Using the Service Configuration Editor: Traffic Accounting and Reporting

Introduction

This chapter explains how to work with usage counters and Raw Data Records (RDRs).

Traffic Accounting and Reporting is the second step in creating a Cisco SCA BB service configuration. This chapter consists of these sections:

Usage Counters

The Cisco SCA BB collects and maintains various network metrics (such as volume and number of sessions) per service. This accounting takes place per subscriber, per group of subscribers (package or group of packages), and for the entire link.

Service Usage Counters

The system uses the service usage counters to generate data about the total use of each service. A service can use either its own usage counters, or the usage counters of its parent service. For example, in the default service configuration the SMTP and POP3 services share the E-Mail service usage counters. Service hierarchy determines the assignment of services to usage counters. For details on how to configure the service hierarchy, see "How to Edit Services" section on page 7-9.

Package Usage Counters

The Cisco SCA BB also collects and maintains various network metrics per package.

The system uses the package usage counters to generate data about the total use of each package. A package can use either its own usage counters, or the usage counters of its parent package. The package hierarchy determines the assignment of packages to usage counters. For details on how to configure the package hierarchy, see "How to Set Advanced Package Options" section on page 9-57.

Raw Data Records

Cisco Service Control Engine (Cisco SCE) platforms generate and transmit Raw Data Records (RDRs) that contain information relevant to the service provider. These RDRs contain a wide variety of information and statistics, depending on the configuration of the system.

- All RDR data is based on Layer 3 volume.

- RDRs are not generated for filtered traffic. For details, see "Filtering the Traffic Flows" section on page 10-23.

The content and structure of each type of RDR is listed in the "Raw Data Records: Formats and Field Contents" chapter of *Cisco Service Control Application for Broadband Reference Guide*.

NetFlow Records

- You enable and disable the export of NetFlow records using the CLI.

  You can export records per supported RDR type. The data in the following RDR types can be exported using NetFlow:

  – Subscriber Usage RDR

  – Package Usage RDR

  – Link Usage RDR

  – Zone Usage RDR

- The NetFlow records can be sent to more than one collection device.

- NetFlow records can be generated concurrently with RDRs.

Managing RDR Settings

This section explains how to configure the generation of the different types of RDRs.

The content and structure of each type of RDR is listed in the "Raw Data Records: Formats and Field Contents" chapter of *Cisco Service Control Application for Broadband Reference Guide*.

- RDRs are not generated for filtered traffic (see "Filtering the Traffic Flows" section on page 10-23).
- All RDR data is based on Layer 3 volume.

The RDR Settings Dialog Box

The RDR Settings dialog box allows you to control the generation of RDRs for an entire service configuration. This dialog box contains seven tabs:

- Usage RDRs tab—Allows you to enable the generation each type of Usage RDR, and define their generation intervals
- Transaction RDRs tab—Allows you to enable the generation of Transaction RDRs and define their maximum rate of generation
- Quota RDRs tab—Allows you to enable the generation of each type of Quota RDR, and define their generation parameters
- Transaction Usage RDRs tab—Allows you to specify the packages and services for which Transaction Usage RDRs are generated
- Log RDRs tab—Allows you to specify the packages and services for which Log RDRs are generated
- Real-Time Subscriber RDRs tab—Allows you to enable the generation of Real-Time Subscriber Usage RDRs, and define their generation intervals and maximum rate of generation
- Real-Time Signaling RDRs tab—Allows you to specify the packages and services for which Real-Time Signaling RDRs are generated

> **Note** Media Flow RDRs and Malicious Traffic Periodic RDRs are enabled and configured in the How to Edit Advanced Service Configuration Options, page 10-64.

How to Manage Usage RDRs

The five types of Usage RDRs contain data about total usage of all services included in a service usage counter:

- Link Usage RDRs—For the entire link
- Package Usage RDRs—For all subscribers to a particular package
- Subscriber Usage RDRs—For a particular subscriber
- Virtual Links Usage RDRs—For a particular group of virtual links
- Zone Usage RDRs—For the entire zone

You can enable or disable the generation of each type of Usage RDR, and set the generation interval for each type of Usage RDR. You can limit the generation rate of Subscriber Usage RDRs. This is advisable when there are a large number of subscribers.

By default, all four types of Usage RDRs are enabled. (Virtual Links Usage RDRs are enabled by default only if Virtual Links mode was enabled when you created the service configuration.)

Note   Usage RDRs are not generated for blocked sessions. A session is blocked if the service to which the session is mapped is blocked for the package for this subscriber (see "How to Define Per-Flow Actions for a Rule" section on page 9-66), or if the subscriber has exceeded the allowed quota for this service (see "Managing Quotas" section on page 9-83).

For detailed information regarding the RDR purpose, default destination, content, generation logic, tag, and fields, see the following sections in *Cisco Service Control Application for Broadband Reference Guide*:

- Link Usage RDR
- Package Usage RDR
- Subscriber Usage RDR
- Virtual Link Usage RDR
- Zone Usage RDR

Step 1 From the Classification tab in the left pane, choose **Configuration > Classification > RDR Settings**.

The RDR Settings dialog box appears (Figure 8-1).

Figure 8-1 *RDR Settings*
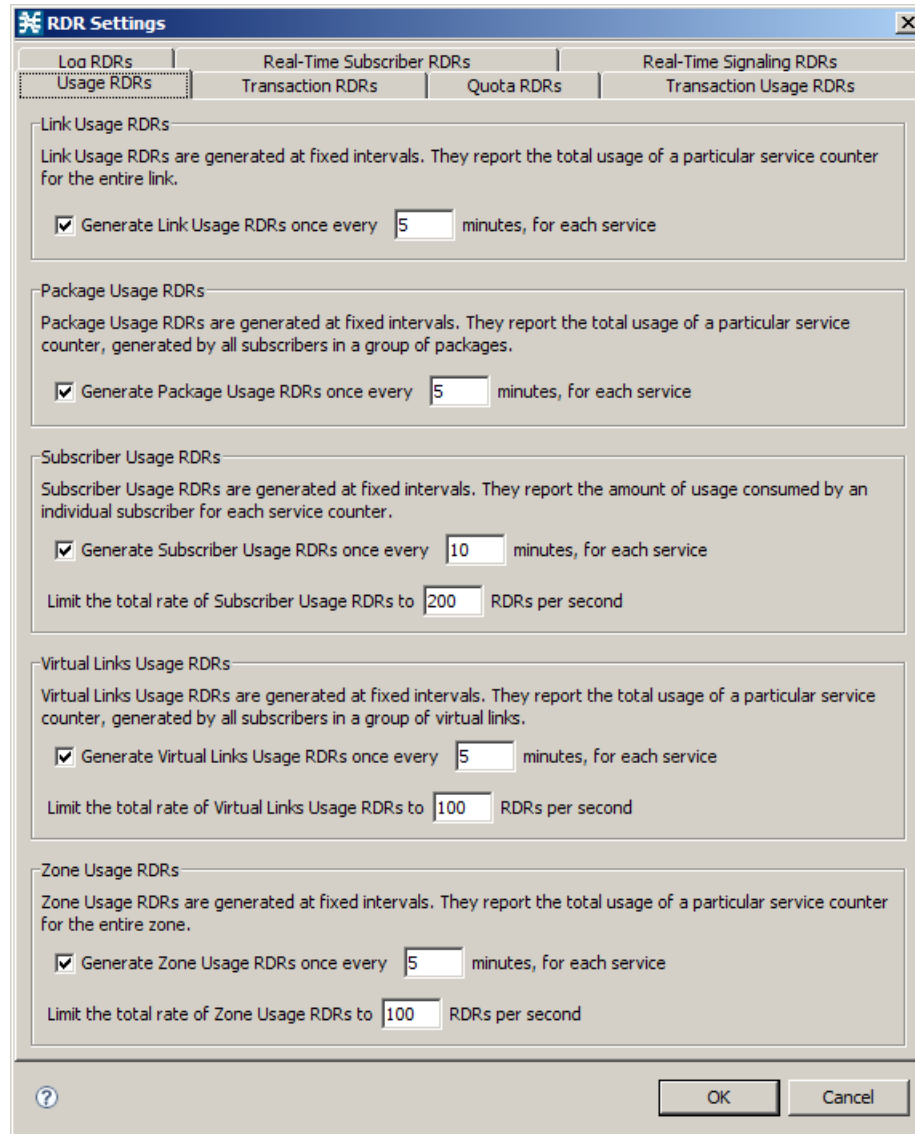
Step 2 To enable the generation of a selected type of Usage RDR, check the appropriate **Generate Usage RDRs** check box.

To disable the generation of a selected type of Usage RDR, uncheck the appropriate **Generate Usage RDRs** check box.

Step 3 To change the generation interval for a selected type of Usage RDR, enter the interval in minutes between each generation of this type of Usage RDRs in the appropriate Generate Usage RDRs field.

> **Note** The interval rate entered in the Subscriber Usage RDR, Virtual Links Usage RDR, and Zone Usage RDR fields is divided by the number of traffic processors present in the Cisco SCE and the same gets updated in the respective tunable.

Step 4 To limit the generation rate of Subscriber Usage RDRs, enter the maximum number of Subscriber Usage RDRs to be generated per second in the Limit the Total Rate of Subscriber Usage RDRs field.

Step 5 Click **OK**.

The RDR Settings dialog box closes.

The new configuration for the generation of Usage RDRs is saved.

How to Manage Transaction RDRs

Each Transaction RDRs contain data about a single network transaction. The Cisco SCE platform can generate Transaction RDRs for selected service types. You can use these RDRs, for example, to generate statistical histograms that help understand the traffic traversing the network.

You can enable or disable the generation of Transaction RDRs, set the maximum number of Transaction RDRs generated per second, and select for which services these RDRs are generated. You can also assign a relative weight to each service. The relative weight determines the relative number of Transaction RDRs that are generated for this service, compared to other services.

By default, at most 100 Transaction RDRs are generated per second, and all services are given the same weight.

For detailed information regarding the RDR purpose, default destination, content, generation logic, tag, and fields, see the "Transaction RDR" section in the *Cisco Service Control Application for Broadband Reference Guide*.

Step 1 From the Classification tab in the left pane, choose **Configuration > Classification > RDR Settings**.

The RDR Settings dialog box appears.

Step 2 Click the **Transaction RDRs** tab.

The Transaction RDRs tab opens (Figure 8-2).

Figure 8-2   Transaction RDRs Tab
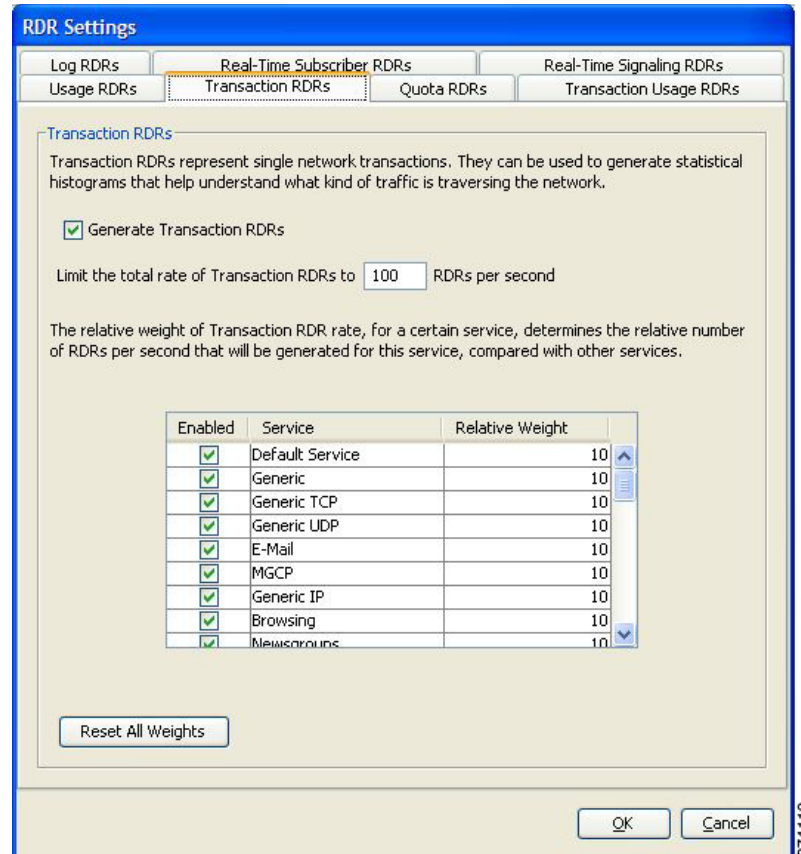
Step 3 To enable the generation of Transaction RDRs, check the **Generate Transaction RDRs** check box.

To disable the generation of Transaction RDRs, uncheck the **Generate Transaction RDRs** check box.

Step 4 To change the maximum generation rate for Transaction RDRs, enter the desired rate in the Limit the Total Rate of Transaction RDRs field.

Step 5 To disable the generation of Transaction RDRs for a selected service, uncheck the **Enabled** check box next to the service name.

Step 6 To set the relative weight for a selected service, double-click in the appropriate cell in the **Relative Weight** column, and enter the desired weight.

Step 7 Click **OK**.

The RDR Settings dialog box closes.

The new configuration for the generation of Transaction RDRs is saved.

How to Manage Quota RDRs

Each Quota RDR contains data for a single subscriber. There are four types of Quota RDRs:

- Quota Breach RDRs—Generated when a quota breach occurs, that is, when services that try to consume from a depleted quota bucket.

    A breached service is handled according to its breach-handling settings. For example, when the quota for a service is consumed, you can block its flows.

- Remaining Quota RDRs—Generated as quota is consumed, but only if a bucket state has change since the last Remaining Quota RDR was generated.

- Quota Threshold Breach RDRs—Generated when the remaining quota in a bucket falls below a threshold. External systems can treat this RDR as a quota request and provision the subscriber with an additional quota before the bucket is depleted.

- Quota State Restore RDRs—Generated when a subscriber is introduced. When a subscriber logs out, their remaining quota is stored in the Cisco Service Control Subscriber Manager (SM). When the subscriber logs in again, this quota is restored from the SM.

You can enable or disable the generation each type of Quota RDR and define the rate of generation of these RDRs.

- For Remaining Quota RDRs, you can set the generation interval, and limit the generation rate (advisable when there are a large number of subscribers).

- For Quota Threshold RDRs, you can configure the threshold.

By default, all Quota RDRs are disabled.

For detailed information regarding the RDR purpose, default destination, content, generation logic, tag, and fields, see the following sections in the *Cisco Service Control Application for Broadband Reference Guide*:

- Quota Breach RDR

- Remaining Quota RDR

- Quota Threshold Breach RDR

- Quota State Restore RDR

Step 1   From the Classification tab in the left pane, choose **Configuration > Classification > RDR Settings**.

The RDR Settings dialog box appears.

Step 2 Click the **Quota RDRs** tab.

The Quota RDRs tab opens (Figure 8-3).

Figure 8-3   *Quota RDRs Tab*
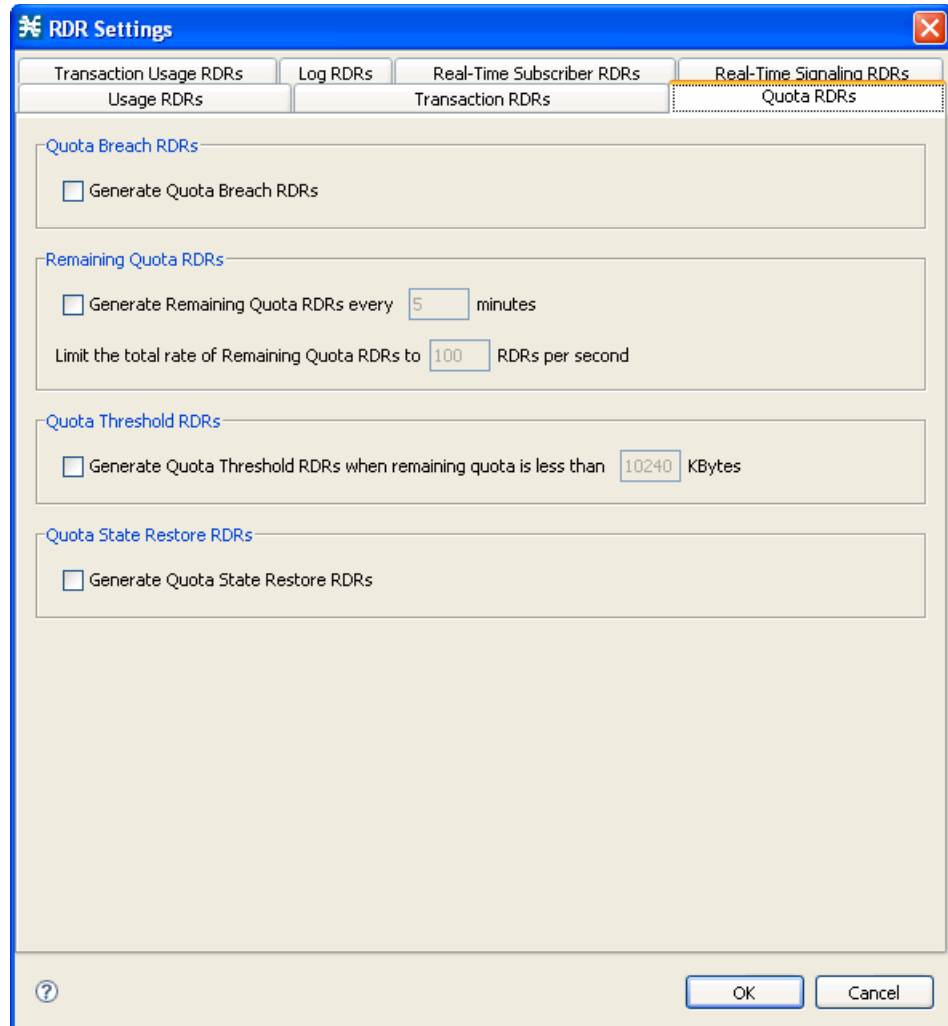
Step 3 To enable the generation of Quota Breach RDRs, check the **Generate Quota Breach RDRs** check box.

Step 4 To enable the generation of Remaining Quota RDRs, check the **Generate Remaining Quota RDRs** check box.

Step 5 To change the generation interval of Remaining Quota RDRs, in the Generate Remaining Quota RDRs field, enter the interval in minutes between each generation of the RDR.

Step 6 To limit the maximum generation rate of Remaining Quota RDRs, in the Limit the Total Rate of Remaining Quota RDRs field, enter the maximum number of Remaining Quota RDRs to be generated per second.

Step 7 To enable the generation of Quota Threshold RDRs, check the **Generate Quota Threshold RDRs** check box.

Step 8 To change the Threshold for Quota Threshold RDRs, in the Generate Quota Threshold RDRs field, enter the threshold for which Quota Threshold RDRs are generated.

Step 9 To enable the generation of Quota State Restore RDRs, check the **Generate Quota State Restore RDRs** check box.

Step 10 Click **OK**.

The RDR Settings dialog box closes.

The new configuration for the generation of Quota RDRs is saved.

How to Manage Transaction Usage RDRs

Transaction Usage RDRs are generated for all transactions of selected packages or for selected services per package. Each Transaction Usage RDR contains data about a single network transaction. You can use these RDRs, for example, to build detailed usage logs for specific services and subscribers for transaction-based billing.

⚠

Caution Generating and collecting an RDR for each transaction can compromise performance. Enable Transaction Usage RDR generation only for services and packages that must be monitored or controlled.

You can select the packages and services for which Transaction Usage RDRs are generated. The following RDRs are also generated for these packages and services:

- HTTP Transaction Usage RDR
- RTSP Transaction Usage RDR
- VoIP Transaction Usage RDR

By default, no Transaction Usage RDRs are generated.

✎

Note Media Flow RDRs are enabled using the Advance Service Configuration Options. When enabled, Media Flow RDRs are generated at the end of every SIP and Skype media flow. You can use the Media Flow RDRs to distinguish between SIP voice and video calls. For details on enabling Media Flow RDRs, see "How to Edit Advanced Service Configuration Options" section on page 10-64.

For details on the RDR purpose, default destination, content, generation logic, tag, and fields, see the following sections in the *Cisco Service Control Application for Broadband Reference Guide*:

- Transaction Usage RDR
- HTTP Transaction Usage RDR
- RTSP Transaction Usage RDR
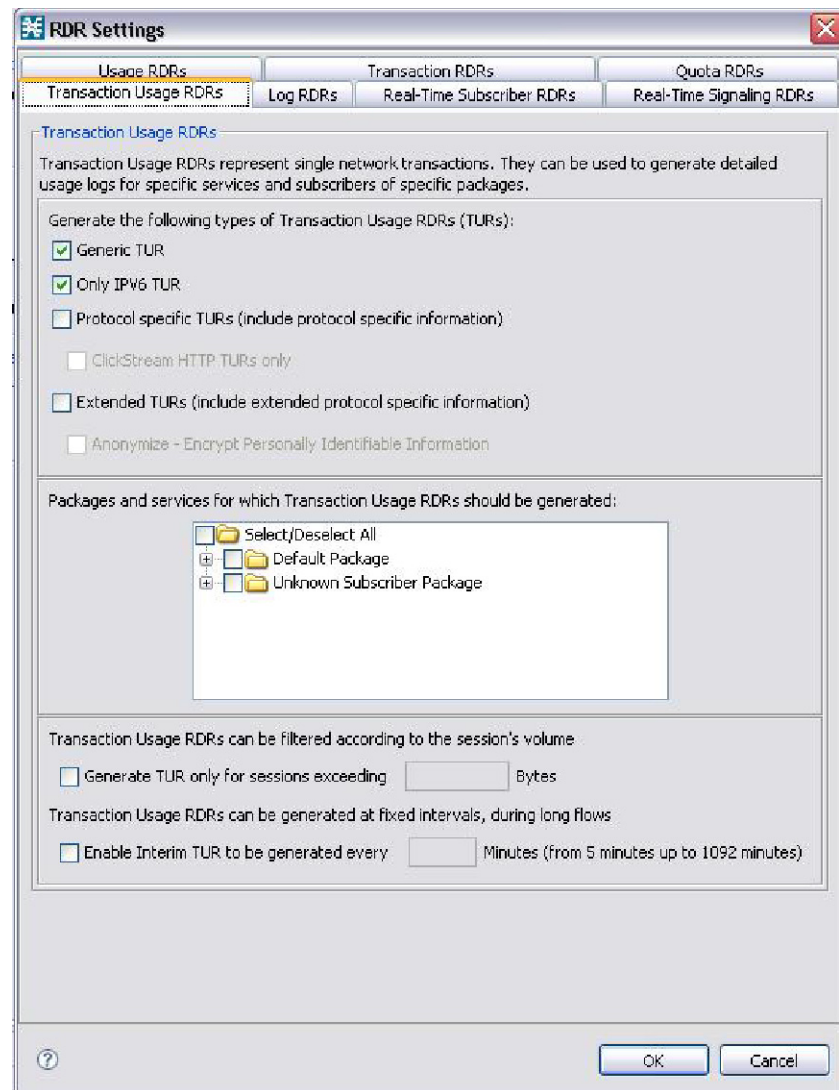- VoIP Transaction Usage RDR

Step 1   From the Classification tab in the left pane of Service Configuration Editor window, choose **Configuration > Classification > RDR Settings**.

The RDR Settings dialog box appears.

Step 2   Click the **Transaction Usage RDRs** tab.

The information under the Transaction Usage RDRs tab is displayed(Figure 8-4).

Figure 8-4   Transaction Usage RDRs Tab

Step 3   Check one or more of the following types of Transaction Usage RDRs to be generated:

- **Generic TUR**
- **Only IPV6 TUR**
- **Protocol Specific TURs (include protocol specific information)**
- **Extended TURs (include extended protocol specific information)**

If you select Only IPV6 TUR, the Only IPV6 TUR checkbox is enabled. Check this box to generate only the IPv6 TUR.

If you check Protocol specific TURs, the ClickStream HTTP TURs only checkbox is enabled. Check this box to generate only the HTTP TUR with clickstream signature for the selected service and packages.

If you check Extended TURS, the Anonymize - Encrypt Personally Identifiable Information checkbox is enabled. Check this box to anonymize data.

Step 4 (Optional) To enable the generation of Transaction Usage RDRs for a selected package, check the check box next to the package name in the package tree.

The package expands to show all component services of the package; all services are checked.

Step 5 Enable the generation of Transaction Usage RDRs for selected services of a package.

a. Expand the node of the desired package.

b. Check the check box next to the service name of each service for which a Transaction Usage RDR is to be generated.

Step 6 (Optional) Limit the generation of Transaction Usage RDRs by session size.

a. Check the **Generate TUR only for sessions exceeding** check box.

The Bytes field is enabled.

b. Enter the minimum session size in bytes for which a Transaction Usage RDR should be generated for the session.

Step 7 (Optional) Enable the generation of additional, interim Transaction Usage RDRs for long flows. (Usually, a Transaction Usage RDR is generated only when a flow closes.)

a. Check the **Enable Interim TUR to be generated every** check box.

The Minutes field is enabled.

b. Enter the required time in minutes between each generation of a Transaction Usage RDR for each flow.

Step 8 Click **OK**.

The RDR Settings dialog box closes.

The new configuration for the generation of Transaction Usage RDRs is saved.

How to Manage Log RDRs

Log RDRs, which provide information about system events, are generated in response to specific actions or state changes. There are two types of Log RDRs:

• Blocking RDRs—Generated each time a transaction is blocked

• Breach RDRs—Generated each time a bucket exceeds the global threshold

You can set the maximum number of Log RDRs generated per second. You can select the packages and services for which Blocking RDRs are generated.By default:

• Blocking RDRs are generated for all packages

• Breach RDRs are always generated

✎
**Note**   At most, 20 Log RDRs are generated for each second.

For details on the RDR purpose, default destination, content, generation logic, tag, and fields, see the following sections in the *Cisco Service Control Application for Broadband Reference Guide*:

- Blocking RDR
- Quota Breach RDR

Step 1   From the Classification tab in the left pane, choose **Configuration > Classification > RDR Settings**.

The RDR Settings dialog box appears.

Step 2   Click the **Log RDRs** tab.

The Log RDRs tab opens (Figure 8-5).

Figure 8-5   *Log RDRs Tab*
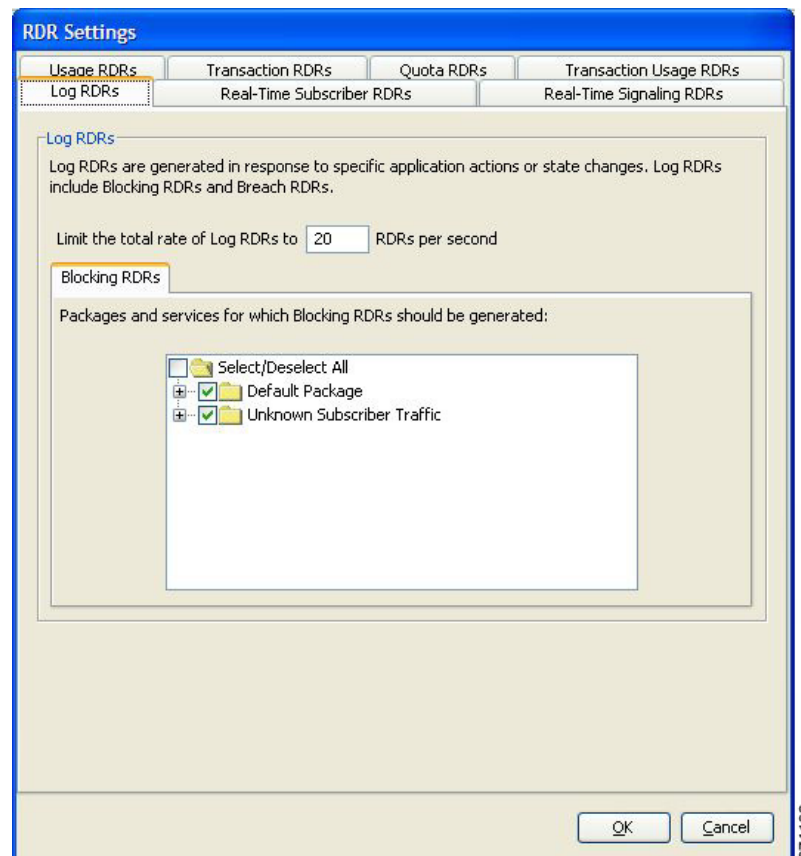
Step 3   To change the maximum generation rate for Log RDRs, enter the desired rate in the Limit the Total Rate of Log RDRs field.

✎
Note   The limit rate entered in the Log RDRs field is divided by the number of traffic processors present in the Cisco SCE. The same rate also gets updated in the respective tunable.

Step 4 To enable the generation of Blocking RDRs for selected packages, check the check box next to the package name in the package tree.

The package expands to show all component services of the package; all the services are checked.

Step 5 Enable the generation of Blocking RDRs for selected services of a package.

a. Expand the node of the desired package.

b. Check the check box next to the service name of each desired service.

Step 6 Click **OK**.

The RDR Settings dialog box closes.

The new configuration for the generation of Log RDRs is saved.

How to Manage Real-Time Subscriber Usage RDRs

Real-Time Subscriber Usage RDRs, which report subscriber usage, are generated for each individual subscriber for each service used, at specified intervals. These RDRs permit a more granular monitoring of selected subscribers when necessary.

For details on selecting the subscribers to be monitored, see "Selecting Subscribers for Real-Time Usage Monitoring" section on page 14-15.

⚠
Caution Generating and collecting Real-Time Subscriber Usage RDRs for many subscribers can compromise performance. Enable Real-Time Subscriber Usage RDR generation only for subscribers that must be monitored.

You can enable or disable the generation of Real-Time Subscriber Usage RDRs, set the generation interval for these RDRs, and set the maximum number generated per second.
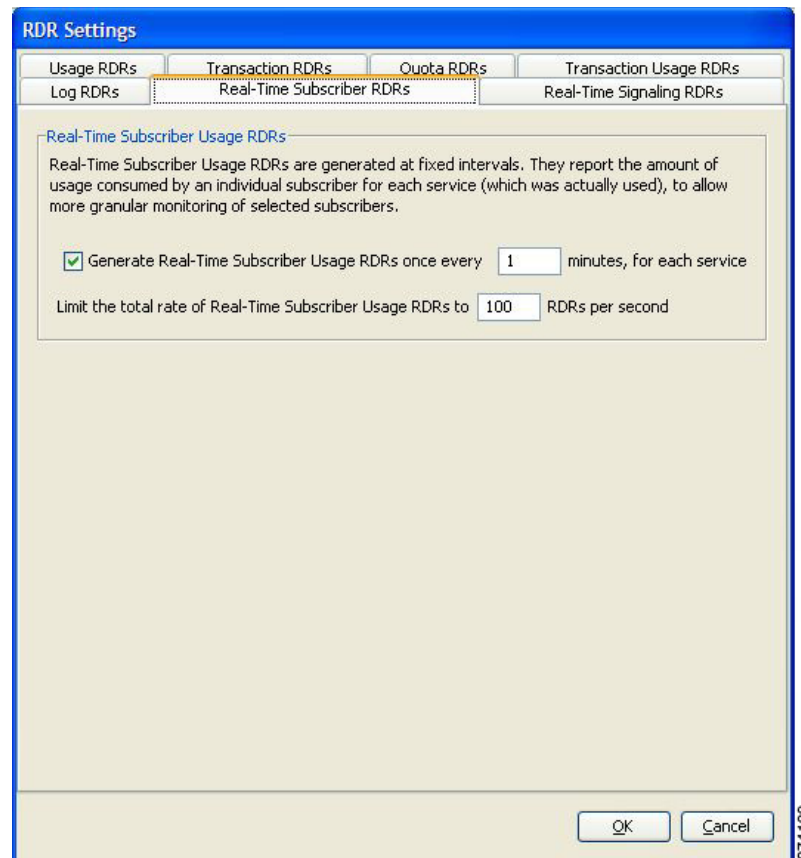
By default, Real-Time Subscriber Usage RDRs:

- Are enabled (but only for selected subscribers)
- Are generated for each subscriber once every minute
- Are limited to 100 RDRs generated per second

For details on the RDR purpose, default destination, content, generation logic, tag, and fields, see the "Real-Time Subscriber Usage RDR" section in the *Cisco Service Control Application for Broadband Reference Guide*.

Step 1 From the Classification tab in the left pane, choose **Configuration > Classification > RDR Settings**.

The RDR Settings dialog box appears.

Step 2 Click the **Real-Time Subscriber RDRs** tab.

The Real-Time Subscriber RDRs tab opens (Figure 8-6).

Figure 8-6 Real-Time Subscriber RDRs Tab

Step 3 To enable the generation of Real-Time Subscriber Usage RDRs, check the **Generate Real-Time Subscriber Usage RDRs** check box.

Step 4 To change the generation interval for Real-Time Subscriber Usage RDRs, enter the desired interval in minutes between each generation of the RDRs in the Generate Real-Time Subscriber Usage RDRs field.

Step 5 To limit the generation rate of Real-Time Subscriber Usage RDRs, enter the maximum number of Real-Time Subscriber Usage RDRs to be generated per second in the Limit the total rate of Real-Time Subscriber Usage RDRs field.

Step 6 Click **OK**.

The RDR Settings dialog box closes.

The new configuration for the generation of Real-Time Subscriber Usage RDRs is saved.

How to Manage Real-Time Signaling RDRs

Real-Time Signaling RDRs can be used to signal external systems concerning events detected by the Cisco SCE platform, allowing real-time actions to be taken across the network.

Real-Time Signaling RDRs, are generated at the beginning and end of a flow, at specified intervals after the beginning of the flow, and at the beginning and end of a network attack.

There are two groups of Real-Time Signaling RDRs:

- Flow Signaling RDRs:
    - Flow Start Signaling RDRs
    - Flow Stop Signaling RDRs
    - Flow Interim Signaling RDRs
- Attack Signaling RDRs:
    - Attack Start Signaling RDRs
    - Attack Stop Signaling RDRs

You can enable or disable the generation of Flow Signaling RDRs for selected packages, or for selected services per package. You can set the generation interval for Flow Interim Signaling RDRs, which can be generated only if Flow Start and Flow Stop Signaling RDRs are enabled.

You can enable or disable the generation of Attack Signaling RDRs for selected packages.

Note Malicious Traffic Periodic RDRs are enabled and configured in How to Edit Advanced Service Configuration Options, page 10-64.

For detailed information regarding the RDR purpose, default destination, content, generation logic, tag, and fields, see the following sections in the *Cisco Service Control Application for Broadband Reference Guide*:

- Flow Start RDR
- Flow End RDR
- Ongoing Flow RDR
- Attack Start RDR
- Attack End RDR

By default, no Real-Time Signaling RDRs are generated.

Step 1   From the Classification tab in the left pane, choose **Configuration > Classification > RDR Settings**.

The RDR Settings dialog box appears.

Step 2   Click the **Real-Time Signaling RDRs** tab.

The Real-Time Signaling RDRs tab opens (Figure 8-7).

Figure 8-7   *Real-Time Signaling RDRs Tab*
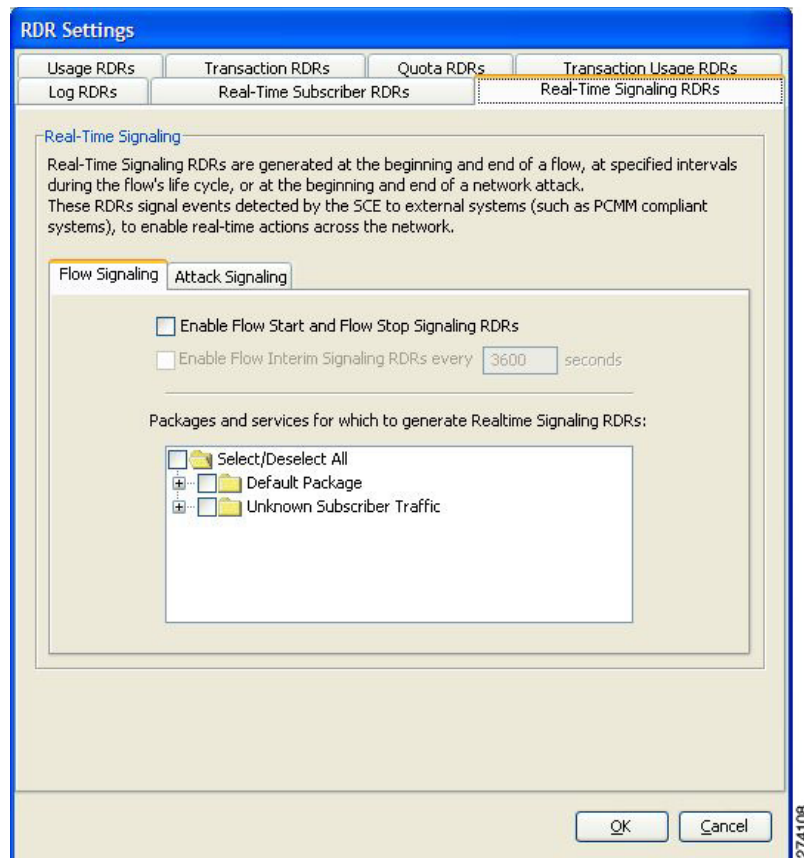
Step 3   To enable the generation of Flow Start and Flow Stop Signaling RDRs, check the **Enable Flow Start and Flow Stop Signaling RDRs** check box.

✎
Note   Generation of Flow Start and Flow Stop Signaling RDRs is not supported when unidirectional classification is enabled. If you try to check the Enable Flow Start and Flow Stop Signaling RDRs check box when unidirectional classification is enabled, an RDR Settings Error message appears.

Click **OK**, and continue at Step 8.

The Enable Flow Interim Signaling RDRs check box is enabled.

Step 4   To enable the generation of Flow Interim Signaling RDRs, check the **Enable Flow Interim Signaling RDRs** check box.

The Enable Flow Interim Signaling RDRs field is enabled.

Step 5   To change the generation interval for Flow Interim Signaling RDRs, enter the interval in minutes between each generation of the RDRs in the Enable Flow Interim Signaling RDRs field.

Step 6   To enable the generation of Flow Interim Signaling RDRs for selected packages, check the check box next to the package name in the package tree.

The package expands to show all component services of the package; all the services are checked.

Step 7   To enable the generation of Flow Interim Signaling RDRs for selected services of a package:

a.   Expand the node of the desired package.

b.   Check the check box next to the service name of each desired service.

Step 8   To enable the generation of Attack Signaling RDRs:

a.   In the body of the Real-Time Signaling RDRs tab, click the **Attack Signaling** tab (Figure 8-8).

Figure 8-8   Attack Signaling Tab

b.   Check the **Enable Attack Start and Attack Stop Signaling RDRs** check box.

Step 9   To enable the generation of Attack Signaling RDRs for selected packages, check the check box next to the package name in the package list.

Step 10   Click **OK**.

The RDR Settings dialog box closes.

The new configuration for the generation of Real-Time Signaling RDRs is saved.