time.

Each subscriber's quota replenishment occurs 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.) In the case of hourly quota replenish period, the scatter should therefore be set to 60 minutes.

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

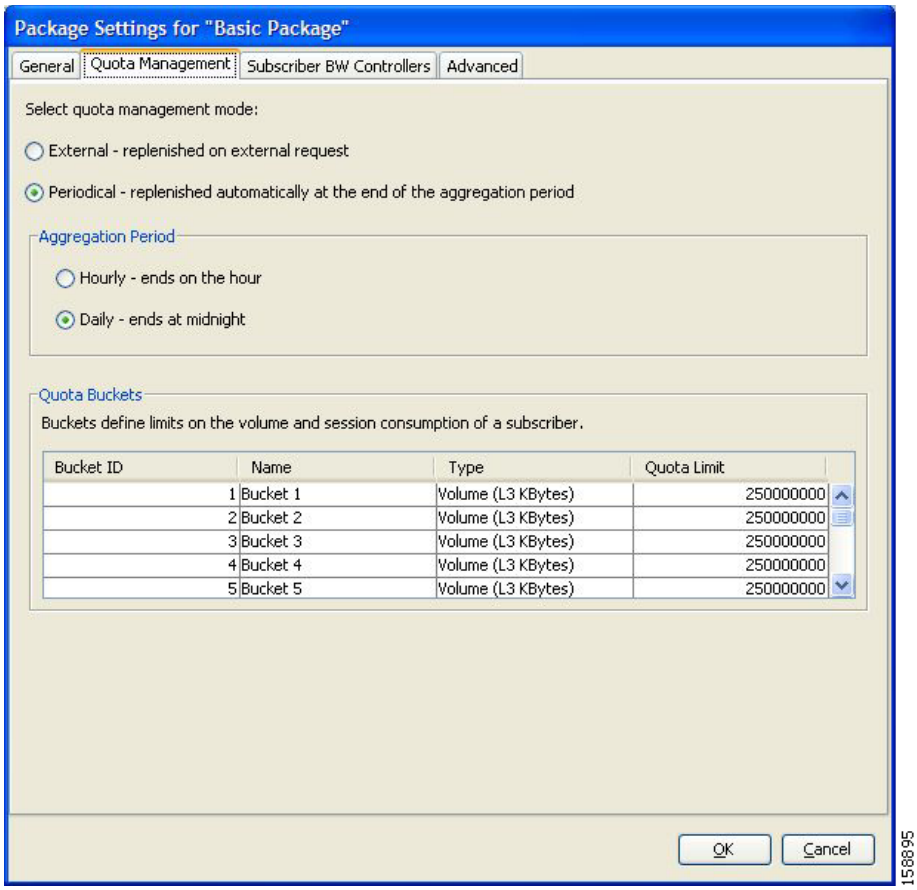
Step 1 In the Policies tab, select a package from the package tree, and click  (**Edit Package**).

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 9-64).

Figure 9-64 Quota Management Tab



Step 3 Select one of the **Select quota management mode** radio buttons.

- **External** —Replenishes quota on external request

Note External quota management is not supported when unidirectional classification is enabled. If you try to select the External radio button when unidirectional classification is enabled, a Package Error message appears.

Click **OK** to continue.

- **Periodical** —Replenishes quota automatically at the end of the aggregation period

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, page 9-75.)

Step 4 If you selected the Periodical radio button, select one of the **Aggregation Period** radio buttons to specify when the quota is renewed for the package:

- **Hourly Resolution** —Replenishes quota at each hour change
- **Daily Resolution** —Replenishes quota at midnight

Step 5 Configure the quota buckets.

Make sure that the configuration is appropriate to the rules that you will apply to the package. For example, if you do not configure a bucket with Type = Number of sessions, you cannot define a rule with usage limits defined in number of sessions.

a. (Optional) In the Name cell, enter a name for the bucket.

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

b. Click in the Type cell, click the drop-down arrow that appears in the cell, and then select either **Volume (L3 Kbytes)** or **Number of sessions** from the drop-down list.

c. In the Quota Limit cell, enter the actual limit for this bucket in kilobytes or number of sessions, depending on the selected Type.

In the Quota Limit cell, enter the actual limit for this bucket in kilobytes or number of sessions, depending on the selected Type.

Note Quota limits can be set only if you selected the Periodical radio button in Step 4 above.

Step 6 Click **OK.**

The Package Settings dialog box closes.

All changes to the quota management settings are saved.

How to Select Quota Buckets for Rules

You can select the quota buckets that the flows mapped to a rule will use. The quota buckets in the drop-down lists were defined during package setup (see How to Edit Quota Management Settings for Packages, page 9-75). 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, select a rule.

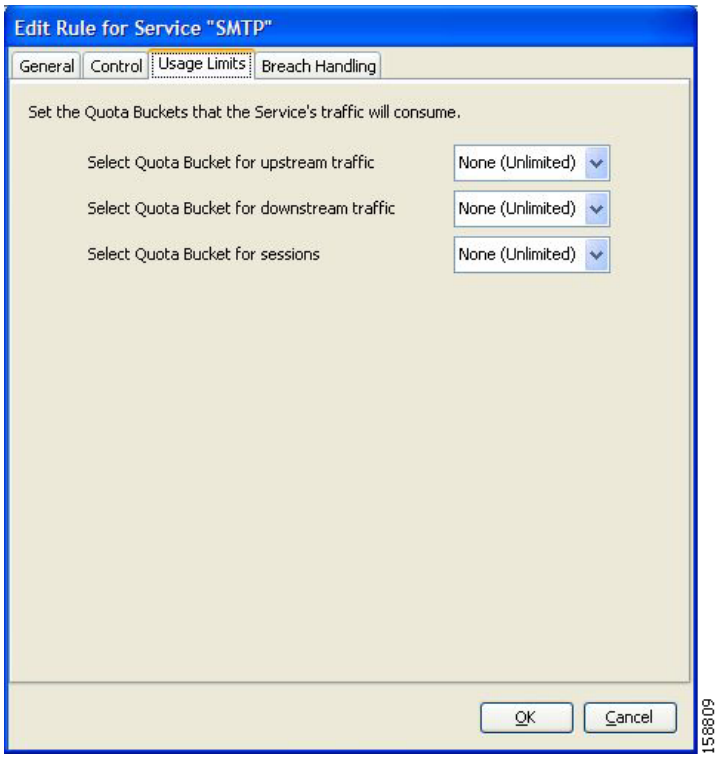
Step 3 Click  (**Edit Rule**).

The Edit Rule for Service dialog box appears.

Step 4 Click the **Usage Limits** tab.

The Usage Limits tab opens (Figure 9-65).

Figure 9-65 Usage Limits Tab



Step 5 Select the desired bucket from each drop-down list.

- **Select Quota Bucket for upstream traffic**
- **Select Quota Bucket for downstream traffic**
- **Select Quota Bucket for sessions**

Note For unlimited quota, select **None (Unlimited).**

Step 6 To define behavior when a quota is breached (not relevant if all quota buckets have unlimited quota), continue with the instructions in the following section.

Step 7 Click **OK.**

The Edit Rule for Service dialog box closes.

All changes to the rule are saved.

How to Edit Breach-Handling Parameters for a Rule

You can define the 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. SCA BB can generate Quota Breach RDRs even when this option is selected (see How to Manage Quota RDRs, page 8-7).
  - 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, page 10-41.) 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 this rule's traffic flows 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, page 10-30.

- 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.

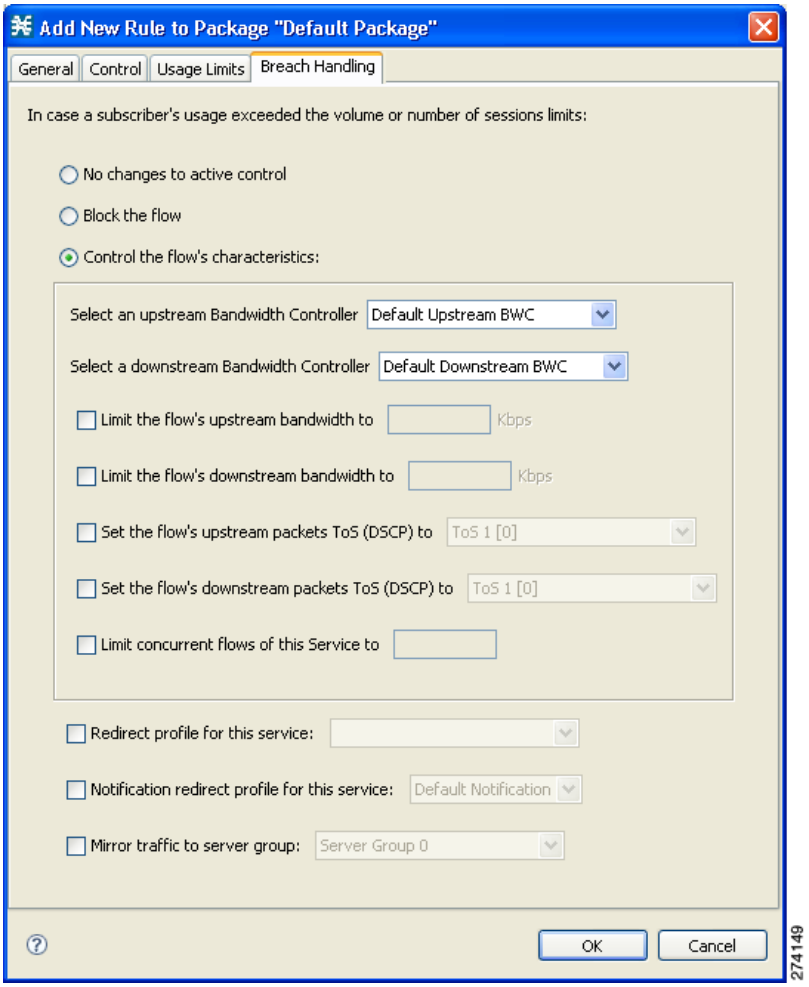
Step 3 Click (**Edit Rule**).

The Edit Rule for Service dialog box appears.

Step 4 Click the Breach Handling tab.

The Breach Handling tab opens (Figure 9-66).

Figure 9-66 Breach Handling Tab



Step 5 Set the flow's behavior when quota is breached.

- To block the flow when quota is breached, continue at Step 6.
- To change the flow's characteristics 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 flow's characteristics.

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 containing the properties of the selected BWC (Peak Information Rate (PIR), Committed Information Rate (CIR), Global Controller, and Assurance Level).

- 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 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, page 9-49.

Step 2 Enable periodical (internal) quota management.

a. Set the aggregation period to Daily

b. 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, page 9-75.

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, page 9-29.

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

For further information, see How to Add Rules to a Package, page 9-57.

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

For further information, see How to Define Per-Flow Actions for a Rule, page 9-59.

Step 6 Set the usage limit for the package to use the quota bucket defined in Step 2, page 351.

For further information, see the How to Select Quota Buckets for Rules, page 9-77 section.

Unknown Subscriber Traffic

A traffic flow that does not match any filter rule (see Filtering the Traffic Flows, page 10-19) is processed by the SCE platform, which tries to identify the subscriber responsible for the traffic flow. The SCE 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, page 9-29)
  - Select a calendar (see How to Set Advanced Package Options, page 9-51)
- Edit the default service rule for the Unknown Subscriber Traffic category:
  - Change the Rule State (see How to Edit Rules, page 9-61)
  - Change per-flow actions for the rule (see How to Define Per-Flow Actions for a Rule, page 9-59)
- Add rules to the Unknown Subscriber Traffic package:
  - Add rules (see How to Add Rules to a Package, page 9-57); edit (see How to Edit Rules, page 9-61) and delete (see How to Delete Rules, page 9-63) these rules
  - Add time-based rules (see How to Add Time-Based Rules to a Rule, page 9-64); edit (see How to Edit Time-Based Rules, page 9-66) and delete (see How to Delete Time-Based Rules, page 9-68) these rules