



## CHAPTER 9

# Using the Service Configuration Editor: Traffic Control

---

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.

- [Unknown Subscriber Traffic, page 9-1](#)
- [Managing Packages, page 9-2](#)
- [Managing Rules, page 9-10](#)
- [Managing Bandwidth, page 9-29](#)
- [Managing Virtual Links, page 9-43](#)
- [Managing Quotas, page 9-49](#)

## Unknown Subscriber Traffic

A traffic flow that does not match any filter rule (see [Filtering the Traffic Flows, page 10-17](#)) 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 9-37](#))
  - Select a calendar (see [How to Set Advanced Package Options, page 9-7](#))
- Edit the default service rule for the Unknown Subscriber Traffic category:
  - Change the Rule State (see [How to Edit Rules, page 9-16](#))
  - Change per-flow actions for the rule (see [How to Define Per-Flow Actions for a Rule, page 9-14](#))
- Add rules to the Unknown Subscriber Traffic package:
  - Add rules (see [How to Add Rules to a Package, page 9-12](#)); edit (see [How to Edit Rules, page 9-16](#)) and delete (see [How to Delete Rules, page 9-18](#)) these rules
  - Add time-based rules (see [How to Add Time-Based Rules to a Rule, page 9-20](#)); edit (see [How to Edit Time-Based Rules, page 9-21](#)) and delete (see [How to Delete Time-Based Rules, page 9-23](#)) these rules

## 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 7-1](#)) 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, page 9-3](#)
- [How to View Packages, page 9-4](#)
- [How to Add Packages, page 9-5](#)
- [How to Set Advanced Package Options, page 9-7](#)
- [How to Duplicate Packages, page 9-8](#)
- [How to Edit Packages, page 9-8](#)
- [How to Delete Packages, page 9-10](#)

## 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.

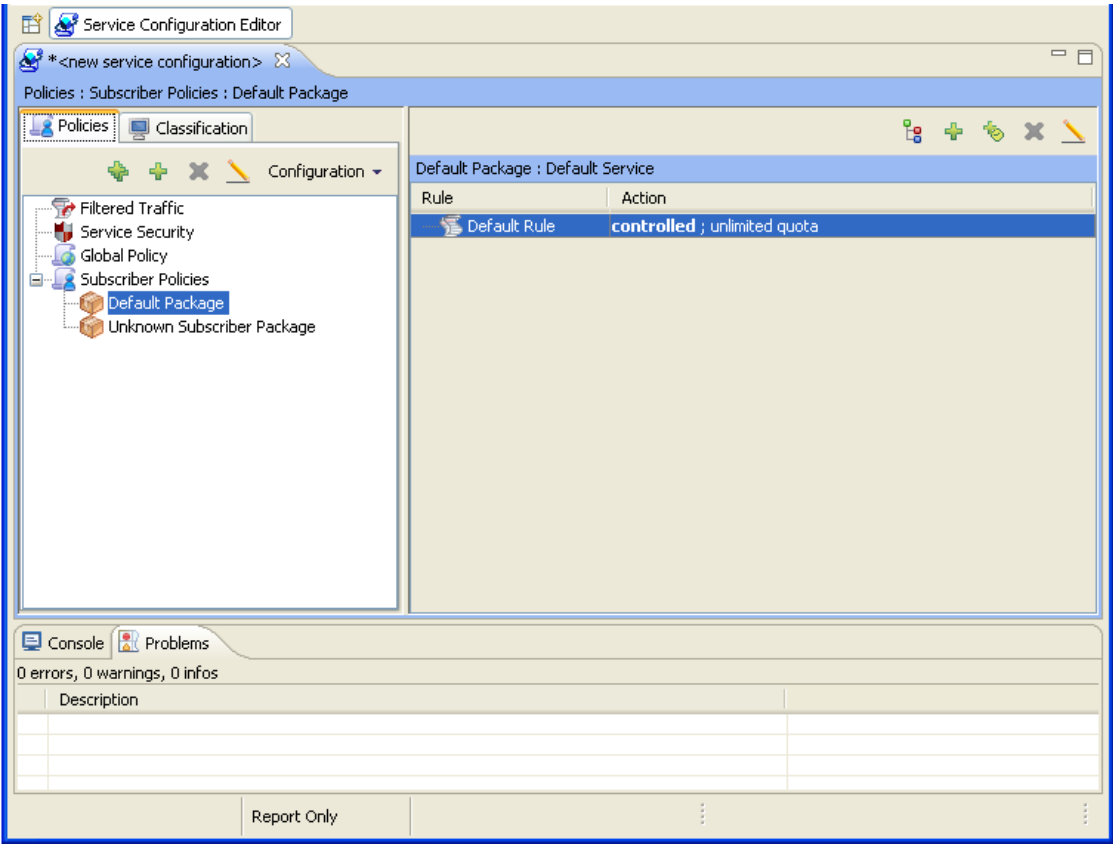
- A unique counter index—A default value of the counter index is provided by the system. Do not modify this value.
- Calendar—The calendar used as the basis for the time-based rules of the package.
- VAS Traffic Forwarding Table—The forwarding table used by the package.

These parameters are defined when you add a new package (see [How to Add Packages, page 9-5](#)). You can modify them at any time (see [How to Edit Packages, page 9-8](#)).

# 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 Network Traffic tab.  
The Network Traffic tab appears.

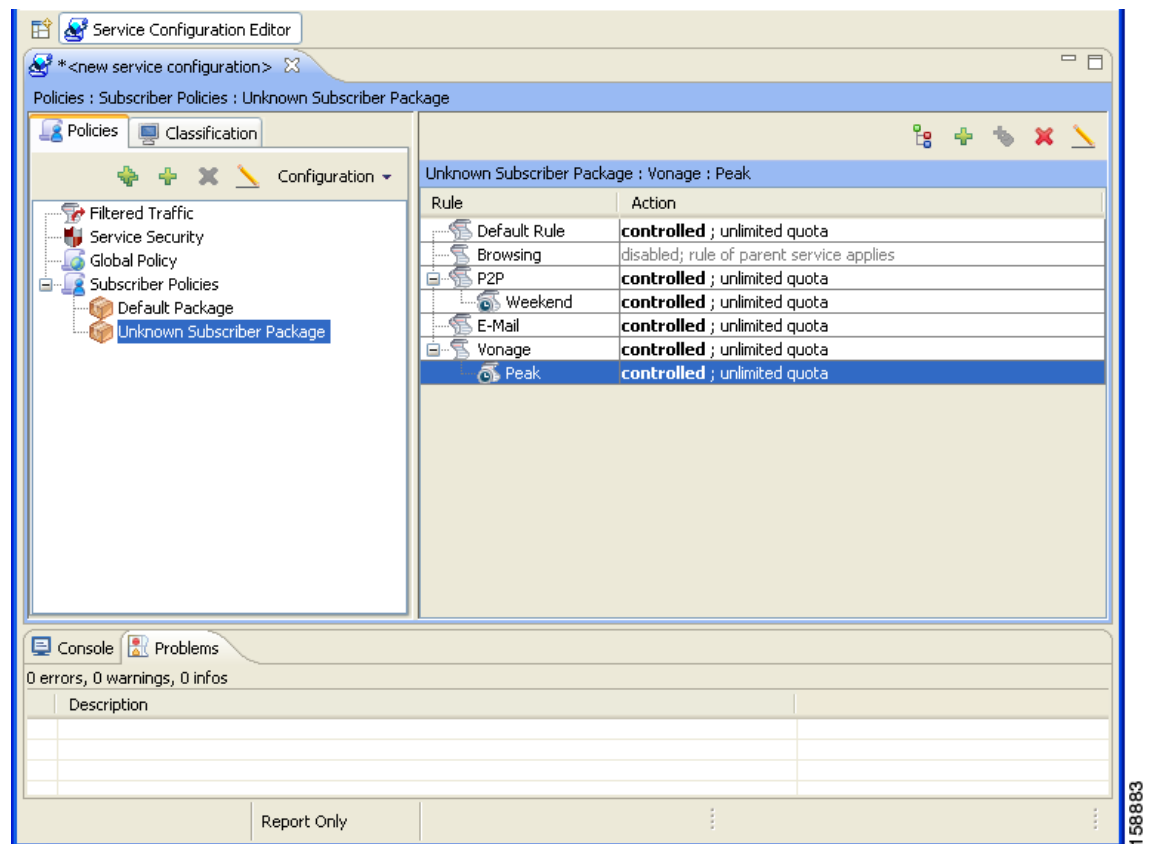


A list of all packages is displayed in the package tree.

**Note**

To view more information about a package, open the Package Settings dialog box (see [How to Edit Packages, page 9-8](#)).

- 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.




158883

## 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 9-12](#)).

- Step 1** In the Network Traffic tab, select a package from the package tree. This package will be the parent of the package you are adding.
- Step 2** In the Network Traffic tab, click  (Add Package).  
The Package Settings dialog box appears.

Package Settings for ""

General Quota Management Subscriber BW Controllers Advanced

Package name:  
Package1

Description:

OK Cancel

158894

- 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 9-10](#).

## What to Do Next

To configure parameters in the Quota Management tab see [How to Edit Quota Management Settings for Packages, page 9-49](#).

To configure parameters in the Subscriber BW Controllers tab, see [How to Edit Package Subscriber BWCs, page 9-37](#).

## 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.

- 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 10-47](#).

- 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 9-10](#).

## 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 Network Traffic tab, select a package from the package tree.

- Step 2** In the Network Traffic 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 9-8](#)).

## How to Edit Packages

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

- Step 1** In the Network Traffic tab, select a package from the package tree.

- Step 2** In the Network Traffic 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** To 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 9-49.
- Step 6** To change bandwidth control settings, see [How to Edit Package Subscriber BWCs](#), page 9-37.
- Step 7** To change advanced settings, click the Advanced tab.
- The Advanced tab opens.
- 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.

- To change the parent package of this package, select the desired parent from the Select Parent Package drop-down list.
- 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.
- 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.
- 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.

- To change the calendar used by this package, select the desired calendar from the Select Calendar for this Package drop-down list.
- 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 10-47.

- Step 8** Click **OK**.
- The Package Settings dialog box closes.
- All changes to the package parameters are saved.

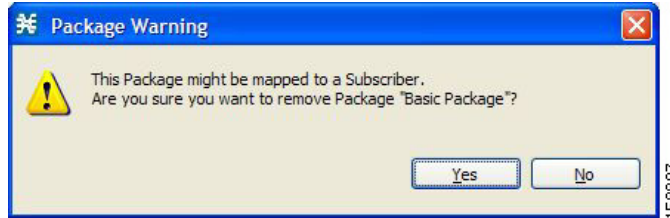
## How to Delete Packages

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

**Step 1** In the Network Traffic tab, select a package from the package tree.

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

A Package Warning message appears.



**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, page 9-11](#)
- [Rule Hierarchy, page 9-11](#)
- [How to View the Rules of a Package, page 9-11](#)
- [How to Add Rules to a Package, page 9-12](#)
- [How to Define Per-Flow Actions for a Rule, page 9-14](#)
- [How to Edit Rules, page 9-16](#)
- [How to Delete Rules, page 9-18](#)
- [How to Display the Services Affected by a Rule, page 9-18](#)
- [Managing Time-Based Rules, page 9-19](#)
- [How to Manage DSCP ToS Marker Values, page 9-28](#)

## 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 .

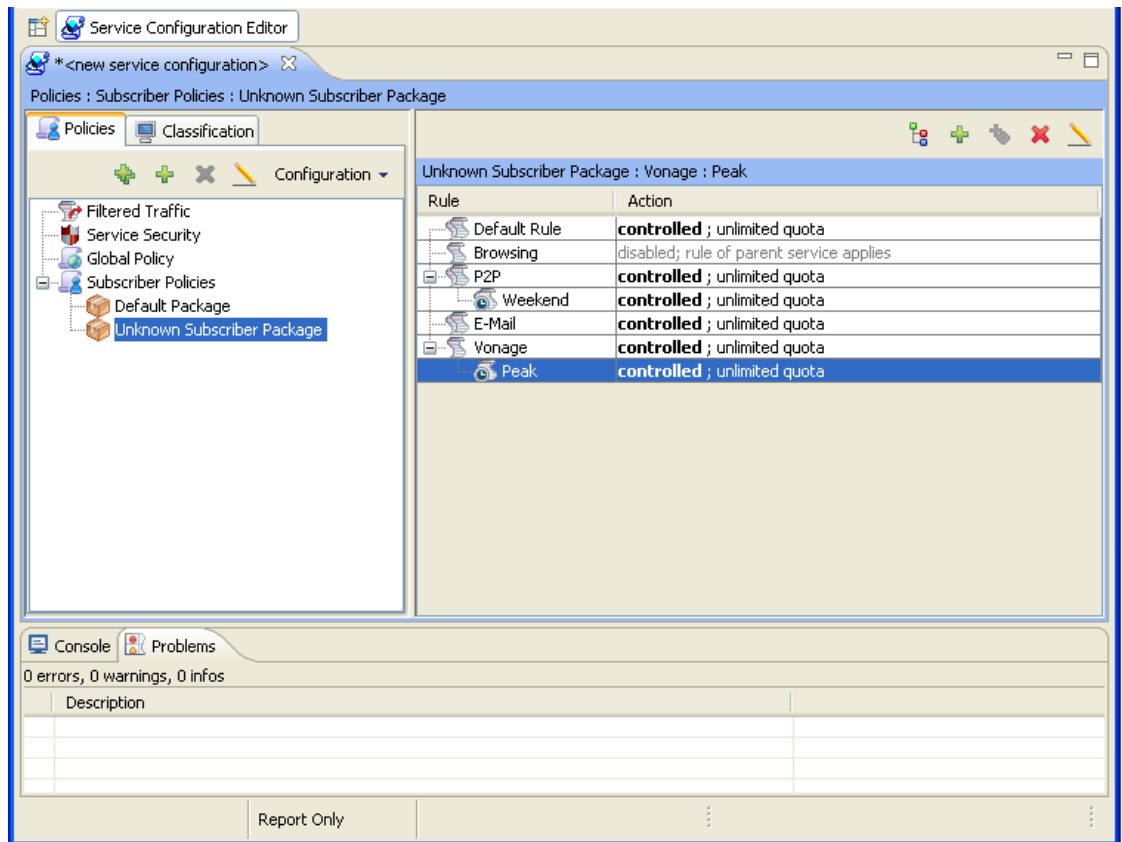
See also [How to Display the Services Affected by a Rule, page 9-18](#).

## 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 Network Traffic tab, select a package from the package tree.
- A list of all rules defined for this package is displayed in the right (Rule) pane.



## 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 9-16).

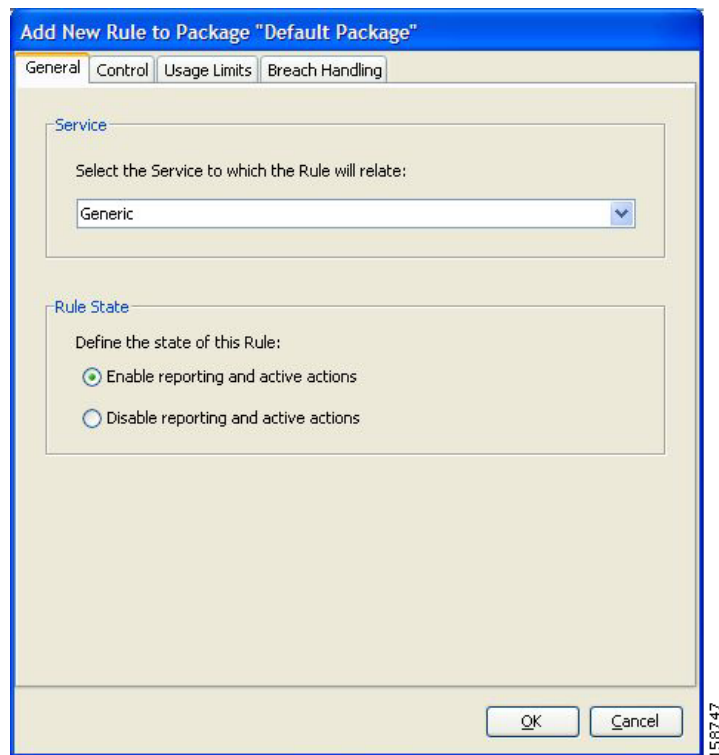
To see more information about a time-based rule, open the Edit Time-Based Rule for Service dialog box (see [How to Edit Time-Based Rules](#), page 9-21).

## 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 9-20.

- Step 1** In the Network Traffic 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.



- 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 9-16](#)).

- Step 5** To 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 9-14](#).

- 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

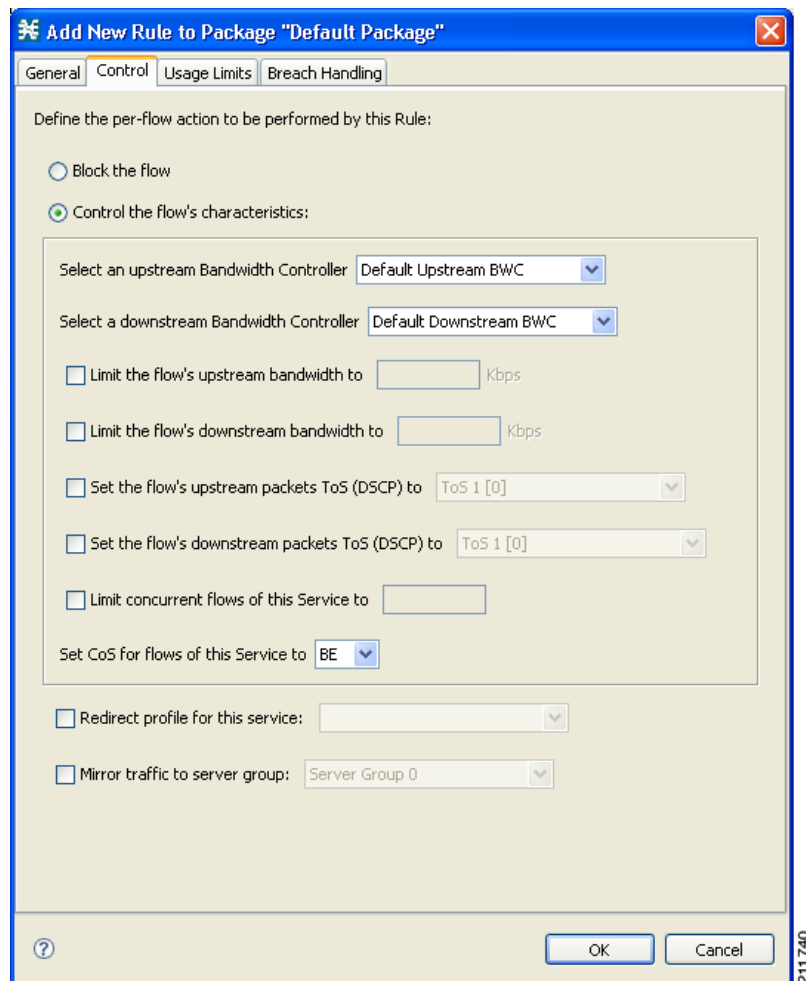
Usage limits and breach handling are part of quota management (see [Managing Quotas, page 9-49](#)):

- To configure parameters in the Usage Limits tab see [How to Select Quota Buckets for Rules, page 9-51](#).
- To configure parameters in the Breach Handling tab, see [How to Edit Breach-Handling Parameters for a Rule, page 9-52](#).

## 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.



To control flows that are mapped to the service of this rule, continue at Step 5.

- Step 2** To block flows that are mapped to the service of this rule, select the **Block the flow** radio button. The Redirect to check box is enabled.



**Note** Only three protocol types support redirection: HTTP, HTTP Streaming, and RTSP.

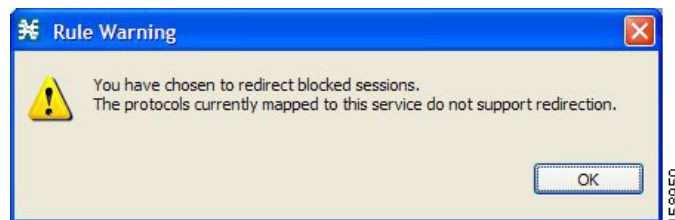
- Step 3** (Optional) To redirect blocked flows, check the **Redirect to** check box.



**Note** Redirection is not supported when unidirectional classification is enabled.

The Redirection URL Set drop-down list is enabled.

- If the service or service group for this rule includes protocols that cannot be redirected, a Rule Warning message appears.



- Click **OK**.

From the Redirection URL Set drop-down list, select a URL set to serve as the redirection target. (URL redirection sets are defined in the System Settings dialog box. See [How to Add a Set of Redirection URLs, page 10-37](#).)

- Step 4** Continue at Step 14.

- Step 5** Select the **Control the flow's characteristics** radio button.

The options in the Flow Characteristic area are enabled.

- Step 6** 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 (see [How to Edit Package Subscriber BWCs, page 9-37](#)).



**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 (see [How to Set the Maximum Bandwidth of Global Controllers, page 9-32](#)). Do not create a separate global controller for each time frame.

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).

**Step 7** From the downstream Bandwidth Controller drop-down list, select a downstream BWC.

**Step 8** (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 9** (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 10** (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.

**Step 11** (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 12** (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 13** From the Set CoS for flows of this Service drop-down list, select a class-of-service.

**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**

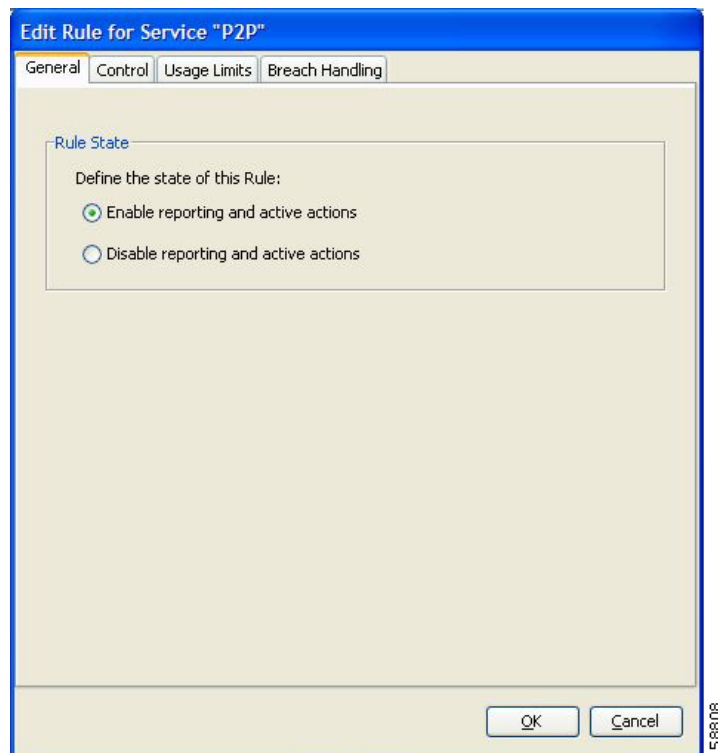
The tabs of the Edit Rule for Service dialog box are the same as the tabs of the Add New Rule to Package dialog box, except for the General tab—you cannot change the service to which the rule applies.

**Step 1** In the 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** 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 9-14.

**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 9-51.

- Step 7** Define behavior when a quota is breached.
- Click the **Breach Handling** tab.  
The Breach Handling tab opens.
  - Follow the instructions in [How to Edit Breach-Handling Parameters for a Rule, page 9-52](#).
- 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 9-16](#)). 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 Network Traffic 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.



- 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 default service rule and the P2P rule in the following figure.


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

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

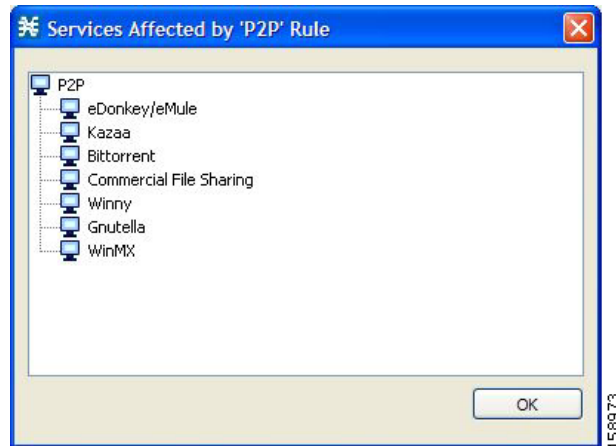
**Note**

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

**Step 1**

In the right (Rule) pane of the Network Traffic tab, select a rule and click  (Show All Services Affected By This Rule).

The Services Affected dialog box appears.

**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 9-23](#)). 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 the following screen capture.

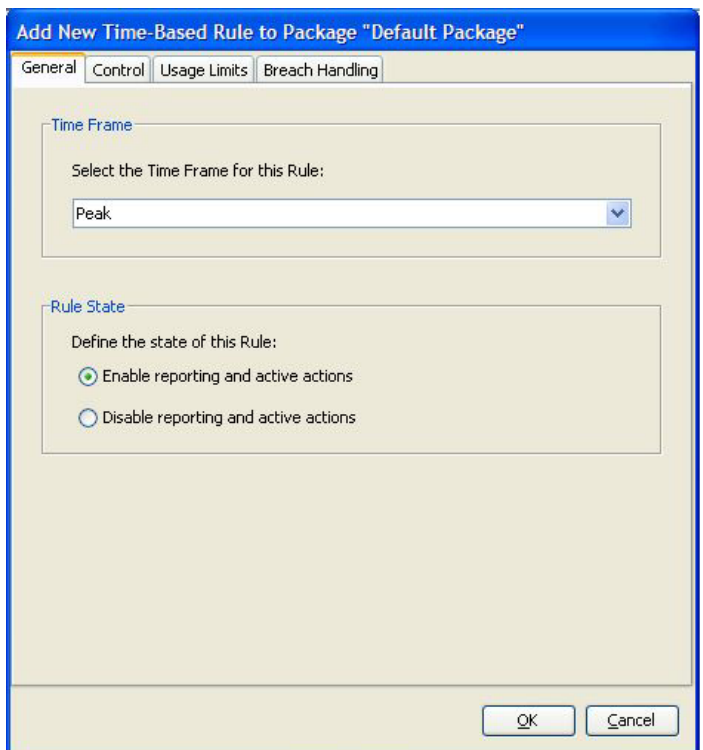
Rule	Action
Default Rule	controlled [Default Upstream BWC; Default Downstream BWC]; unlimited quota
P2P	controlled [Default Upstream BWC; Default Downstream BWC]; quota replenished ...
Weekend	controlled [Default Upstream BWC; Default Downstream BWC]; quota replenished ...
Yahoo Messenger VoIP	controlled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

**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  (**Add Time-Based Rule**).

The Add New Time-Based Rule dialog box appears.



The dialog box titled "Add New Time-Based Rule to Package 'Default Package'" has four tabs: General, Control, Usage Limits, and Breach Handling. The General tab is active. It contains two sections: "Time Frame" and "Rule State".

**Time Frame:** A label "Select the Time Frame for this Rule:" is above a dropdown menu currently set to "Peak".

**Rule State:** A label "Define the state of this Rule:" is above two radio buttons: "Enable reporting and active actions" (which is selected) and "Disable reporting and active actions".

At the bottom right are "OK" and "Cancel" buttons.

- 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 9-14](#).
- 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 9-51](#).
- 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 9-52](#).
- 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.

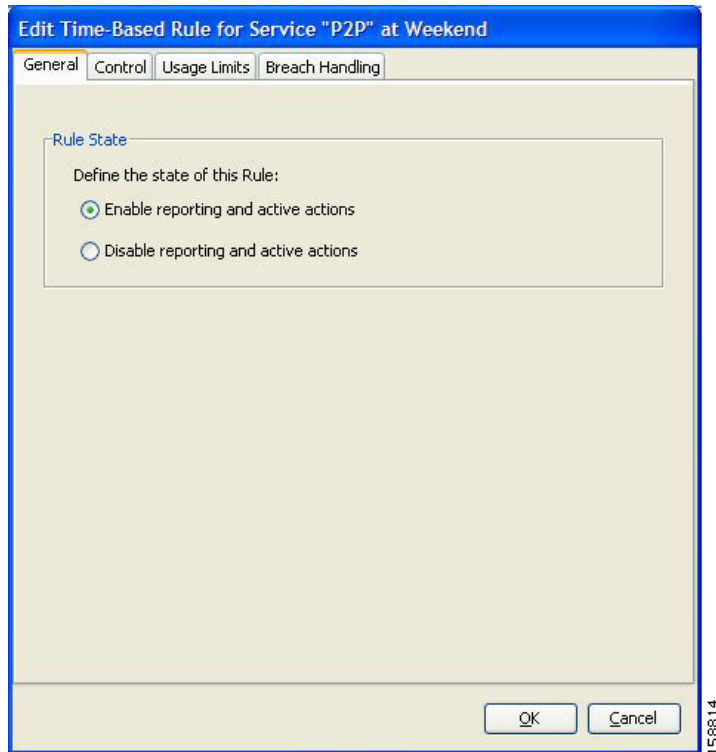


### Note

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 Network Traffic 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.



- 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 9-14.
- 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 9-51.
- 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 9-52.
- 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

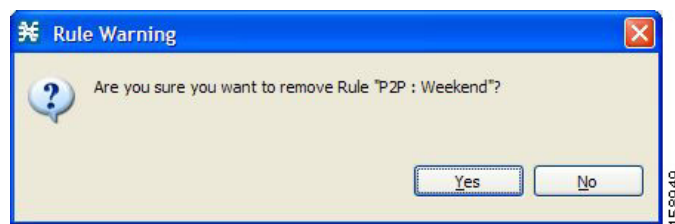
You can *disable* a rule without losing its profile (see [How to Edit Time-Based Rules, page 9-21](#)). This allows you to enable the rule again later, without having to reset all its parameters.

**Step 1** In the Network Traffic 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.



**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.

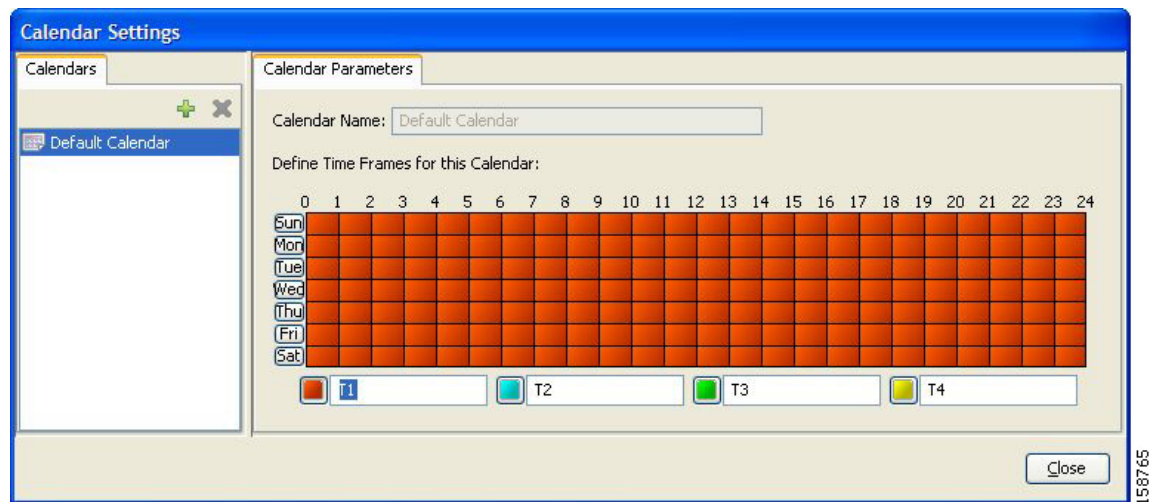
- [How to View Calendars, page 9-24](#)
- [How to Add Calendars, page 9-24](#)
- [How to Rename the Time Frames, page 9-25](#)
- [How to Delete Calendars, page 9-26](#)
- [How to Configure the Time Frames, page 9-26](#)

### How to View Calendars

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

**Step 1** From the Console main menu, choose **Configuration > Weekly Calendars**.

The Calendar Settings dialog box appears.



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 Console main menu, choose **Configuration > Weekly Calendars**.

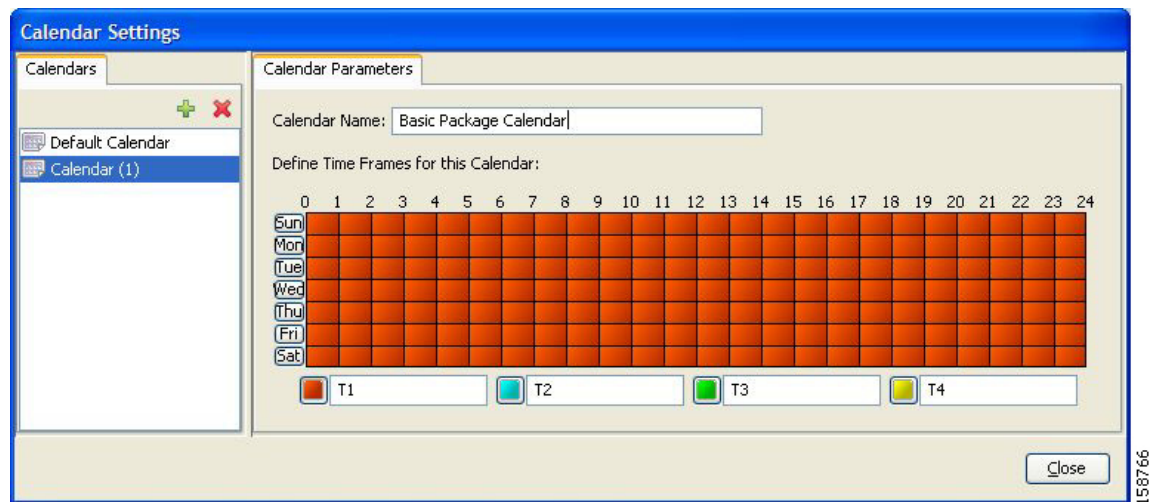
The Calendar Settings dialog box appears.

**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, click in the Calendar Name field and enter the name for this calendar.





**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

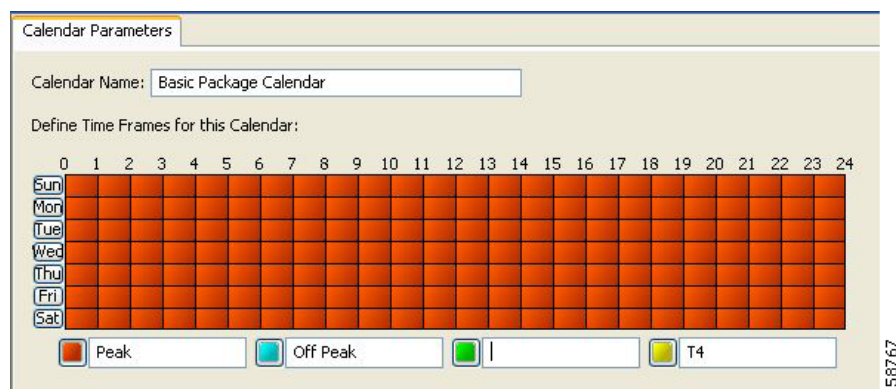
Although you can configure the time frames differently in each calendar, the names of the time frames are the same in all of the calendars. If you change the name when configuring one calendar, the names are also changed for all other calendars.

**Step 1** From the Console main menu, choose **Configuration > Weekly Calendars**.

The Calendar Settings dialog box appears.

In the Calendar Parameters tab, 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.



**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.)

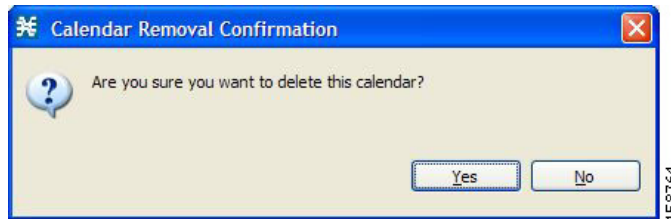
To delete the calendar, you must first select a different calendar for each package using the calendar that will be deleted. See [How to Set Advanced Package Options, page 9-7](#) for information about changing the calendar associated with a package.

**Step 1** From the Console main menu, 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.



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

The calendar is deleted.

**Step 4** Click **Close**.

The Calendar Settings dialog box closes.

### How to Configure the Time Frames

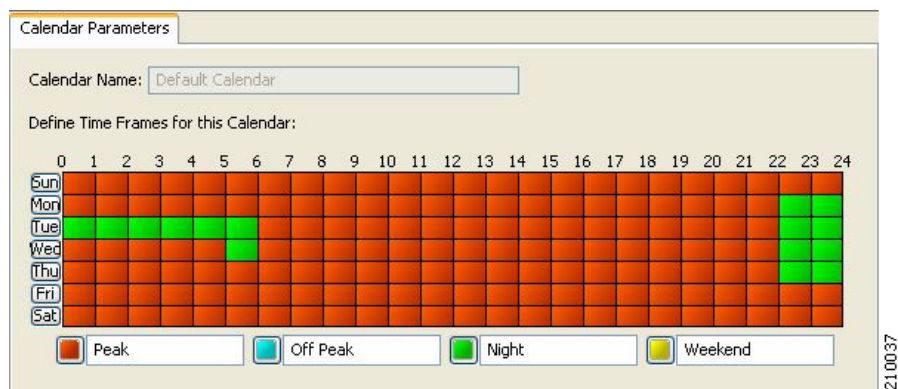
By default, all the hours of the week belong to one time frame. The Console allows you to assign each of the 168 (24x7) hours of the week to one of four separate time frames. These time frames allow you to supply time-dependent differentiated services and to impose constraints on any service.

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

- Peak
- Off Peak
- Night
- Weekend

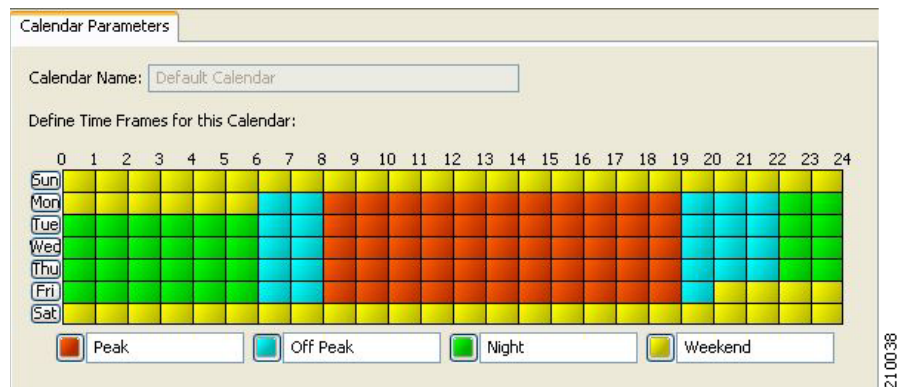
You can define different time frames for each calendar.

- Step 1** From the Console main menu, 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.



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. The following figure illustrates a possible time partition plan:



- 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 10-20) or a service rule (see Steps 10 and 11 of [How to Define Per-Flow Actions for a Rule](#), page 9-14 and Step 9 of [How to Edit Breach-Handling Parameters for a Rule](#), page 9-52).

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 (see [How to Reconfigure DSCP Marking for Release 3.1.5 and Higher](#), page 4-9).

## 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 Console main menu, choose **Configuration > ToS Marking Settings**.

The ToS Marking Settings dialog box appears.

ToS Marking Settings

ToS Marking allows setting the DSCP ToS value of the flow.  
ToS Marking are enabled per direction.

☐ Enable Upstream ToS Marking

☐ Enable Downstream ToS Marking

ToS Marking allows setting seven DSCP ToS values as an action of the Package rules or for Flow Filter rules.  
The values allowed are between 0 and 63 and are given as an integer.

ToS Markers

ToS Marker Class	DSCP Value
ToS 1	0
ToS 2	0
ToS 3	0
ToS 4	0
ToS 5	0
ToS 6	0
ToS 7	0

OK

Cancel

**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 Bandwidth

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

A service configuration can contain up to 1024 upstream global controllers and 1024 downstream global controllers (including the default global controllers).

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, page 9-30](#)
- [How to View Global Controller Settings, page 9-30](#)
- [How to Edit the Total Link Limits, page 9-31](#)
- [How to Add Global Controllers, page 9-32](#)
- [How to Set the Maximum Bandwidth of Global Controllers, page 9-32](#)
- [How to Delete Global Controllers, page 9-34](#)

- [Defining Global Controllers in a Dual-Link System, page 9-34](#)
- [Managing Subscriber Bandwidth, page 9-35](#)
- [Managing Bandwidth: a Practical Example, page 9-39](#)
- [How to Set BW Management Prioritization Mode, page 9-42](#)

## Managing Global Bandwidth

The upstream and downstream interfaces are each assigned one default global controller that, by default, controls 100 percent of the link traffic. You can add up to 1023 more global controllers for each interface, and assign a maximum percentage 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

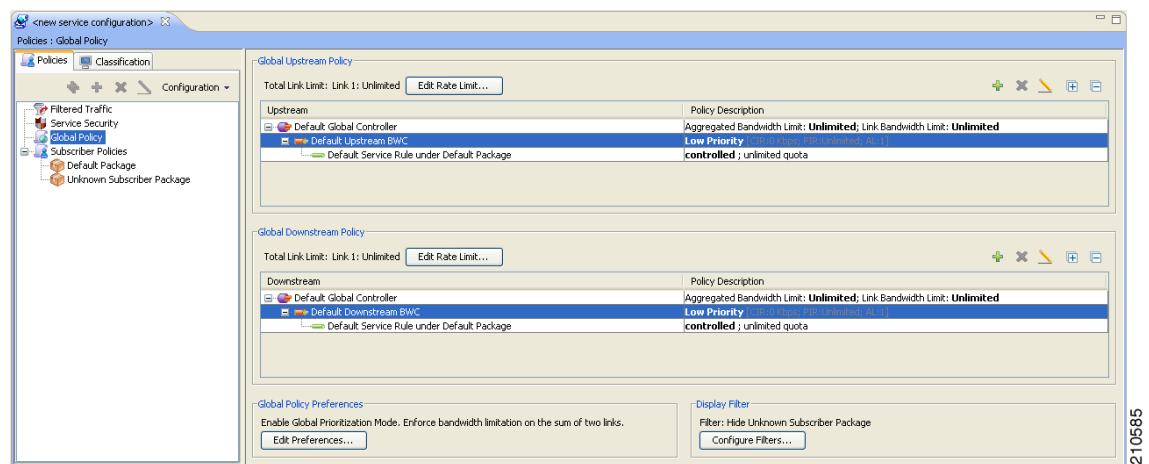


### Note

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** From the Console main menu, choose **Configuration > Global Bandwidth Settings**.  
The Global Bandwidth Settings dialog box appears.



The two check boxes near the top of the Global Controllers tab are used only in dual-link systems (see [Defining Global Controllers in a Dual-Link System, page 9-34](#)).

The main part of the dialog box contains the Upstream area listing upstream global controllers and the Downstream area listing downstream global controllers. Each list has four columns; the third and fourth columns are relevant to dual-link systems:

- **Name** —A unique name assigned to the global controller. The system automatically assigns the names Controller 1, Controller 2, and so on.
- **Link 1 BW (%)** —The maximum percentage of the total link limit permitted to this global controller.

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 9-23):

- 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.

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

- If two time frames have the same maximum bandwidth, the value is not repeated. (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.)

Name	Link 1 BW (%)
Downstream Total Link Limit	100
Default Global Controller	100
Downstream Controller 1	40,,,100

- Trailing commas are suppressed. (So **40,100** means that the first time frame has a maximum bandwidth of 40 percent of the total link limit, and the other three time frames have a maximum bandwidth equal to the total link limit.)

**Step 2** To view the actual maximum bandwidth values, place the cursor over the Link 1 BW (%) cell.

A tooltip appears, showing the actual maximum bandwidth permitted to this global controller, in Mbps. This figure is calculated automatically by the system based on the possible SCE platform types (Gigabit Ethernet or Fast Ethernet), the controller maximum bandwidth percentage, and the total link bandwidth percentage.

Name	Link 1 BW (%)	Link 2 BW (%)	Aggregated BW (%)
Upstream Total Link Limit	100	100	N/A
Default Global Controller	100	100	N/A
Upstream Controller 1	40,60,80,100	40,60,80,100	N/A

**Fast Ethernet** = 40Mbps, 60Mbps, 80Mbps, 100Mbps  
**Gigabit Ethernet** = 800Mbps, 1200Mbps, 1600Mbps, 2000Mbps

**Step 3** Click **OK**

The Global Bandwidth Settings dialog box closes.

## How to Edit the Total Link Limits

You can limit the total bandwidth passing through the SCE platform.



For example, if another device sitting next to the SCE platform on the IP stream has limited BW capacity, you can limit the bandwidth 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** From the Console main menu, choose **Configuration > Global Bandwidth Settings**.  
The Global Bandwidth Settings dialog box appears.
- Step 2** Click in the Link 1 BW (%) cell of the Upstream Total Link Limit or Downstream Total Link Limit, and enter the maximum percentage of the SCE platform capacity that the platform will carry.  
The values displayed in the tooltips of all the cells in the Link 1 BW (%) cells change to reflect the new total link limit.
- Step 3** Click **OK**  
Your changes are saved.  
The Global Bandwidth Settings dialog box closes.
- 

## How to Add Global Controllers

You can add up to 1023 upstream global controllers and 1023 downstream global controllers to a service configuration.

- 
- Step 1** From the Console main menu, choose **Configuration > Global Bandwidth Settings**.  
The Global Bandwidth Settings dialog box appears.
- Step 2** Above the area (Upstream or Downstream) of the desired interface, click  (**Add**).  
A new global controller is added to the interface global controller list with a maximum bandwidth capacity of 100 percent of the total link limit.
- Step 3** In the Name cell of the new global controller, enter a meaningful name.
-  **Note** You can use the default name for the global controller. It is recommended that you enter a meaningful name.
- 
- Step 4** 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 9-32](#).
- Step 5** Click **OK**  
Your changes are saved.  
The Global Bandwidth Settings dialog box closes.
- 

## How to Set the Maximum Bandwidth of Global Controllers

You can edit the maximum bandwidth (as a percentage of the total link limit) that a global controller can carry.

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

In a dual-link system, you can set different values for each link and for the aggregated BW of the two links.



**Step 1** From the Console main menu, choose **Configuration > Global Bandwidth Settings**.

The Global Bandwidth Settings dialog box appears.

**Step 2** Click in a BW (%) cell of a global controller listing.

A Browse button appears in the cell.

**Step 3** Click the **Browse** button.

The Global Controller Bandwidth Settings dialog box appears.

**Step 4** Set a single value for the maximum percentage of the total link limit that this global controller carries.

- Select **Enforce a single BW limit**, and enter the desired value for the maximum percentage of bandwidth.

**Step 5** Set the maximum percentage of the total link limit that this global controller carries to vary according to time frame.

- Select **Enforce a separate BW limit per Time Frame**, and enter the desired value in each BW (%) cell.



**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 BW (%) cell changes to reflect the new bandwidth limits.

- Step 7** Repeat Steps 2 to 6 for other global controllers.
- Step 8** Click **OK**
- Your changes are saved.
- The Global Bandwidth Settings dialog box closes.
- 

## 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** From the Console main menu, choose **Configuration > Global Bandwidth Settings**.
- 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 9-37](#)), 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.
- 

## Defining Global Controllers in a Dual-Link System

In a dual-link system, you can define each global controller's maximum bandwidth separately for each link.

Alternatively, you can apply bandwidth limitations to the sum of the two links.



### Note

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

---

- [How to Set Global Controller Bandwidth Limits Separately for Each Link, page 9-35](#)
- [How to Set Global Controller Bandwidth Limits as the Sum of Two Links, page 9-35](#)

## How to Set Global Controller Bandwidth Limits Separately for Each Link

- 
- Step 1** From the Console main menu, choose **Configuration > Global Bandwidth Settings**.  
The Global Bandwidth Settings dialog box appears.
- Step 2** Add global controllers, as described in [How to Add Global Controllers, page 9-32](#).
- Step 3** Check the **Allow separate BW setting for each link** check box.  
The cells in the Link 2 BW (%) column are enabled.  
Each cell has the same value as the parallel cell in the Link 1 BW (%) column.
- Step 4** Define the bandwidth percentages (Link 1 BW (%)) for the global controllers for link 1.  
Changes to bandwidth percentages are not copied to the Link 2 tab.
- Step 5** In the Link 2 BW (%) column, define the bandwidth percentages for the global controllers for link 2.
- Step 6** Click **OK**  
Your changes are saved.  
The Global Bandwidth Settings dialog box closes.
- 

## How to Set Global Controller Bandwidth Limits as the Sum of Two Links

- 
- Step 1** From the Console main menu, choose **Configuration > Global Bandwidth Settings**.  
The Global Bandwidth Settings dialog box appears.
- Step 2** Check the **Enforce BW limitation on the sum of two links** check box.  
The cells in the Aggregated BW (%) column are enabled and contain the value 100.
- Step 3** Click **OK**  
Your changes are saved.  
The Global Bandwidth Settings dialog box closes.
- 

## 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 9-14](#).
- Extra BWCs also operate at the subscriber level. Extra BWCs (based on the CIR, PIR, global controller, and AL) can be allocated for services that are not included in the Primary BWC. These are services that are not often used but have strict bandwidth requirements, for example, video conference calls. The Extra BWCs are BWCs that control a single service (or service group). BWCs cannot borrow bandwidth from Extra BWCs and vice versa.

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



#### Caution

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

- [Subscriber BWC Parameters, page 9-36](#)
- [How to Edit Package Subscriber BWCs, page 9-37](#)

## 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

Bandwidth for a subscriber BWC has a granularity of 16 Kbps:

If you specify a bandwidth of, for example, 64 Kbps, the bandwidth will be stable at this value.

If you specify a bandwidth of, for example, 70 Kbps, the bandwidth will be unstable and oscillate between 64 Kbps and 80 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 Network Traffic 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 **Subscriber BW Controllers** tab. The Subscriber BW Controllers tab opens.

**Package Settings for "Basic Package"**

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

Subscriber BW Controllers limit the BW of transaction groups and prioritize between transactions of different services for a single subscriber. They are also used for linking services to Global Controllers.

**Upstream**

Subscriber relative priority (upstream): 1

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



**Downstream**

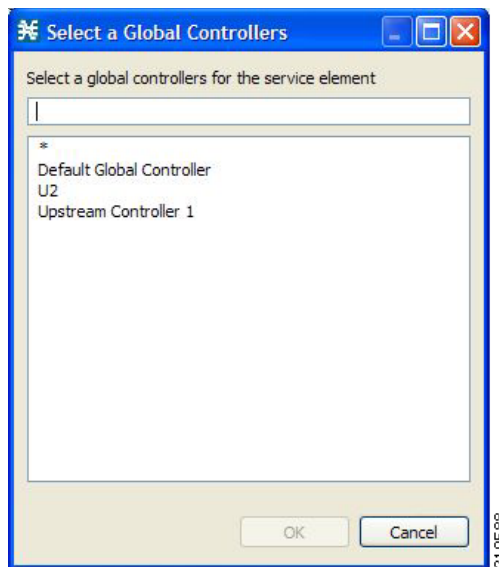
Subscriber relative priority (downstream): 1

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

OK Cancel

158896

- Step 3** Set your requirements for upstream bandwidth control in the Upstream area of the dialog box.
- Select a value from the Subscriber relative priority drop-down list.
  - Set the parameters for the Primary Upstream BWC.
    - In the CIR field, enter the BWC CIR in Kbps.
    - In the PIR field, select **Unlimited** from the drop-down list, or enter the BWC PIR in Kbps.
  - To add BWCs to the package, click  (**Add a sub BW Controller**) once for each additional BWC.
  - To add Extra BWCs to the package, click  (**Add an extra BW Controller**) once for each additional BWC.
  - 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.



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

**Step 4** Repeat Step 3 for downstream bandwidth control in the Downstream area of the dialog box.

**Step 5** 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 9-39](#)
- [Example: How to Limit P2P and Streaming Traffic Using the Console, page 9-39](#)

### 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 percentage of 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 percentage of total available bandwidth. (See [How to Use the P2P Traffic Optimization Wizards, page 4-30.](#))

- 
- Step 1** In the Global Bandwidth Settings dialog box, add two upstream global controllers and two downstream global controllers and assign the desired percentage of traffic to each global controller.

**Global Upstream Policy**

Total Link Limit: Link 1: Unlimited [Edit Rate Limit...](#)

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

**Global Downstream Policy**

Total Link Limit: Link 1: Unlimited [Edit Rate Limit...](#)

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

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

**Package Settings for "Gold"**

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

Subscriber BW Controllers limit the BW of transaction groups and prioritize between transactions of different services for a single subscriber. They are also used for linking services to Global Controllers.

**Upstream**

Subscriber relative priority (upstream): 1

Name	CIR (L3 K...	PIR (L3 K...	Global Controller	AL
Primary Upstream BWC	0	Unlimited		
Default Upstream BWC	0	Unlimited	Default Global Controller	1
BWC 1	0	Unlimited	Upstream Global Controller 1	1
BWC 2	0	Unlimited	Upstream Global Controller 2	1

**Downstream**

Subscriber relative priority (downstream): 1

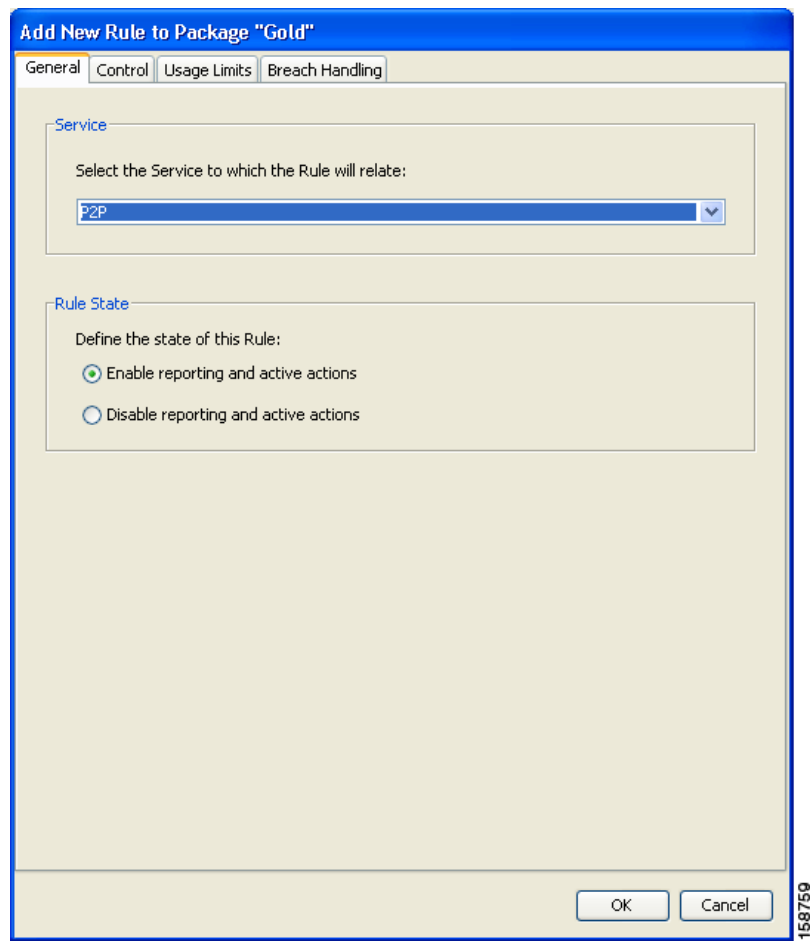
Name	CIR (L3 K...	PIR (L3 K...	Global Controller	AL
Primary Downstream BWC	0	Unlimited		
Default Downstream BWC	0	Unlimited	Default Global Controller	1
BWC 3	0	Unlimited	Downstream Global Controller 1	1
BWC 4	0	Unlimited	Downstream Global Controller 2	1

OK Cancel

(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 3** Add a rule for the P2P service.





**Step 4** In the Control tab, assign BWC 1 as the upstream BWC and BWC 3 as the downstream BWC.

**Add New Rule to Package "Default Package"**

General Control Usage Limits Breach Handling

Define the per-flow action to be performed by this Rule:

☐ Block the flow

☒ Control the flow's characteristics:

Select an upstream Bandwidth Controller: BWC 1

Select a downstream Bandwidth Controller: BWC 3

☐ Limit the flow's upstream bandwidth to: [ ] kbps

☐ Limit the flow's downstream bandwidth to: [ ] kbps

☐ Set the flow's upstream packets ToS (DSCP) to: ToS 1 [0]

☐ Set the flow's downstream packets ToS (DSCP) to: ToS 1 [0]

☐ Limit concurrent flows of this Service to: [ ]

Set CoS for flows of this Service to: BE

☐ Redirect profile for this service: [ ]

☐ Mirror traffic to server group: Server Group 0

OK Cancel

**Step 5** Repeat Steps 3 and 4 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.

## 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:

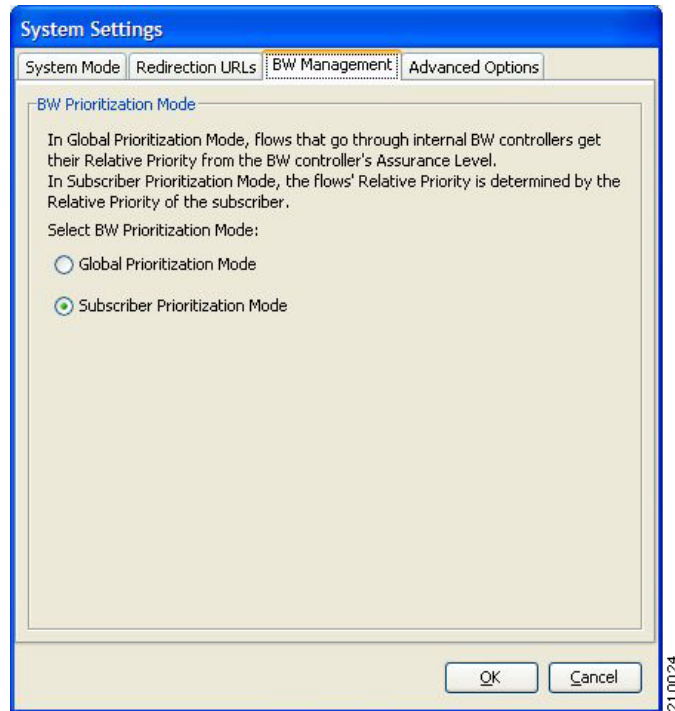
- The iBWC—In Global Prioritization Mode
- The subscriber—In Subscriber Prioritization Mode

**Step 1** From the Console main menu, choose **Configuration > System Settings**.

The System Settings dialog box appears.

**Step 2** Click the **BW Management** tab.

The BW Management tab opens.



**Step 3** Select one of the **BW Prioritization Mode** radio buttons.

- **Global Prioritization Mode**
- **Subscriber Prioritization Mode**

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

The System Settings 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).

A service configuration can contain up to 1024 upstream global controllers and 1024 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.

**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.)

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 “Managing Virtual Links” 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** From the Console main menu, choose **Configuration > Global Bandwidth Settings**.

The Global Bandwidth Settings dialog box appears.

**Step 2** 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 3** Click **OK**.

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** From the Console main menu, choose **Configuration > Global Bandwidth Settings**.

The Global Bandwidth Settings dialog box appears.

**Global Bandwidth Settings**

Use global bandwidth settings to enforce a rate cap on traffic of the same type. Create **Global Controller (GC)** and set the maximum rate of the upstream and/or downstream direction. Rate is set as percentage relative to the rate limit of the physical link. Traffic is mapped to GCs by configuring Subscriber Bandwidth Controllers (BWCs).

☒ Enable Virtual Links Mode

Global Controllers Virtual Links Global Controllers

In **Virtual Links mode**, the physical link is divided into as a set of smaller "virtual" links, which are separately monitored and controlled. Each Virtual Link has its own set of GCs, which are modeled after the Virtual Link **Template GCs**.

Total Link Upstream L1 Bandwidth (% of physical link limit)

Total Link Downstream L1 Bandwidth (% of physical link limit)

In a dual link system, each GC has a counterpart GC on the other link. In virtual link mode, the configured rate limit is enforced on the aggregated rate of this pair of GCs.

The **Template GC** column values are copied to GCs of newly-created Virtual Link.  
The **Default GC** column values are set to the GCs of the Default Virtual Link(Virtual Link 0).

**Upstream**

Name	Template Virtual Link GC BW (%)	Default Virtual Link GC BW (%)
Upstream Total Link Limit		
.....Default Global Controller	100	100

**Downstream**

Name	Template Virtual Link GC BW (%)	Default Virtual Link GC BW (%)
Downstream Total Link Limit		
.....Default Global Controller	100	100

210816

The maximum percentage of the total physical link bandwidth that can be used by any global controller is displayed at the top of the Virtual Links Global Controllers tab:

- **Total Link Upstream L1 bw (% of physical link limit)**
- **Total Link Downstream L1 bw (% of physical link limit)**

The percentage values of the global controllers defined in the rest of the dialog box depend on the values displayed here. So, for example, if the Total Link Upstream L1 bw (%) has a value of 80 and the upstream default global controller has a value of 100, this is 100% of 80% of the physical link bandwidth.

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

- **Name** —A unique name assigned to the global controller. The system automatically assigns the names Controller 1, Controller 2, and so on.
- **Template Virtual Link GC BW (%)** —The default maximum percentage of the total link limit permitted to global controllers of any created virtual links.
- **Default Virtual Link GC BW (%)** —The maximum percentage of the total link limit permitted to global controllers of the default virtual link.

For an explanation of the values in these columns, see [How to View Global Controller Settings](#), page 9-30.

- Step 2** To view the actual maximum bandwidth values, place the cursor over the Link 1 BW (%) cell. A tooltip appears, showing the actual maximum bandwidth permitted to this global controller, in Mbps. This figure is calculated automatically by the system based on the possible SCE platform types (Gigabit Ethernet or Fast Ethernet), the controller maximum bandwidth percentage, and the total link bandwidth percentage.
- 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 9-32](#)
- [How to Set the Maximum Bandwidth of Global Controllers, page 9-32](#)
- [How to Delete Global Controllers, page 9-34](#)
- [Managing Subscriber Bandwidth, page 9-35](#)

## 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 a dual-link system, bandwidth limitations are applied to the sum of the two links.

- 
- Step 1** From the Console main menu, choose **Configuration > Global Bandwidth Settings**.  
The Global Bandwidth Settings dialog box appears.
- Step 2** Enter the maximum percentage of the physical link capacity that the link will carry in the **Total Link Upstream L1 bw (% of physical link limit)** field or the **Total Link Downstream L1 bw (% of physical link limit)** field.  
The values displayed in the tooltips of all the cells in the Link 1 BW (%) cells change to reflect the new total link limit.
- Step 3** Click **OK**.  
Your changes are saved.  
The Global Bandwidth Settings dialog box closes.
-

## 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 Service Control Engine \(SCE\) 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 9-49.

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

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

This command is a line interface configuration command. To run this command see [How to Enter Line Interface Configuration Mode](#), page 9-49.

- 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



**Table 9-1 Virtual Links CLI Commands (continued)**

Command	Description
show interface LineCard 0 virtual-links all	Show information about all virtual links
show interface LineCard 0 virtual-links 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 Quotas

- [How to Edit Quota Management Settings for Packages, page 9-49](#)
- [How to Select Quota Buckets for Rules, page 9-51](#)
- [How to Edit Breach-Handling Parameters for a Rule, page 9-52](#)

## 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 9-51](#)).

### 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 10-39](#)). 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.

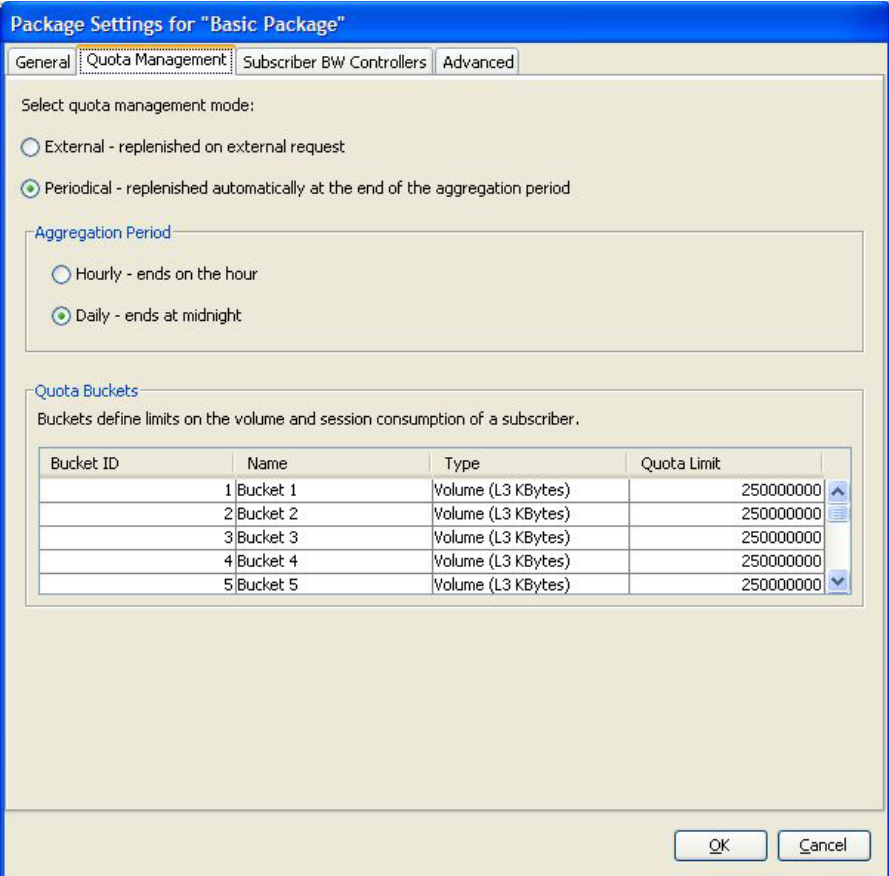
The quota replenish scatter function is independent of all other quota management parameters.

**Step 1** In the Network Traffic 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.



**Package Settings for "Basic Package"**

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

Select quota management mode:

☐ External - replenished on external request

☒ Periodical - replenished automatically at the end of the aggregation period

Aggregation Period:

☐ Hourly - ends on the hour

☒ Daily - ends at midnight

Quota Buckets

Buckets define limits on the volume and session consumption of a subscriber.

Bucket ID	Name	Type	Quota Limit
1	Bucket 1	Volume (L3 KBytes)	250000000
2	Bucket 2	Volume (L3 KBytes)	250000000
3	Bucket 3	Volume (L3 KBytes)	250000000
4	Bucket 4	Volume (L3 KBytes)	250000000
5	Bucket 5	Volume (L3 KBytes)	250000000

OK Cancel

**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 9-49.)

- 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 9-49). If no quota bucket is appropriate for the rule, add a new quota bucket to the package or edit an existing bucket.

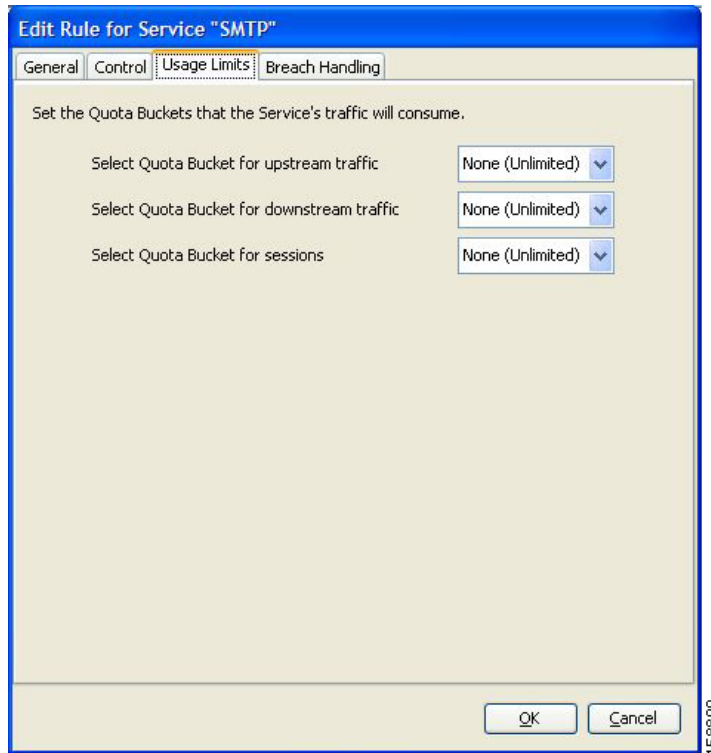
- Step 1** In the Network Traffic tab, select a package from the package tree.

- 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.



- 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 8-6](#)).
  - 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 10-37](#).) 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 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 10-27](#).

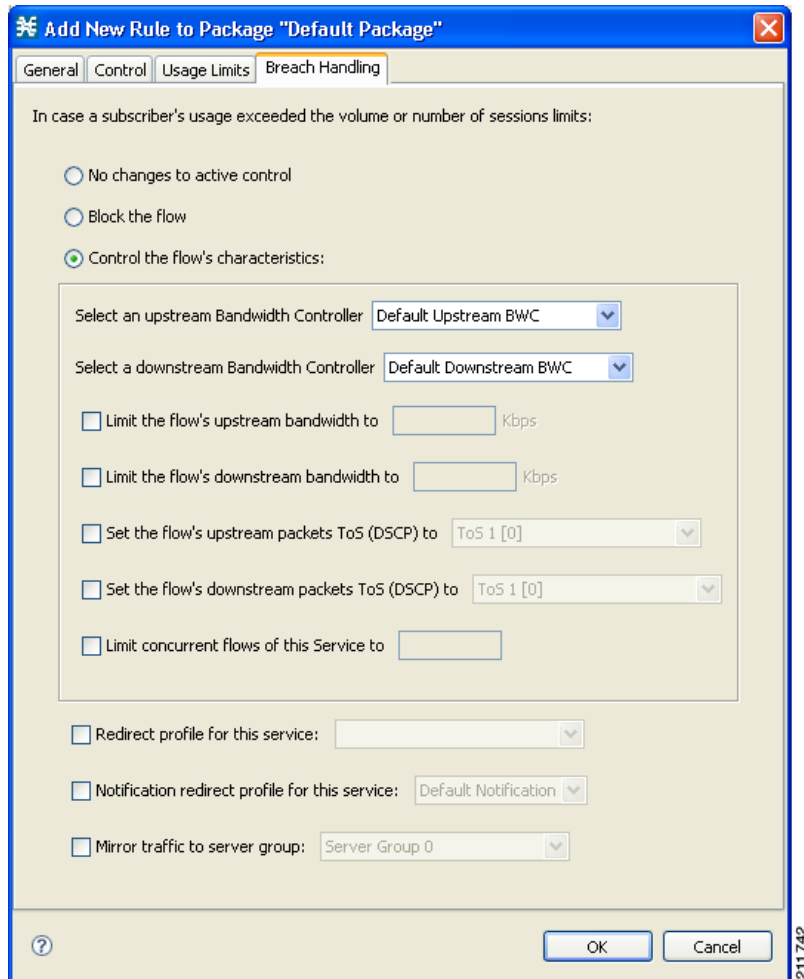
**Step 1** In the Network Traffic tab, select a package from the package tree.

**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 Breach Handling tab.  
The Breach Handling tab opens.



The screenshot shows the 'Add New Rule to Package "Default Package"' dialog box with the 'Breach Handling' tab selected. The dialog has four tabs: General, Control, Usage Limits, and Breach Handling. The 'Breach Handling' tab contains the following options:

- ☐ No changes to active control
- ☐ Block the flow
- ☒ Control the flow's characteristics:
  - Select an upstream Bandwidth Controller: Default Upstream BWC
  - Select a downstream Bandwidth Controller: Default Downstream BWC
  - ☐ Limit the flow's upstream bandwidth to [ ] Kbps
  - ☐ Limit the flow's downstream bandwidth to [ ] Kbps
  - ☐ Set the flow's upstream packets ToS (DSCP) to ToS 1 [0]
  - ☐ Set the flow's downstream packets ToS (DSCP) to ToS 1 [0]
  - ☐ Limit concurrent flows of this Service to [ ]
- ☐ Redirect profile for this service: [ ]
- ☐ Notification redirect profile for this service: Default Notification
- ☐ Mirror traffic to server group: Server Group 0

At the bottom of the dialog are 'OK' and 'Cancel' buttons, and a help icon (?) is located in the bottom left corner.

- Step 5** Set the flow's behavior when quota is breached.
- To block the flow when quota is breached, continue at Step 7.
  - To change the flow's characteristics when quota is breached, continue at Step 9.
  - To leave the flow unchanged when quota is breached, select the **No changes to active control** radio button.
- Step 6** Continue at Step 10.
- Step 7** Block flows that are mapped to the service of this rule.
- Select the **Block the flow** radio button.  
The Redirect to check box is enabled.
  - (Optional) To redirect blocked flows (for HTTP, HTTP Streaming, and RTSP), check the **Redirect to** check box.

**Note**

Redirection is not supported when unidirectional classification is enabled. If you try to check the Redirect to check box when unidirectional classification is enabled, a Rule Error message appears.

Click **OK** to continue.

The Redirection URL Set drop-down list is enabled.

**Note**

If the service or service group for this rule includes protocols that cannot be redirected, a Rule Warning message appears.

Click **OK**, and continue at Step 10.

- c. Select a redirection URL set from the Redirect drop-down list.

**Step 8** Continue at Step 10.

**Step 9** 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 (see [How to Edit Package Subscriber BWCs, page 9-37](#)).  
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.

**Step 10** (Optional) Activate subscriber notification.

**Note**

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

- Check the **Activate a Subscriber Notification** check box and then select the desired subscriber notification from the drop-down list.

**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.

Click **OK** to continue.

**Step 11** Click **OK**.

The Edit Rule for Service dialog box closes.

All changes to the rule are saved.