



## **CISCO SERVICE CONTROL SOLUTION GUIDE**



### **Cisco Service Control Policy Integration Solution Guide, Release 4.0.x**

- 1** [Solution Overview](#)
- 2** [Service Creation Integration Model](#)
- 3** [Service Creation Integration: Examples](#)
  - [Obtaining Documentation and Submitting a Service Request](#)



---

**Note** This document supports all 4.0.x releases.

---

# 1 Solution Overview

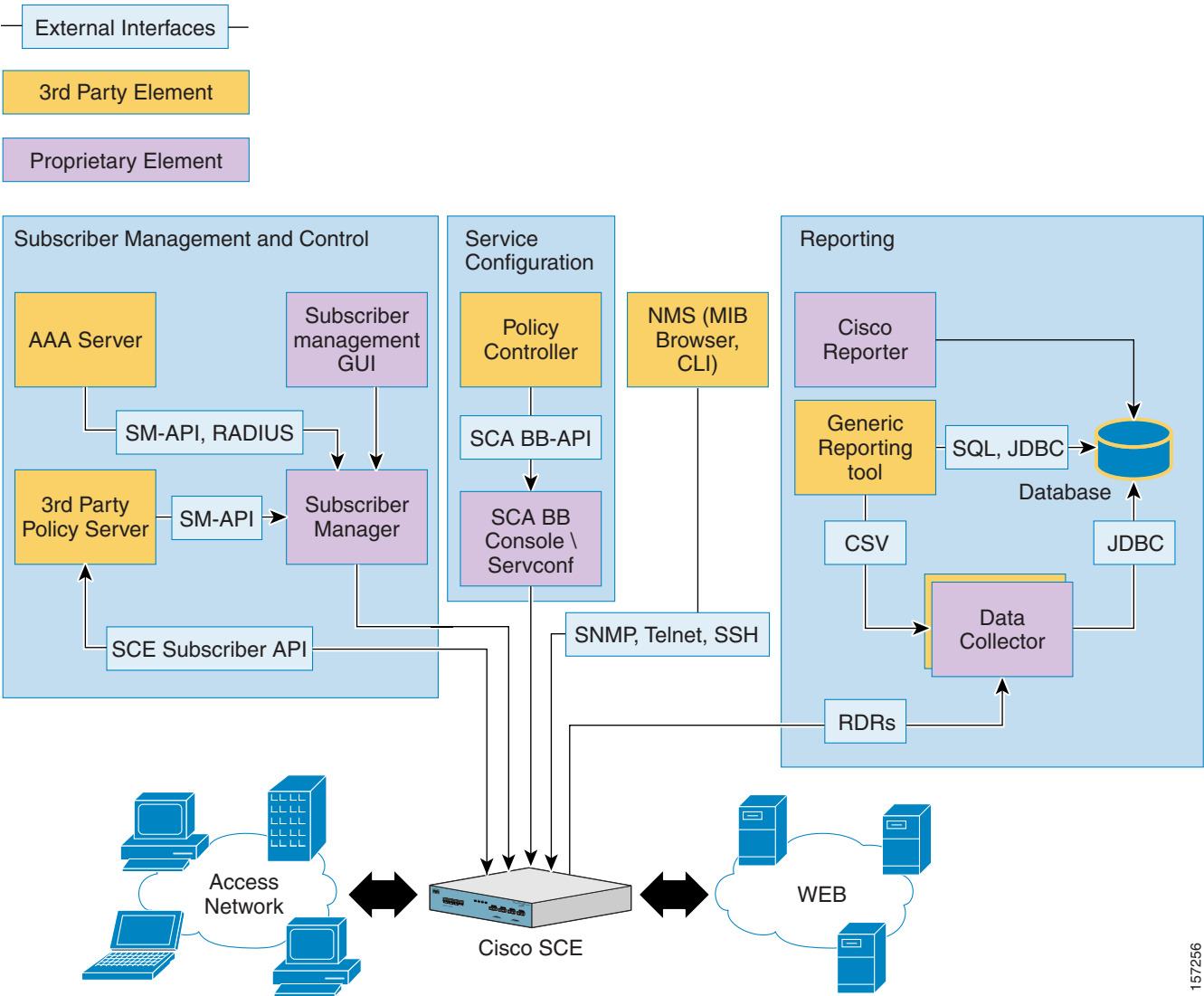
This chapter describes the logical components that make up the Cisco Service Control Application for Broadband (Cisco SCA BB) solution. The Cisco SCA BB solution can serve as a platform for service creation for a service provider.

This chapter contains these sections:

- [Cisco SCE Platform, page 4](#)
- [Policy and Service Configuration, page 5](#)
- [Real-Time Subscriber Management and Control, page 5](#)
- [Reports, page 6](#)

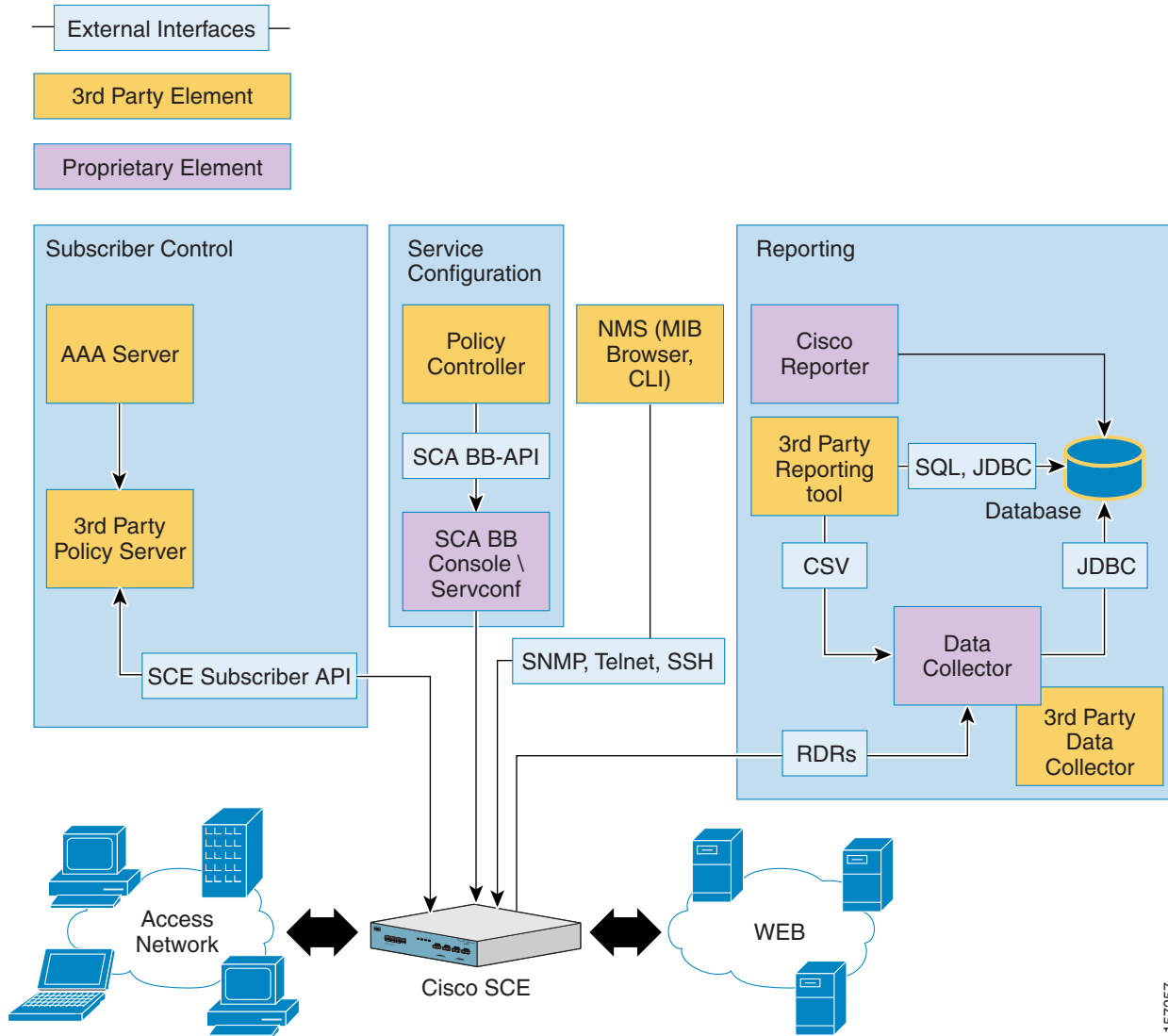
[Figure 1](#) and [Figure 2](#) illustrate the high-level architecture of the Cisco SCA BB solution when integrated in a typical service provider environment. These figures show the major components and the relationship between each component. [Figure 1](#) shows the Cisco SCA BB solution including the Subscriber Manager component. [Figure 2](#) diagram shows direct integration with the Cisco Service Control Engine (Cisco SCE) platform (also known as SM-less integration). In this case, the Cisco Service Control Subscriber Manager component is not included and the third-party Policy Server communicates directly with the Cisco SCE platform.

Figure 1 Cisco SCA BB Solution System Including Subscriber Manager



157256

**Figure 2 Cisco SCA BB Solution System—Without Subscriber Manager Integration**



157257

## Cisco SCE Platform

The Cisco SCE platform is a hardware-accelerated, deep packet inspection (DPI) device that forms the core of the solution. In a service-creation scenario, the Cisco SCE platform is deployed inline on the subscriber IP data path. Cisco SCE provides DPI, and application and protocol recognition along with the enforcement of the relevant policies, per subscriber, according to the customer business logic.

The device is configured and monitored through Network Management System (NMS)—over CLI, SNMP—and a number of proprietary tools used for service configuration, subscriber management, and multi-unit configuration. All the tools are combined in the Cisco SCA BB Console application. The platform is subscriber aware and can be used for usage-based services, for example, subscriber-level quota management and billing. For details on subscriber awareness, see the [“Real-Time Subscriber Management and Control”](#) section on page 5. The platform also generates network usage data at various granularities for monitoring and analysis purposes.

For details on the Cisco SCE platform and its various configuration interfaces, see the [Cisco SCE 2000 Installation and Configuration Guide](#) and the [Cisco SCE 2000 QuickStart Guide](#).

## Policy and Service Configuration

Policy and service configuration refers to the static system configuration that defines the way traffic is analyzed and controlled globally, in addition to the various policies available for controlling specific subscriber traffic.

A policy definition is a prerequisite for any deployment, and provides the context for the definition of the other aspects of the solution.

Policy and service configuration is created by using the Cisco SCA BB Console or using the Cisco SCA BB Service Configuration API. The service configuration is compiled into a proprietary file format called PQB. A PQB can be applied to the Cisco SCE platform through the Cisco SCA BB Console or through the `servconf` command line utility.



---

**Note** For policy enforcement, apply the policy and service configuration before subscriber traffic starts coming through the Cisco SCE.

---

For details on the service configuration, see these guides:

- [Cisco Service Control Application for Broadband User Guide](#)
- [Cisco SCA BB Service Configuration API Programmer Guide](#)

## Real-Time Subscriber Management and Control

Subscriber management is required to be real time for a subscriber-aware solution in a dynamic IP or dynamic policy environment. This aspect of the solution provides the capabilities related to:

- Mapping network IP addresses, or other network identifiers, to managed subscriber entities
- Real-time control of the policy applied to a subscriber
- Application of usage-quota restrictions
- Using other aspects of dynamic policy management such as self-care portals, turbo-buttons, and so on.

The Cisco Service Control Subscriber Manager component provides most of this subscriber-related functionality and APIs.

The Cisco SCA BB solution also facilitates subscriber management by using direct integration with the Cisco SCE platform. In many cases, this direct integration is beneficial to service providers who may better utilize existing applications. For example, when the provider has already invested in a complete Policy Server or similar system. The service provider may also decrease the number of deployed and managed network elements by eliminating the Cisco Service Control Subscriber Manager component and therefore optimizing overall operational expenses.

Direct integration generally simplifies the deployment; however, the application that communicates to the Cisco SCE platform must implement some functionality that Cisco Service Control Subscriber Manager provided earlier. These include support for multiple Cisco SCE units, addressing high-availability issues by supporting redundancy schemes, and various cases of fail-over.

Subscriber management integration can be implemented using two integration modes—Push and Pull. These modes utilize different sequences of events for subscriber logins. In Push mode, the external entity such as the Policy Server triggers a subscriber creation or update, and provisions the information to the Cisco SCE before the subscriber starts sending data traffic. In Pull mode, the Cisco SCE identifies subscribers upon receiving data traffic belonging to an unknown (anonymous) source. It then queries the Policy Server by sending a request to provide the subscriber identity and thus triggering the login operation. The Policy Server provisions the required subscriber information back to the Cisco SCE.



---

**Note** Subscriber management and quota provisioning may be implemented by two separate applications. In this case, the Cisco SCE must be integrated with both the applications.

---

For details, see these guides:

- [Cisco Service Control Management Suite Subscriber Manager User Guide](#)
- [Cisco SCMS Subscriber Manager Java API Programmer Guide](#)
- [Cisco SCMS Subscriber Manager C/C++ API Programmer Guide](#)
- [Cisco SCMS SCE Subscriber API Programmer Guide](#).

## Reports

The Cisco SCA BB reporting solution includes the generation, collection, and aggregation of network usage as analyzed by the Cisco SCE devices. The data is available in several granularities. The data is also tailored for use in several scenarios such as network analysis and trend determination, postpaid billing, and offline auditing.

Cisco SCA BB enables the collection of Raw Data Records (RDRs) through its Collection Manager software. RDRs can be stored in a Java Database Connectivity (JDBC)-compliant database or written to file depending on their type and the instance addressed by the customer. Reporting tools (either proprietary or generic) can be used to present the collected information. The Cisco SCA BB solution includes a reporter application as part of the Cisco SCA BB Console.

Reporting is a major function in most implementations of the Cisco SCA BB solution. However, it is not directly related to Service Creation, and hence it is not discussed here.

For more details on reporting, see the [Cisco SCMS Collection Manager User Guide](#).

## 2 Service Creation Integration Model

This chapter contains these sections:

- [Service Configuration, page 6](#)
- [Real-Time Subscriber Provisioning and Monitoring, page 7](#)

In a Service Creation environment, the Cisco SCA BB would typically integrate with a Policy Server (PS) system, which would be a part of the Operations Support System (OSS) of the service provider. This system would manage subscriber policies in real time, provision usage quotas for a subscriber (as well as monitor subscriber usage), and handle billing for the solution.

The system can be either an internal system that is closed to the subscriber or an open system. The internal system has no subscriber-facing interfaces (assigning subscribers with their predefined service levels and quotas, as purchased offline). The open system allows subscribers to purchase and provision their own usage policies and quotas (based on the provider definitions) through a self-care portal.

The entire solution depends on the functionality and capabilities of the Policy Server, with the Cisco SCA BB solution providing the network enforcement and accounting platform within the solution.

To keep the solution synchronized with the dynamic network mappings of the subscribers, it is necessary to integrate the solution with the back-end systems, of the service provider, that are responsible for IP mapping (such as DHCP, AAA).

The main aspects of the solution that concern a Policy Server vendor or developer are:

- Service-configuration plane
- Real-time subscriber policy profile mapping
- Quota provisioning
- Monitoring plane

Subscriber IP mapping is also a requirement and in many cases the Policy Server is also responsible for subscriber IP mapping. However, it is not a mandatory functionality for the server, because, the mapping can be achieved by integrating the Policy Server with the back end system responsible for IP mapping (for example, DHCP server) rather than through the policy server itself. Subscriber IP mapping can also be achieved by intercepting data from RADIUS and DHCP traffic.

Reporting in the SCA BB solution is less relevant to the real-time-integration process. Reporting is relevant only if postpaid billing has to be provided through RDR-based interfaces.

For more details on integration over the reporting plane, see these guides:

- [Cisco SCMS Collection Manager User Guide](#) (for integration by using the Cisco Collection Manager software)
- [Cisco Service Control Application for Broadband Reference Guide](#) (for direct integration by using RDRs).

## Service Configuration

The service configuration is static and defines the various policy profiles available as plans, products, or packages for the subscribers of a service provider. Defining the business logic, according to the policy definitions created by the service provider, allows the provider to assign a predefined policy to subscribers according to their subscription type. A policy profile defines:

- Per-service and overall quality of service (QoS) allocated to a subscriber
- Allowed and restricted (blocked) services that the subscription includes
- Structure of quotas on which the policy is based (that is, which services are consumed from which quota, which services are not accounted for usage, and so on) and the corresponding definitions to be applied when the usage of the subscribers exceeds their allowed quota.

For details on service configuration, see these guides:

- [Cisco Service Control Application for Broadband User Guide](#)
- [Cisco SCA BB Service Configuration API Programmer Guide](#)

## Real-Time Subscriber Provisioning and Monitoring

The Cisco SCA BB solution provides a number of APIs and interfaces that support real-time subscriber provisioning and monitoring.

- Cisco Service Control Subscriber Manager API (SM-API)—Used for updating, querying, and configuring the Cisco Service Control Subscriber Manager in deployments that include the SM component.
- Cisco SCE Subscriber API—Used for SM-less deployments and for quota management purposes.

### Cisco Service Control Subscriber Manager API (SM-API)

The SM-API is used for various subscriber management functions throughout the Cisco SCA BB solution in deployments that use SM rather than direct integration. In such deployments, Policy Server use the SM-API to define the policy to be applied to a subscriber. The policy profile (the package) ID identifies the policy, as defined in the service configuration. This API can be used in various instances, such as, static introduction of a subscriber, self provisioning, and turbo-button activation.

The SM-API is provided as a client API (both nonblocking and blocking implementations) and is available in Java and C/C++ (Windows, Sparc Solaris, and Red Hat Linux).

The SM-API is provided as a part of the Cisco Service Control Management Suite Subscriber Manager suite.

For more details on SM-API, see the [Cisco SCMS SM Java API Programmer's Guide](#) and the [Cisco SCMS SM C/C++ API Programmer's Guide](#).

### Cisco SCE Subscriber API

The Policy Server use the Cisco SCE Subscriber API for direct integration with the Cisco SCE without involving the Cisco Service Control Subscriber Manager component. The API supports various functions such as:

- Network ID association—An association between a unique subscriber identifier, subscriber network identifier, and policy profile or package assigned to the subscriber
- Policy provisioning—An association between a unique subscriber identifier and a policy profile or package assigned to the subscriber
- Quota provisioning—An association between a unique subscriber identifier and a quota amount that is available for service consumption

### Network ID Association

The subscriber mapping API functionality includes the login operation to:

- Create the subscriber.
- Modify the subscriber attributes, if the subscriber exists.

The Policy Server invokes this operation when the server has to provision the subscriber identity and other information to the Cisco SCE. For example, when the server receives a notification that a subscriber has logged in to the network, or when the server responds to a pull request.

The login operation includes a number of parameters, such as:

- Subscriber identifier (OSS ID)—Uniquely identifies the subscriber.
- Subscriber network ID—Can represent multiple instances of IP address, IP range, VLAN, and tunnel ID.

- (Optional) Policy profile identifier—Identifier of the policy profile assigned by the Policy Server and preconfigured during service configuration phase.
- (Optional) Initial service quota—Initial service quota, if available, for the subscriber.

The login operation can be reused to update (add or set) the subscriber network ID in these scenarios:

- When the subscriber network ID is modified (for example, when the DHCP server assigns a different IP address)
- When adding IP address instances for a subscriber with multiple IP addresses
- When modifying the subscriber policy after the subscriber is created

## Policy Provisioning

The policy profile can be assigned to a subscriber by using the login operation in these scenarios:

- During the initial creation of the subscriber.
- When the subscriber is upgraded or downgraded and requires the enforcement of a different policy.




---

**Note** The policy may be provisioned this way regardless of the integration mode, that is, push or pull.

---

## Quota Provisioning

The quota provisioning mechanism is based on the ability to assign a quota to a subscriber for consuming a specific service and to manage it later. The Cisco SCE Subscriber API supports quota provisioning events, such as:

- Quota setting and addition
- Notification that the quota falls below a configurable threshold
- Notification that the quota is depleted
- Notification of the value of the remaining quotas

The quota may be provisioned along with subscriber login (see the [“Network ID Association” section on page 7](#)). This can be used, for example, in cases where the Policy Server also supports quota provisioning. When the ecosystem of the network operator includes a separate quota provisioning system, the quota may be set after and independently on the login operation.

The quota is provisioned in small portions depending on the business logic of the service provider. When the current quota of a certain service or bucket in the Cisco SCE falls below a configured threshold (due to consumption of the service by the subscriber), or becomes depleted, the Cisco SCE sends a notification event to the Quota Provisioning system. This event is interpreted as a quota replenishment request from the subscriber. The Quota Provisioning system responds with a quota setting or adding operation.

The changes in quota reflecting consumption of the service by the subscriber is reported by using periodical or on-demand notifications of the value of the remaining quota. It may be used, for example, to show the subscriber the status of their quota through the portal. Subscribers can optionally be notified when they breach their quota.

The remaining quota is reported to the Quota Provisioning system upon subscriber logout. To improve the user experience of a subscriber accessing a service for the first time (with no quota in place), a grace period can be configured by using the Cisco SCA BB. During this grace period, the subscriber can be allowed to access the service until the initial quota provisioning stage is complete.

For details on quota provisioning, see the [Cisco Service Control Application for Broadband User Guide](#).

The Cisco SCE Subscriber API is currently implemented in Java.

For details on the Cisco SCE Subscriber API, see the [Cisco SCMS SCE Subscriber API Programmer Guide](#).



## 3 Service Creation Integration: Examples

This chapter contains examples of particular instances. The examples are basic, but illustrate the use of the various interfaces for implementing business logic primitives. The actual implementations might be more complex and use a larger mixture of the primitives described here.

This chapter contains these subsections:

- [Example I: Periodic Quota-Based Services, page 9](#)
- [Example II: Turbo Button with “Free Usage”, page 20](#)

### Example I: Periodic Quota-Based Services

#### Business Scenario

Traffic is divided into two services:

- General Internet Access—General broadband Internet access.
- Premium Content—Access to specific content sites that the broadband operator is marketing as “premium content.”

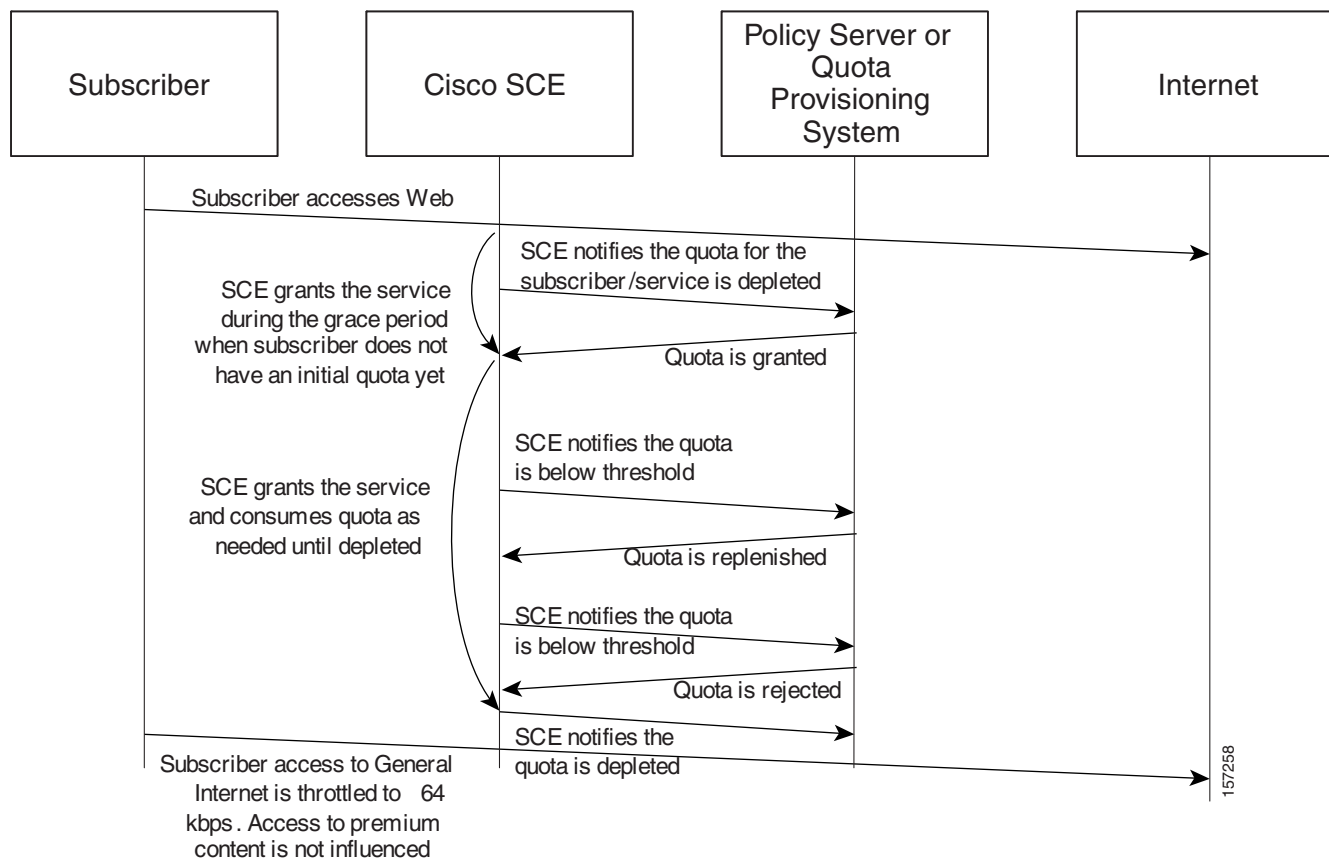
Subscribers have a monthly quota (not accumulated across months) for general Internet access. When the quota is depleted, the traffic rate is reduced to a dial-up rate of 64 kbps. Access to the Premium Content is not counted as part of the monthly quota and is not reduced to dial-up rates.

When the quota is depleted, the subscriber is notified by using the subscriber-notification event.

#### Overview

[Figure 3](#) shows an overview of the implementation of this business scenario. We recommend that you return to this section after reading the step-by-step description.

**Figure 3 Periodic Quota—Scenario Overview**



## Step-By-Step Implementation

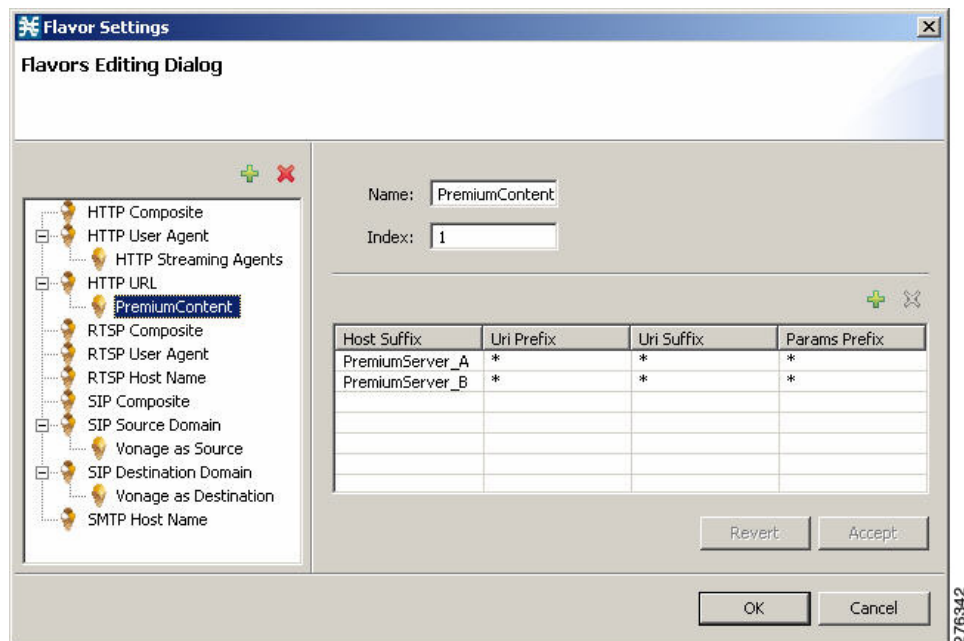
### Step I—Policy Configuration

#### Defining the Premium Content Service

To define the Premium Content service:

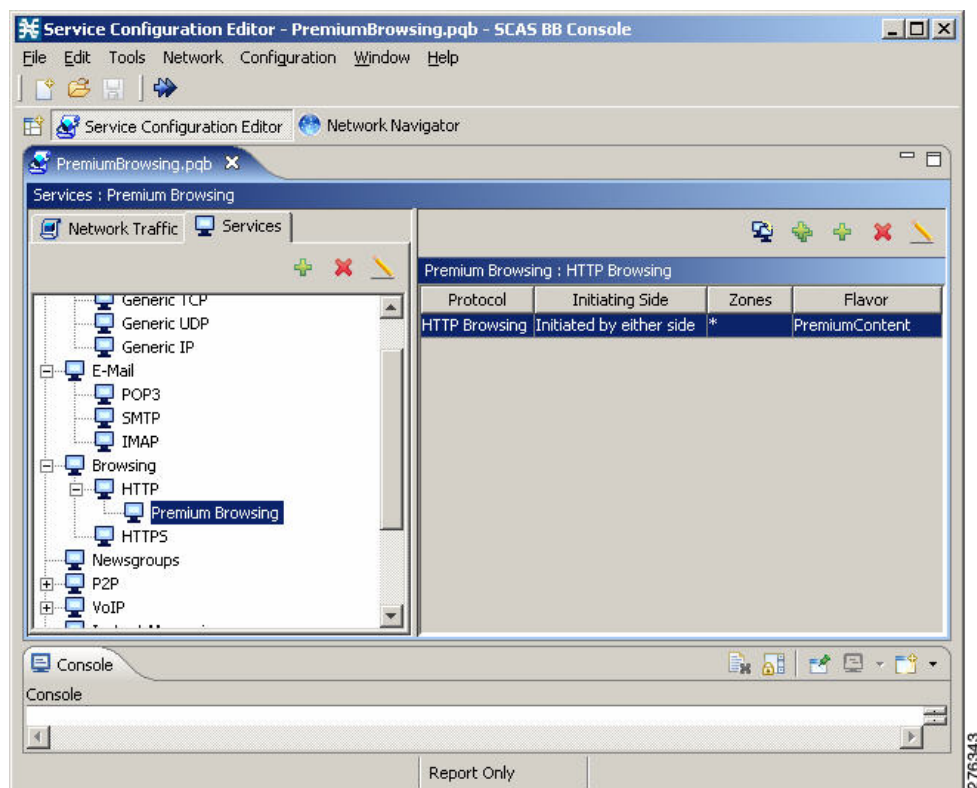
- Step 1** Define the list of servers for the Premium Content service by using the Flavors Settings window as shown in [Figure 4](#). For simplicity, this example assumes that the Premium Content service is defined based on a list of servers.

**Figure 4 Flavor Settings Window—Flavors Editing Dialog**



**Step 2** Modify the services of the Premium Browsing service such that it is based on the HTTP protocol together with the Premium Content flavor that contains the list of designated servers defined in Step 1 (Figure 5).

**Figure 5 Service Configuration Editor Window—Premium Browsing Service**



## Assigning Services to Quotas

The business logic used in this example specifies that the traffic for a subscriber is partitioned between General Internet Access and Premium Content. General Internet Access is quota controlled from one bucket (both upstream and downstream consuming from the same bucket). Premium Content traffic is not quota controlled (but rather post paid charged).

To assign services to quotas, complete these steps:

---

**Step 1** Add a new package to the Premium Browsing service called Free Premium Content as shown in [Figure 6](#).

**Figure 6** *Package Settings Window—General Tab*

Package Settings

General | Quota Management | Subscriber BW Controllers | Advanced

Package name:  
Free Premium Content

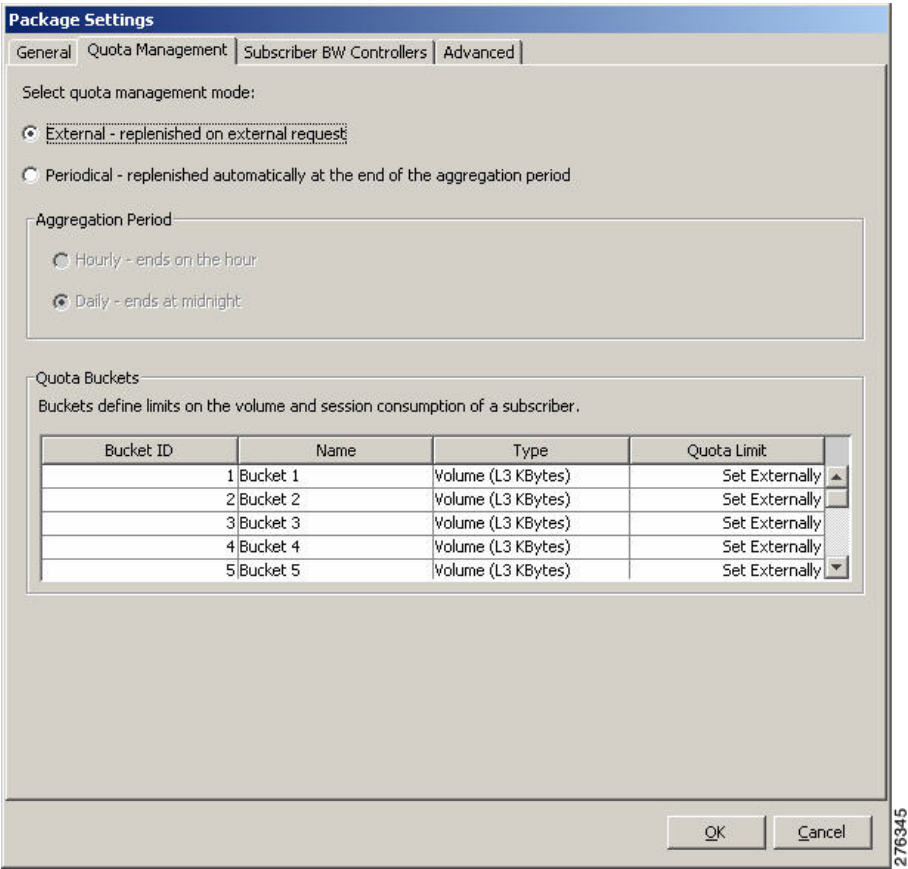
Description:

OK Cancel

276344

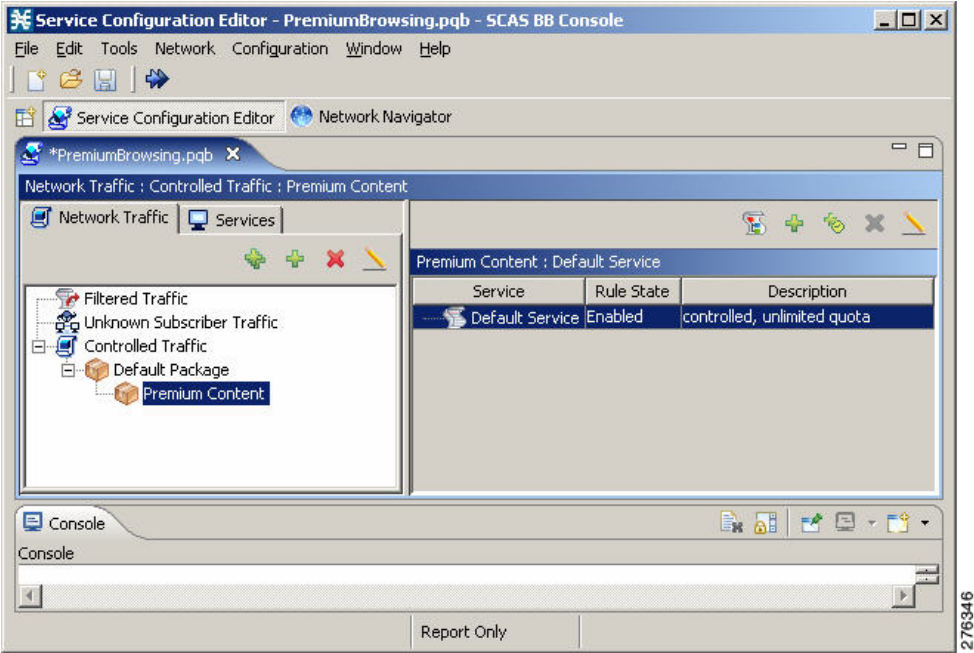
**Step 2** Set quota management to external control using the Quota Management tab as shown in [Figure 7](#).

**Figure 7**     *Package Settings Window—Quota Management Tab*



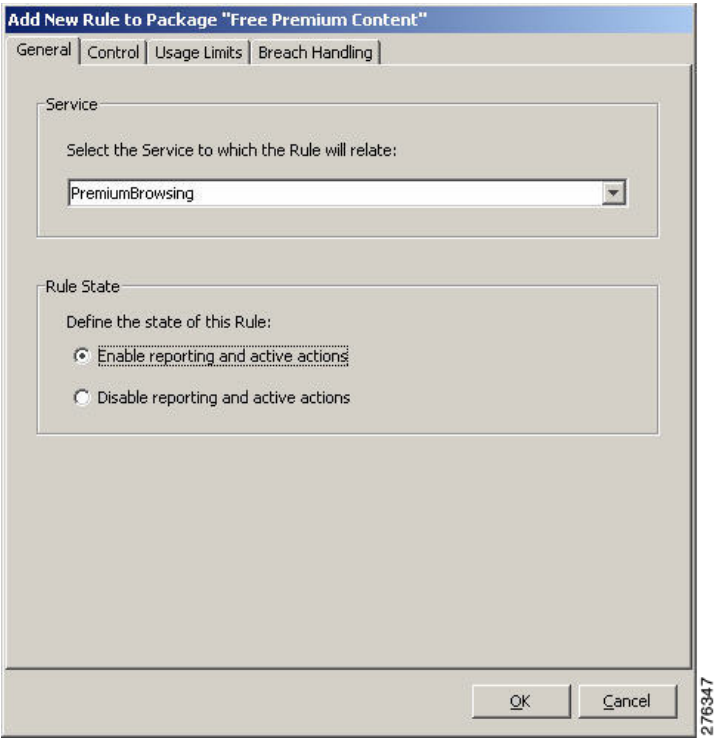
The package is created as shown in [Figure 8](#).

**Figure 8**     *Service Configuration Editor Window—Premium Browsing Service*



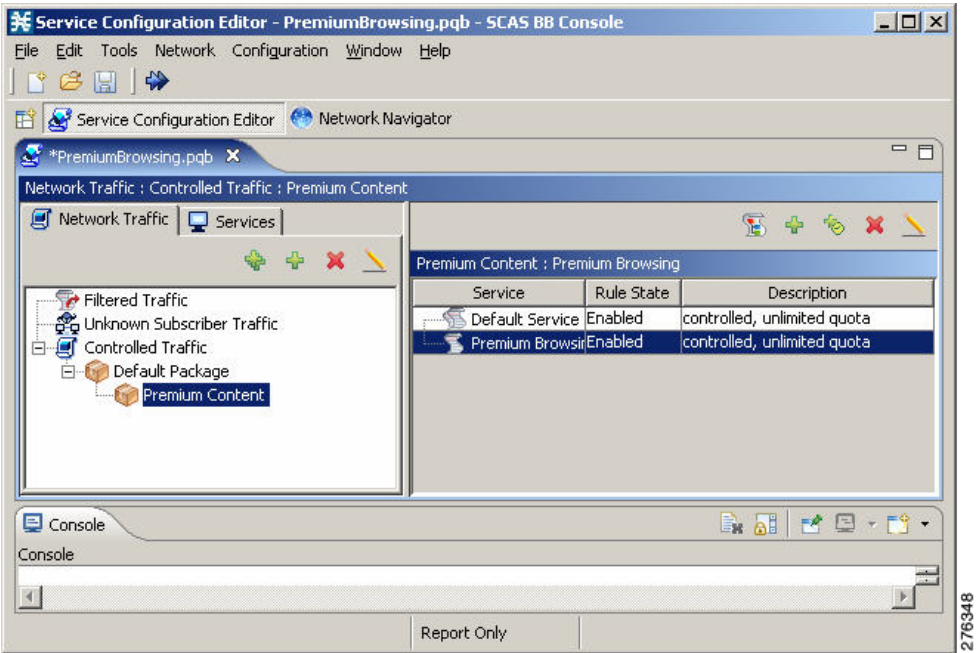
**Step 3**     Add a new rule to the Premium Browsing service as shown in [Figure 9](#).

**Figure 9     Add New Rule to Package—General Tab**



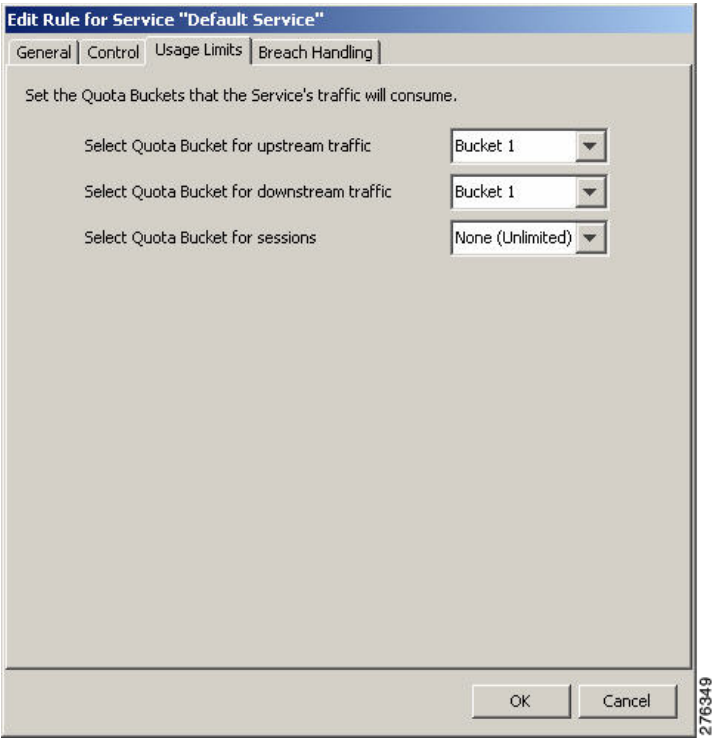
The Free Premium Content package now contains two service rules as shown in [Figure 10](#).

**Figure 10     Service Configuration Editor Window—Premium Browsing Service**



**Step 4** Define all other services, except Premium Browsing, as consuming quota from bucket number 1 for both upstream and downstream traffic. To define, use the Edit Rule for Service dialog box and the Usage Limits tab. Buckets can normally be used to manage upstream volume, downstream volume, and sessions. This example deals only with volume-based quota (see [Figure 11](#)).

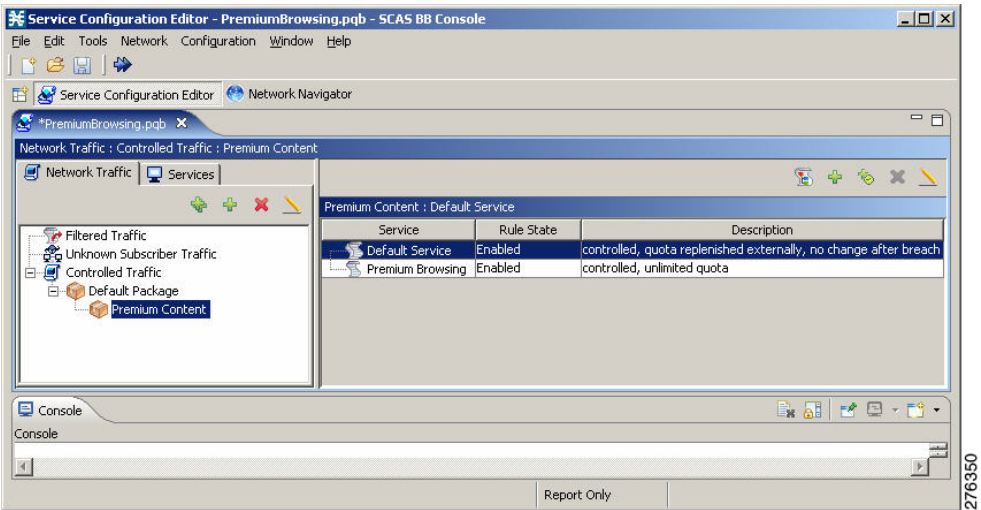
Figure 11 Edit Rule for Service Window—Usage Limits Tab



The Premium Browsing service is not associated with a quota bucket and therefore is not quota limited. But use of this service reflects in the quota-usage notifications using the Cisco SCE Subscriber API.

An overview of the monthly quota package is shown in [Figure 12](#).

Figure 12 Service Configuration Editor Window—Premium Browsing Service



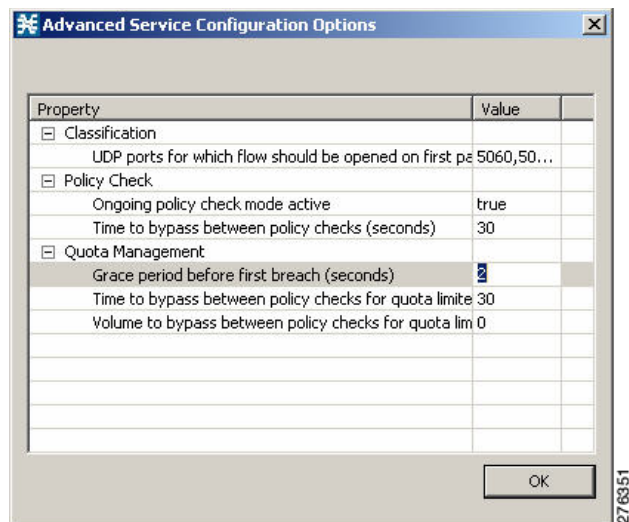
Defining a Grace Period

A grace period can be configured in SCA BB to improve the user experience for a subscriber accessing a service for the first time. The grace period allows the subscriber to access a service until the initial quota provisioning stage is complete. Configure a relatively short grace period. A short grace period allows subscribers to get services regardless of the allocated quota amount

even when the subscriber does not have available balance. The grace period reflects the willingness of the provider to credit the subscriber with service assuming that the balance is positive. This behavior is fully configurable and depends on the provider business logic.

To define a grace period, use the Advanced Service Configuration window (see [Figure 13](#)).

**Figure 13** *Advanced Service Configuration Options Window*



## Defining Quota-RDR Settings

Quota RDRs are the internal triggers for quota notifications that are part of the Cisco SCE Subscriber API. When using the quota functionality, ensure that all RDRs are enabled.

Set the period of the remaining quota RDRs based on the preferences of the operator.

The operator must determine the threshold value for RDR generation based on the size of the quota chunks provisioned and the expected bandwidth consumed by the service. Quota threshold notifications allow the policy server to provision a new quota chunk before an existing quota is depleted. Hence, these notifications enable service continuity while the subscriber has a positive account balance.

Configure the system to enable the RPC server, and to send RDRs to the internal RDR listener. These RDRs are converted into notifications by the Cisco SCE Subscriber API. Use this command to configure the system using the Cisco SCE CLI:

```
# RDR-formatter destination 127.0.0.1 port 33001 category number 4 priority 100
```

## Defining the Control Scheme

In this section, package bandwidth controllers are defined. The total bandwidth allocated to a subscriber is limited to 1 Mbps. “Depletion BWC”, designed for limiting the breached service traffic, is also defined (upstream and downstream).

To define a control scheme, define the package BW controllers and the Depletion BWC by using the Package Settings window ([Figure 14](#)).



**Figure 14** Package Settings Window—Subscriber BW Controllers Tab

Package Settings

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 (Kbps)	PIR (Kbps)	Global Controller	AL
[-] Primary Upstream BWC	0	Unlimited		
[-] Default Upstream BWC	0	1000	Default Global Controller	1
[-] Upstream Depletion	0	64	Default Global Controller	1

Downstream

Subscriber relative priority (downstream): 5

Name	CIR (Kbps)	PIR (Kbps)	Global Controller	AL
[-] Primary Downstream BWC	0	Unlimited		
[-] Default Downstream BWC	0	1000	Default Global Controller	1
[-] Downstream Depletion	0	64	Default Global Controller	1

OK Cancel

276352

By default, all services are placed under the total BW controller.

After the General Internet Access quota is depleted, this service will be mapped to a subscriber BW controller allowing it to consume up to 64 kbps. Notify the subscriber, through subscriber-notification, that their bandwidth has been reduced because of quota depletion.

### Defining Subscriber Notification

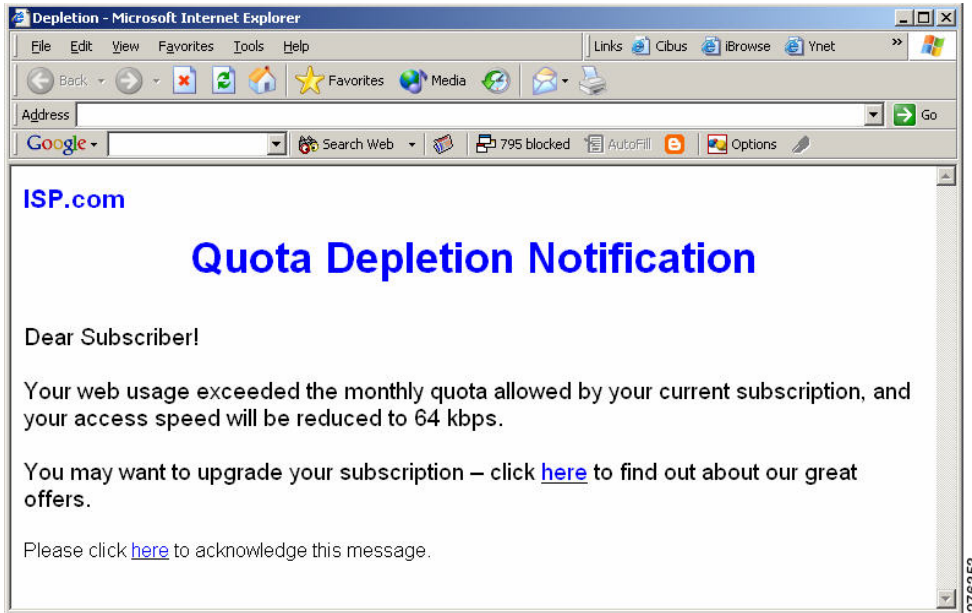
Using the subscriber-notification capability, subscribers can be put automatically into a state where their browsing session is redirected to a predefined web portal. The web portal page informs subscribers that their quota has depleted and therefore their internet access speed is reduced.

To define a subscriber notification, complete these steps:

---

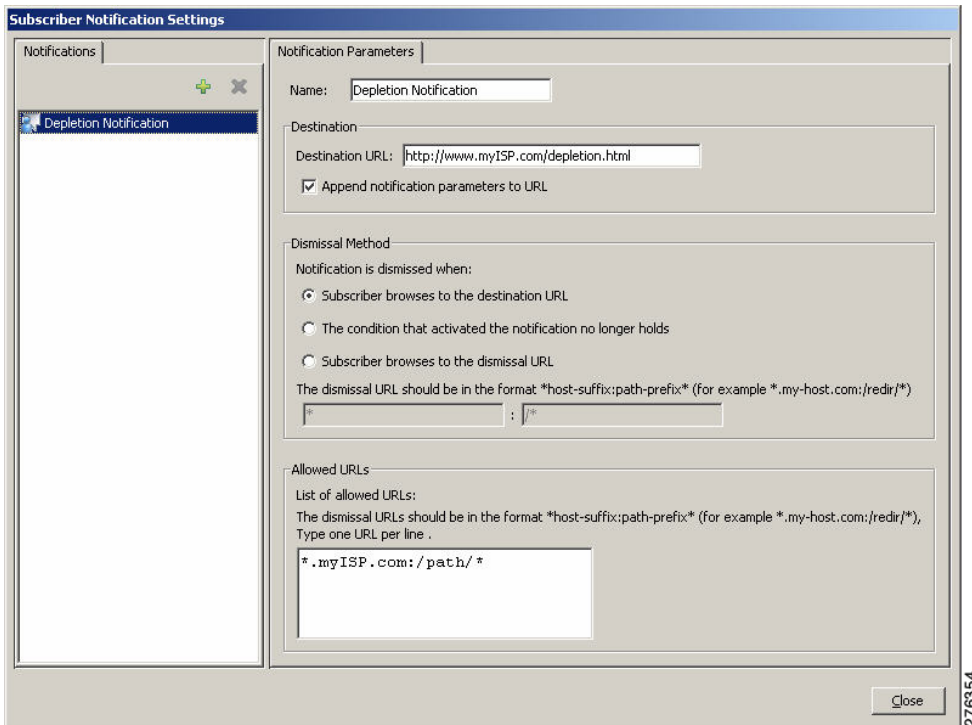
**Step 1** Design an appropriate web page as shown in [Figure 15](#).

**Figure 15 Depletion Window**



**Step 2** Define a subscriber notification by using the Subscriber Notifications Settings window (Figure 16).

**Figure 16 Subscriber Notification Settings Window**



The destination URL directs the subscriber to the web portal page created in Step 1.

**Step 3** Select the action to be taken upon breach (see Figure 17). This action maps all the services that consume bandwidth from the General Internet Traffic Quota (bucket 1) to the Depletion Bandwidth Controller.

**Step 4** Check Activate a Subscriber Notification to activate the subscriber notifications (see Figure 17)

**Figure 17** Edit Rule for Service Window—Breach Handling Tab

**Edit Rule for Service "Default Service"**

General | Control | Usage Limits | **Breach Handling**

In case a subscriber's usage exceeded the volume or number of sessions limits:

☐ No changes to active control

☐ Block the flow ☐ Redirect to: Default set

☒ Control the flow's characteristics:

Select an upstream Bandwidth Controller: Upstream Depletion

Select a downstream Bandwidth Controller: Downstream Depletion

☐ Limit the flow's upstream bandwidth to [ ] Kbps

☐ Limit the flow's downstream bandwidth to [ ] Kbps

☐ Limit concurrent flows of this Service to [ ]

☒ Activate a Subscriber Notification: Depletion Notification

OK Cancel

**Note** The method used here (using SCA BB breach-handling behavior) is useful for implementing a simplified quota breach behavior. For implementing more complex control logic, the Policy Server can use the quota depletion notification as a trigger for changing the subscriber package. This method allows the Policy Server a higher flexibility in the nature of control that is enforced over a subscriber upon quota depletion.

## Step II—Building the Real-Time Quota Provisioning Process

The real-time quota provisioning process for this business scenario is based on a subscriber balance manager that allocates subscriber quota upon request (through the Quota Below Threshold and the Quota Depleted notifications), based on quota availability.

To implement this business logic, the Policy Server uses the Cisco SCE Subscriber API to receive quota requests and to provision the quota accordingly by using the Quota Update method.

There are two main scenarios:

- A subscriber logs in with no quota—The Policy Server provisions the quota based on the balance with the subscriber received in response to an Cisco SCE-generated Quota Depleted event. If the Policy Server handles both subscriber mapping and quota provisioning, the quota may be provisioned along with the login operation.

The Cisco SCE Subscriber API events such as LOGINREQUEST and LOGINPULL-RESPONSE are optimized to allow sending all the subscriber information to the Cisco SCE. If a single Policy Server performs all parts of the subscriber provisioning including quota provisioning, use these events for Policy Profile and Quota Updates.

- Quota chunk allocated to a subscriber is about to run out—The Policy Server provisions quota based on the quota balance with the subscriber and in response to a Quota Below Threshold event generated by the Cisco SCE.

For details on using these operations, see the [Cisco SCMS SCE Subscriber API Programmer Guide](#).

## Step III—Acting Upon Depletion Events

Depletion events are signaled to the Policy Server through the Quota Depleted notification event. The Policy Server is required to receive such notifications to run some predefined logic. In this specific example, where the breach behavior is implemented inside Cisco SCA BB, the Policy Server is required only to log the event details.

### Handling Cases of Subscriber Logout

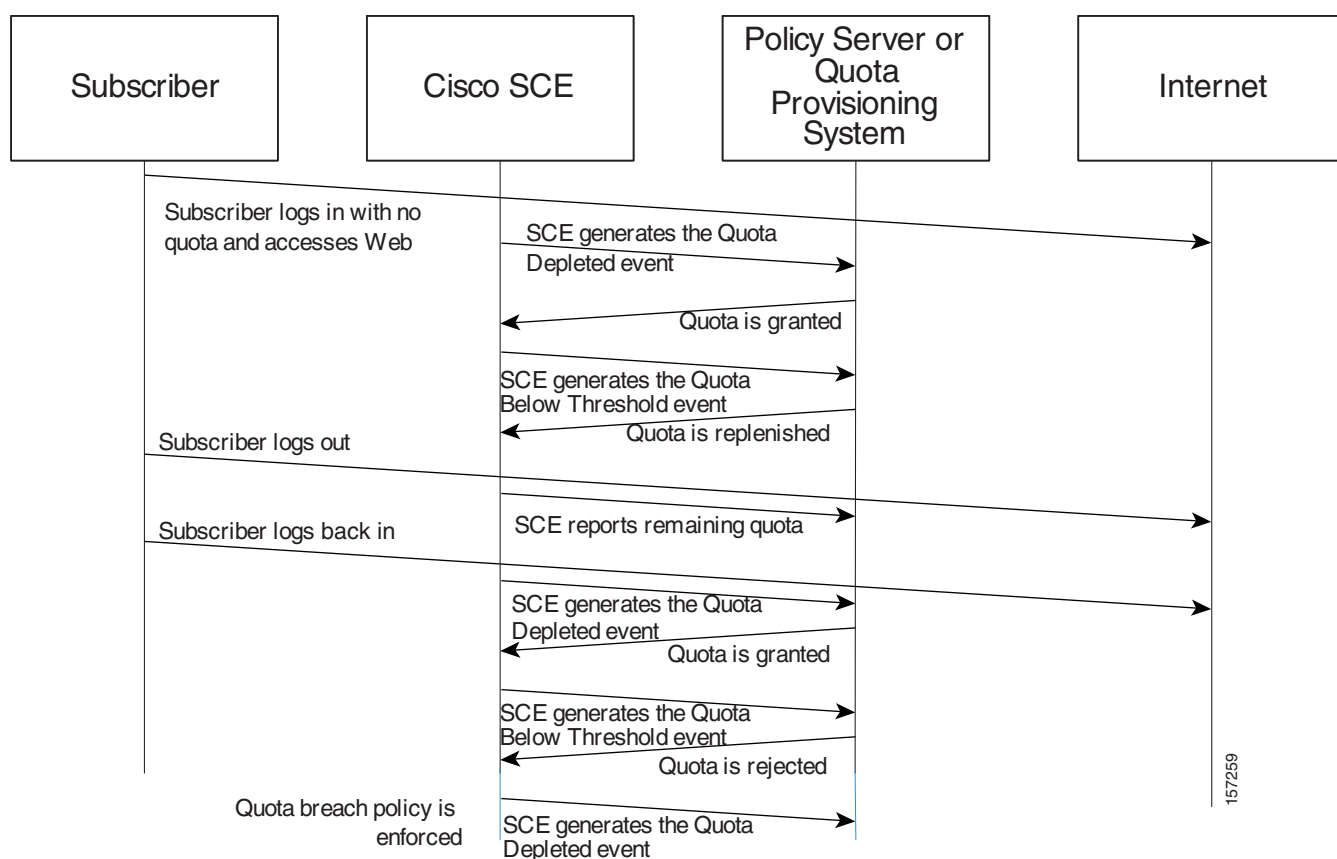
When subscribers log out of the network, either intentionally or implicitly (for example, because of session expiration), their records are removed from the Cisco SCE until they log back in.

In such a case, a notification is triggered. The notification includes the amount of quota left in the bucket of the specific subscriber. This notification allows the Policy Server to:

- Add the remaining quota back to the bucket of the specific subscriber; so that no quota is lost.
- Process the amount of used quota; so that no revenue is lost.

This sequence of events is shown in [Figure 18](#).

**Figure 18 Logout Handling Behavior Definition**



## Example II: Turbo Button with “Free Usage”

### Business Scenario

This business scenario is a simplified quota-based scenario. A subscriber is assigned a policy that allows for a certain access speed. Usage on all services is consumed from a single quota bucket.

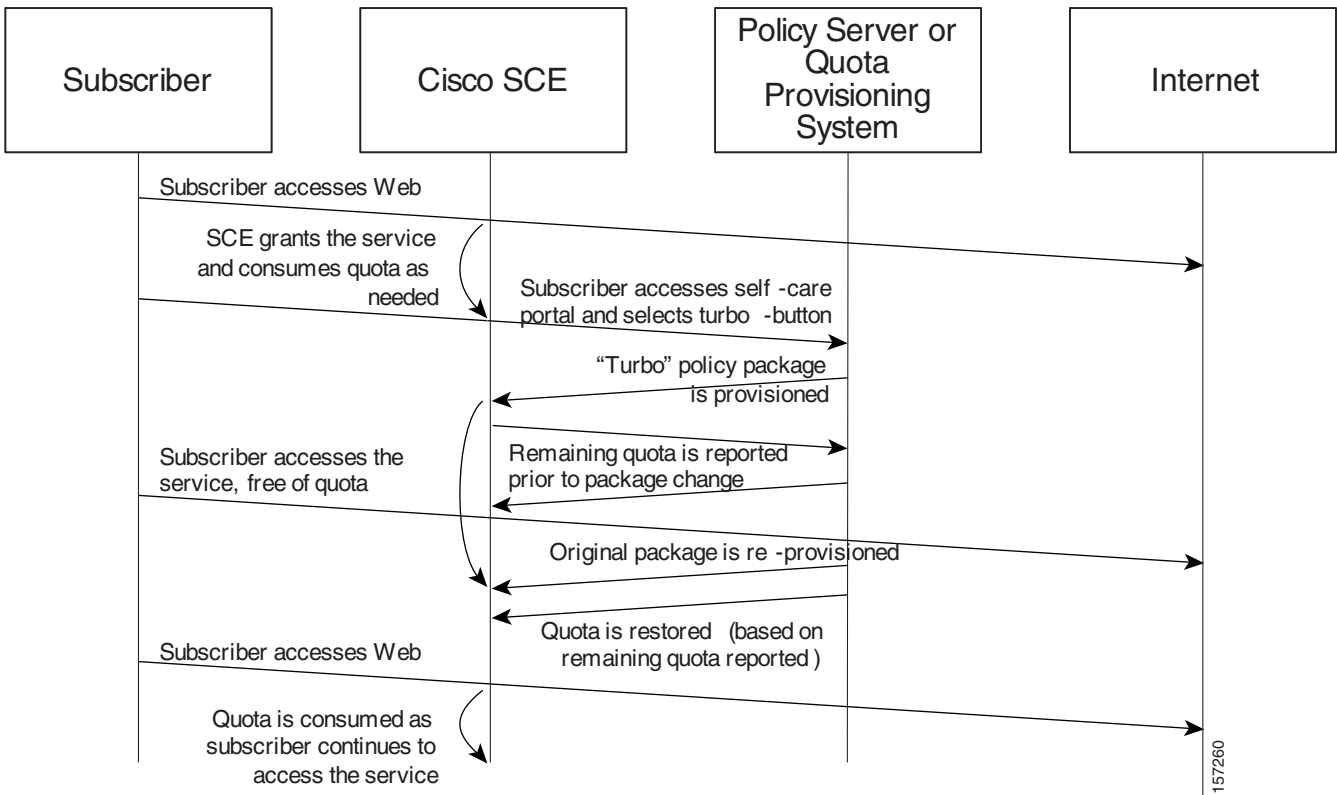
Subscribers can use a web interface to boost their access speed for a limited period using a “Turbo Button.”

During this period, subscribers are granted increased-speed, with quota-free access. When the time period is over, subscribers are reassigned their regular access plan and reassigned their remaining quota.

Overview

Figure 19 shows an overview of how this business scenario is implemented. We recommend that you return to this section after reading the step-by-step description.

Figure 19 Turbo Button Scenario Overview



This figure shows the sequence of events when direct integration is used. Policy provisioning can also be done through the Subscriber Manager API in Subscriber Manager deployments.

Step-By-Step Implementation

Step I—Policy Configuration

Defining the Quota-Based Package

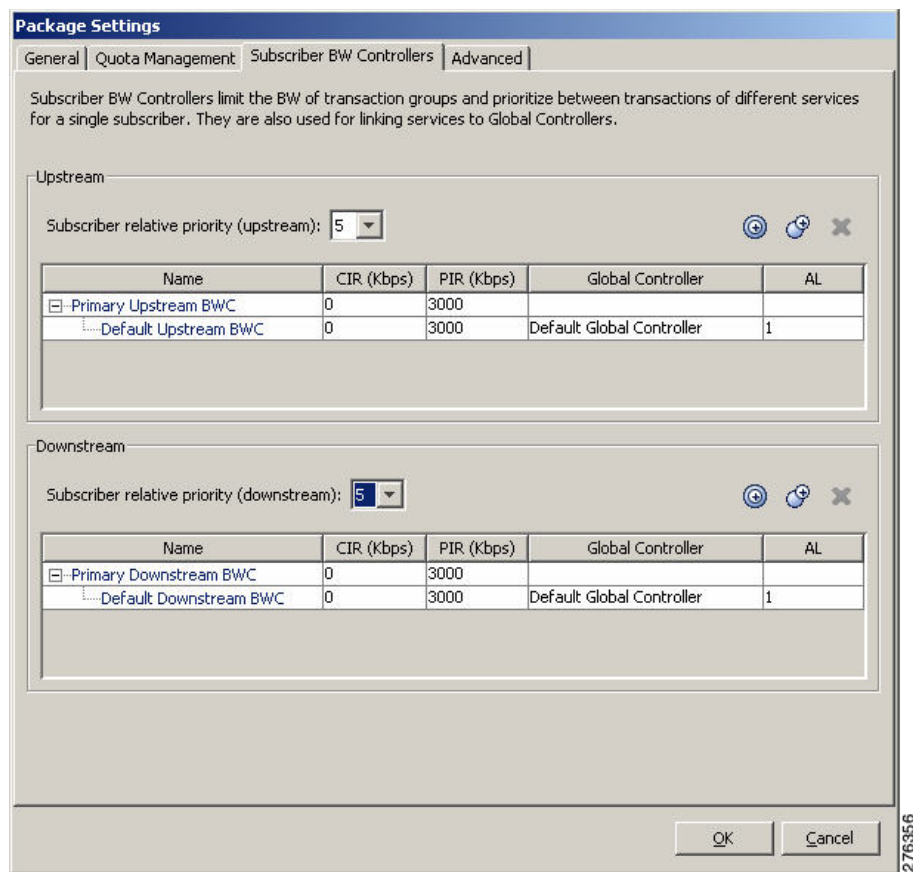
The quota-based package is built and managed in a similar manner to the previous example (“Example I: Periodic Quota-Based Services” section on page 9). See the Step II—Building the Real-Time Quota Provisioning Process, page 19 for details on how to build the quota-related portion of this policy.

Defining the “Turbo Button” Package

The “Turbo Button” package is provisioned to a subscriber after the subscriber select a “Turbo button”. This package boosts the total access speed of the subscriber and frees the subscriber from quota charging for a specific period. All the services of this package must be defined with “unlimited quota.” The Turbo Button package is deprovisioned when the “turbo” period is over.

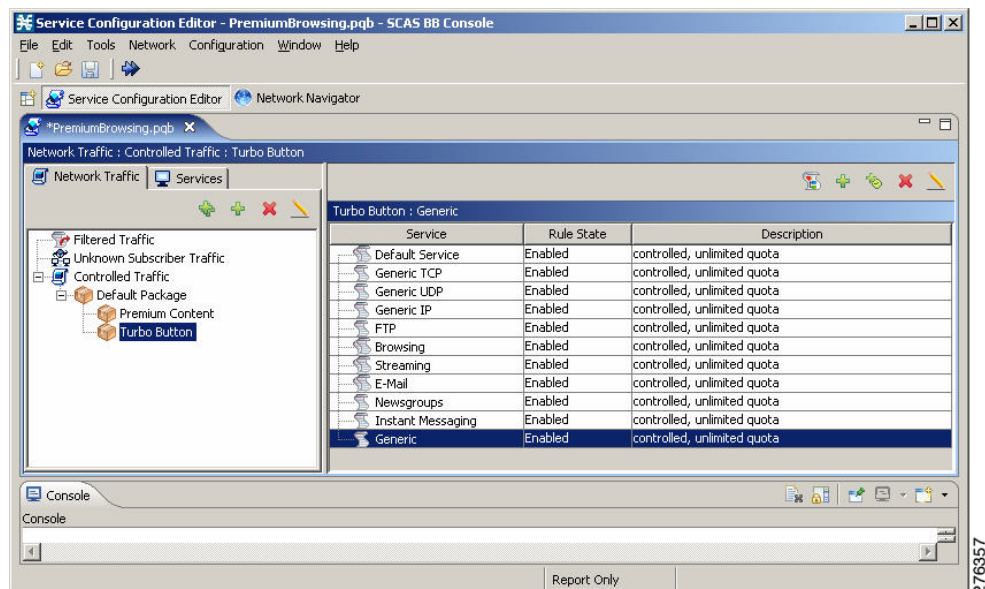
To define Turbo Button package, define the package bandwidth controllers (BWC) by using the Package Settings window (see Figure 20).

**Figure 20 Package Settings Window—Subscriber BW Controllers Tab**



The overview of the “Turbo” package is shown in Figure 21.

**Figure 21 Service Configuration Editor Window—Premium Browsing Service—Turbo**



## Step II—Real-Time Provisioning Process

This section refers to the logic that the Policy Server must implement—using the Cisco SCA BB Subscriber APIs, interfaces, and tools—to support the required business logic.

### Quota Provisioning

Quota provisioning in this example is identical to that of the previous example (“[Example I: Periodic Quota-Based Services](#)” section on page 9). However, upon a package change, the Cisco SCE generates a remaining-quota-notification, reflecting the remaining quota of the subscriber.



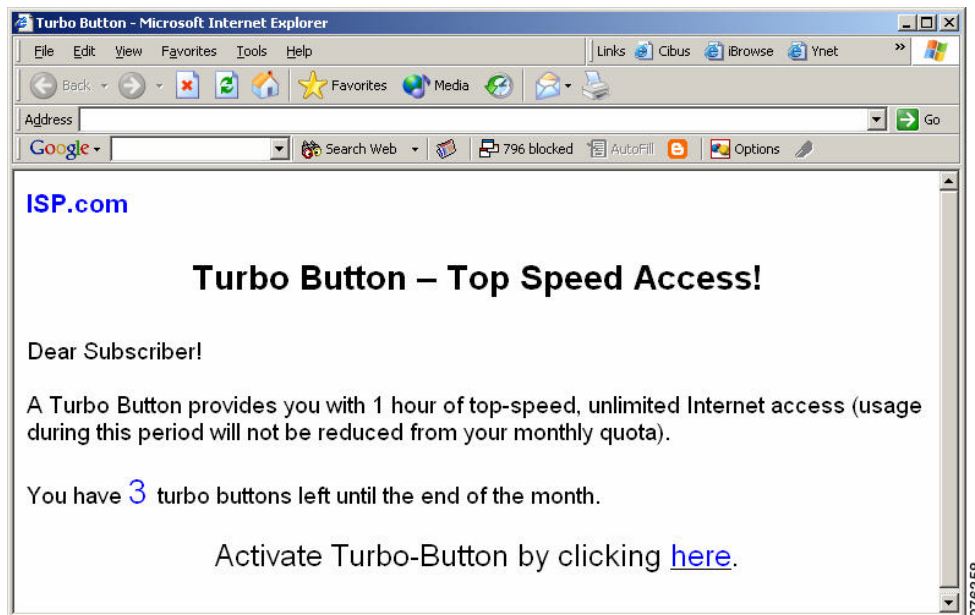
**Note** Upon package change, the balance with the subscriber does not change. When the “Turbo time” is over, the quota buckets are in the same state as they were before the “Turbo time.”

### Turbo Button Activation

The vendor must first build the front end for the activation of the Turbo Button. For this example, the front end is a web page, where subscribers can authenticate themselves and select to upgrade their access package temporarily by using a Turbo Button. To activate the Turbo Button, complete these steps:

**Step 1** Build the front end for subscriber activation as shown in [Figure 22](#).

**Figure 22** Turbo Button Front End



**Step 2** After the turbo button is selected, the Policy Server should provision the “Turbo Button” package for the subscriber to the SCA BB solution. This provisioning is done by using the Cisco SCE Subscriber API in the case of direct integration or using the SM API in other cases.

### Turbo Button Deactivation

The Policy Server is responsible for restoring the original package after the accelerated-speed, free usage period allowed by the turbo button is over.

**Step 1** The Policy Server restores the original package. This restoration is done by using the Cisco SCE Subscriber API in the case of direct integration or using the SM-API in other cases.



**Step 2** The Policy Server reprovisions quota when it is needed. During the Turbo Button active period, the quota is not changed; the subscriber has the same quota when the Turbo Button period ends. When the subscriber accesses the service after the Turbo period, the quota starts to be consumed as usual and may need to be replenished in the normal way. This is done by using the Cisco SCE Subscriber API (set primitive) triggered by the Quota Below Threshold or Quota Depleted notification.

---

For more details, see the [Cisco SCMS SCE Subscriber API Programmer Guide](#).

## Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at: <http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.

---

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2013 Cisco Systems, Inc. All rights reserved.



---

**Americas Headquarters**  
Cisco Systems, Inc.  
San Jose, CA

**Asia Pacific Headquarters**  
Cisco Systems (USA) Pte. Ltd.  
Singapore

**Europe Headquarters**  
Cisco Systems International BV Amsterdam,  
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

---