Cisco Service Control Application for Broadband Reference Guide

Release 4.1.x
January 31, 2014

Cisco Systems, Inc.
www.cisco.com

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.

Text Part Number: OL-30607-04

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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. 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.

Cisco Service Control Application for Broadband Reference Guide
© 2013 Cisco Systems, Inc. All rights reserved.

About this Guide ix

Introduction ix

Document Revision History x

Organization xii

Related Documentation xiii

Conventions xiv

Obtaining Documentation and Submitting a Service Request xv

CHAPTER 1 **Default Service Configuration Reference Tables** 1-1

Introduction 1-1

Filter Rules 1-2

Information About Protocols 1-4

Generic Protocols 1-4

Signature-Based Protocols 1-5

IP Protocols 1-12

Port-Based Protocols 1-16

Protocols Identified on Unidirectional Flows 1-38

Services 1-41

RDR Settings 1-46

Rules 1-49

System Mode 1-49

CHAPTER 2 **Raw Data Records: Formats and Field Contents** 2-1

Introduction 2-1

Raw Data Records Overview 2-3

Universal RDR Fields 2-4

ADDITIONAL_INFO Field 2-6

Transaction RDR 2-7

Anonymized Transaction RDR 2-10

Transaction Usage RDR 2-15

Anonymized Transaction Usage RDR 2-19

HTTP Transaction Usage RDR 2-24

Anonymized HTTP Transaction Usage RDR 2-30
RTSP Transaction Usage RDR 2-34
Anonymized RTSP Transaction Usage RDR 2-38
VoIP Transaction Usage RDR 2-42
Anonymized VoIP Transaction Usage RDR 2-46
Video Transaction Usage RDR 2-50
Anonymized Video Transaction Usage RDR 2-55
Generic Usage RDR 2-60
Using the Generic Usage RDR to Report IPv6 Usage 2-63
Subscriber Usage RDR 2-64
Real-Time Subscriber Usage RDR 2-68
Link Usage RDR 2-71
Zone Usage RDR 2-75
Package Usage RDR 2-77
Virtual Links Usage RDR 2-81
Blocking RDR 2-84
Anonymized Blocking RDR 2-86
Quota Breach RDR 2-89
Quota Status RDR 2-92
Quota Threshold Breach RDR 2-95
Session Creation RDR 2-99
DHCP RDR 2-101
DHCPv6 RDR 2-102
RADIUS RDR 2-104
Flow Start RDR 2-105
Anonymized Flow Start RDR 2-107
Flow End RDR 2-109
Anonymized Flow End RDR 2-111
Flow Ongoing RDR 2-113
Anonymized Flow Ongoing RDR 2-115
Media Flow RDR 2-117
Anonymized Media Flow RDR 2-126
Attack Start RDR 2-135
Attack End RDR 2-136
Malicious Traffic Periodic RDR 2-137

Spam RDR 2-139
Anonymized Spam RDR 2-142
Information About RDR Enumeration Fields 2-145
Block Reason (uint8) 2-145
String Fields 2-145
Aggregation Period (uint8) 2-147
Flow Close Mode (uint8) 2-147
Time Frames (unint16) 2-148
RDR Tag Assignment Summary 2-149
Periodic RDR Zero Adjustment Mechanism 2-152

CHAPTER 3 **NetFlow Records: Formats and Field Contents** 3-1
Introduction 3-1
NetFlow 3-1
NetFlow Field Types 3-2
NetFlow Ports 3-6

CHAPTER 4 **Database Tables: Formats and Field Contents** 4-1
Introduction 4-1
Database Tables Overview 4-2
Table RPT_NUR 4-3
Table RPT_SUR 4-3
Table RPT_PUR 4-5
Table RPT_LUR 4-6
Table RPT_GUR 4-7
Table RPT_TR 4-9
Table RPT_OSFP 4-10
Table OSFP_TYPES 4-10
Table RPT_MEDIA 4-11
Table RPT_MALUR 4-12
Table RPT_TOPS_PERIOD0 4-13
Table RPT_TOPS_PERIOD1 4-14
Table RPT_TOPS_PERIOD0_CUMULATIVE 4-15
Table RPT_TOPS_PERIOD1_CUMULATIVE 4-16
Table RPT_TOPS_PEAK_PERIOD 4-17
Table RPT_TOPS_PEAK_CUMULATIVE 4-18

Table RPT_VLUR 4-19
Table INI_VALUES 4-20
Table VLINK_INI 4-23
Table CONF_SE_TZ_OFFSET 4-23
Table RPT_TOP_APN 4-24
Table RPT_TOP_DEVICE_TYPE 4-24
Table RPT_TOP_NETWORK_TYPE 4-25
Table RPT_TOP_SGSN 4-25
Table RPT_TOP_USER_LOCATION 4-26
Table RPT_DVLINK 4-27
Table RPT_UVLINK 4-28
Table RPT_TOP_HTTP_DOMAINS 4-29
Table RPT_TOP_HTTP_HOSTS 4-30
Table RPT_TOP_VIDEO_DOMAINS 4-31
Table RPT_TOP_VIDEO_HOSTS 4-32
Table RPT_ZUR 4-33
Table RPT_SPAM 4-34
Table RPT_FUR 4-35
Table IMEI_DEVICETYPE 4-36
Table RTP_VIDEO_QOE 4-36
Table RPT_VIDEO_DURATION 4-36
Table RPT_VIDEO_RESOLUTION 4-37
Table RPT_VIDEO_BITRATE 4-37
Table VIDEO_MONITOR_TYPES 4-38
Table RPT_DEVICE_COUNT 4-38
Table RPT_DEVICE_TYPES 4-38

CHAPTER 5 **CSV File Formats** 5-1
Introduction 5-1
Information About Service Configuration Entities CSV File Formats 5-2
Service CSV Files 5-2
Protocol CSV Files 5-3
Zone CSV Files 5-3
Standard Format 5-3
Easy Format 5-3
Information About Flavor CSV Files 5-3

HTTP URL CSV Files 5-4
HTTP Referer CSV Files 5-4
HTTP User Agent CSV Files 5-5
HTTP Composite CSV Files 5-5
RTSP User Agent CSV Files 5-5
RTSP Host Name CSV Files 5-5
RTSP Composite CSV Files 5-6
SIP Destination Domain CSV Files 5-6
SIP Source Domain CSV Files 5-6
SIP Composite CSV Files 5-6
SMTP Host Name CSV Files 5-6
ToS CSV Files 5-6
Information About Subscriber CSV File Formats 5-7
Import/Export File: Format of the Mappings Field 5-7
SCE Subscriber CSV Files 5-8
SCMS SM Subscriber CSV Files 5-8
SCE Anonymous Group CSV Files 5-8
Cisco SCA BB Anonymous Group Import CSV File 5-9
SCE Subscriber Template CSV File 5-9
Information About Collection Manager CSV File Formats 5-9
CSV Adapter CSV Files 5-9
TA Adapter CSV Files 5-10
RAG Adapter CSV Files 5-10

CHAPTER 6 **Cisco SCA BB Proprietary MIB Reference** 6-1
Introduction 6-1
Information About SNMP Configuration and Management 6-2
Configuring the SNMP Interface on the SCE Platform 6-2
Related Information 6-2
Required MIB Files 6-2
The Order in Which to Load the MIB Files 6-3
Information About the Service Control Enterprise MIB 6-3
Information About the CISCO-SCAS-BB MIB 6-4
Using This Reference 6-4
pcubeEngageObjs (pcubeWorkgroup 2) 6-5
pcubeEngageObjs Objects 6-5
pcubeEngageObjs Structure 6-5
Service Group: serviceGrp (pcubeEngageObjs 1) 6-6
Link Group: linkGrp (pcubeEngageObjs 2) 6-7

Package Group: packageGrp (pcubeEngageObjs 3) **6-11**
Subscriber Group: subscriberGrp (pcubeEngageObjs 4) **6-17**
Service Counter Group: serviceCounterGrp (pcubeEngageObjs 5) **6-20**
Guidelines for Using the CISCO-SCAS-BB MIB **6-23**
globalScopeServiceCounterTable and subscriberScopeServiceCounterTable **6-23**
packageCounterTable **6-24**
Accessing Subscriber Information (the spvIndex) **6-24**
Accessing Subscriber Information in Cisco SCE 2000 **6-24**
Accessing Subscriber Information in Cisco SCE 8000 **6-25**

About this Guide

Revised: January 31, 2014

Introduction

This chapter describes who should read *Cisco Service Control Application for Broadband Reference Guide*, how it is organized, its document conventions, and how to obtain documentation and technical assistance. This guide assumes a basic familiarity with the concept of the Cisco Service Control solution, the Service Control Engine (SCE) platforms, and related components.

This guide provides information about the data structures created and used by Cisco Service Control Application for Broadband (Cisco SCA BB). It is intended for the:

- Administrator who is responsible for daily operations of the Cisco Service Control solution.
- Integrators who are developing applications on top of Cisco SCA BB.

Document Revision History

The following Document Revision History table records the changes made to this document.

Table 1 Document Revision History

Revision	Cisco Service Control Release Number and Date	Change Summary
OL-30607-04	Release 4.1.x January 31, 2014	Updated the following sections: • "Link Usage RDR" section on page 2-71. • "Zone Usage RDR" section on page 2-75. • "Package Usage RDR" section on page 2-77. • "Virtual Links Usage RDR" section on page 2-81. • "Transaction RDR" section on page 2-7. • "Anonymized Transaction RDR" section on page 2-10. • "Transaction Usage RDR" section on page 2-15. • "Anonymized Transaction Usage RDR" section on page 2-19. • "HTTP Transaction Usage RDR" section on page 2-24. • "Anonymized HTTP Transaction Usage RDR" section on page 2-30. • "RTSP Transaction Usage RDR" section on page 2-34. • "Anonymized RTSP Transaction Usage RDR" section on page 2-38. • "VoIP Transaction Usage RDR" section on page 2-42. • "Anonymized VoIP Transaction Usage RDR" section on page 2-46. • "Video Transaction Usage RDR" section on page 2-50. • "Anonymized Video Transaction Usage RDR" section on page 2-55. • "Generic Usage RDR" section on page 2-60.
OL-30607-03	Release 4.1.x January 29, 2014	Updated the following sections: • "Blocking RDR" section on page 2-84. • "Real-Time Subscriber Usage RDR" section on page 2-68.

Table 1 Document Revision History (continued)

Revision	Cisco Service Control Release Number and Date	Change Summary
OL-30607-02	Release 4.1.x January 08, 2014	• Updated the "Media Flow RDR" section on page 2-117. • Updated the "Anonymized Media Flow RDR" section on page 2-126.
OL-30607-01	Release 4.1.x December 23, 2013	First version of this document (new for the Release 4.1.x train). Release 4.1.0 updates: • Updated Chapter 2, "Raw Data Records: Formats and Field Contents."

Organization

This guide contains the following sections.

Table 2 Document Organization

Section	Title	Description
Chapter 1	Default Service Configuration Reference Tables	Describes the default service configuration provided with Cisco SCA BB.
Chapter 2	Raw Data Records: Formats and Field Contents	Lists the various RDRs produced by the Cisco SCE platform. Provides the structure of RDRs, describes the columns and fields of each RDR, and states under what conditions each RDR is generated. Also provides field-content information for fields generated by Cisco Service Control components (such as tags), and a description of the Periodic RDR Zero Adjustment Mechanism.
Chapter 3	NetFlow Records: Formats and Field Contents	Lists the RDRs whose data can be generated as NetFlow records and describes the fields possible in a NetFlow record.
Chapter 4	Database Tables: Formats and Field Contents	Presents the different database tables used for storing RDRs (after their conversion by an adapter), and a description of the table columns (field names and types).
Chapter 5	CSV File Formats	Describes the location and structure of CSV files pertaining to service configuration, subscriber management, and data collection management.
Chapter 6	Cisco SCA BB Proprietary MIB Reference	Describes the part of the Cisco SCE proprietary MIB that provides configuration and run-time status for Cisco SCA BB.

Related Documentation

Use the *Cisco Service Control Application for Broadband Reference Guide* with the following Cisco documentation:

- Cisco Service Control Product Documentation

Conventions

This document uses the following conventions.

Table 3 Document Conventions

Convention	Indication
bold font	Commands and keywords and user-entered text appear in **bold** font.
italic font	Document titles, new or emphasized terms, and arguments for which you supply values are in *italic* font.
[ ]	Elements in square brackets are optional.
{x | y | z }	Required alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string includes the quotation mark.
`courier` font	Terminal sessions and information the system displays appear in `courier` font.
< >	Nonprinting characters such as passwords are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.

Tip Means *the following information will help you solve a problem.* The tips information might not be troubleshooting or even an action, but could be useful information, similar to a Timesaver.

Caution Means *reader be careful*. In this situation, you might perform an action that could result in equipment damage or loss of data.

Timesaver Means *the described action saves time*. You can save time by performing the action described in the paragraph.

Warning **Means *reader be warned*. In this situation, you might perform an action that could result in bodily injury.**

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

Default Service Configuration Reference Tables

Published: December 23, 2013

Introduction

This chapter describes the default service configuration provided with Cisco SCA BB. The default service configuration serves as a starting point for creating a service configuration tailored to meet customer needs.

This chapter consists of these sections:

- Filter Rules, page 1-2
- Information About Protocols, page 1-4
- Services, page 1-41
- RDR Settings, page 1-46
- Rules, page 1-49
- System Mode, page 1-49

Filter Rules

Filter rules allow you to instruct the Cisco SCE platform to ignore some types of flow based on Layer 3 and Layer 4 properties of the flow, and transmit the flows without any changes.

Table 1-1 lists the filter rules defined in the default service configuration.

Table 1-1 Filter Rules

Flow Filter Name	Default State	Description
ICMP Filter	Active	Applies to ICMP packets, packets bypass the policy engine and are mapped to CoS BE.
DNS (to network)	Active	Applies to UDP packets, network-side port is equal to 53, packets bypass the policy engine and are mapped to CoS BE.
DNS (to subscriber)	Active	Applies to UDP packets, subscriber-side port is equal to 53, packets bypass the policy engine and are mapped to CoS BE.
net-bios (to network)	Active	Applies to UDP packets, network-side port is equal to 137, packets bypass the policy engine and are mapped to CoS BE.
net-bios (to subscriber)	Active	Applies to UDP packets, network-side port is equal to 137, packets bypass the policy engine and are mapped to CoS BE.
eDonkey UDP (to network)	Inactive	Applies to UDP packets, network-side ports in the range 4661 – 4665, packets bypass the policy engine and are mapped to CoS BE.
eDonkey UDP (to subscriber)	Inactive	Applies to UDP packets, subscriber-side ports in the range 4661 – 4665, packets bypass the policy engine and are mapped to CoS BE.
eMule UDP (to network)	Inactive	Applies to UDP packets, network-side ports in the range 4670 – 4674, packets bypass the policy engine and are mapped to CoS BE.
eMule UDP (to subscriber)	Inactive	Applies to UDP packets, subscriber-side ports in the range 4670 – 4674, packets bypass the policy engine and are mapped to CoS BE.
eMule UDP 2 (to network)	Inactive	Applies to UDP packets, network-side ports in the range 5670 – 5674, packets bypass the policy engine and are mapped to CoS BE.
eMule UDP 2 (to subscriber)	Inactive	Applies to UDP packets, subscriber-side ports in the range 5670 – 5674, packets bypass the policy engine and are mapped to CoS BE.
eMule UDP 3 (to network)	Inactive	Applies to UDP packets, network-side ports in the range 5780 – 5784, packets bypass the policy engine and are mapped to CoS BE.
eMule UDP 3 (to subscriber)	Inactive	Applies to UDP packets, subscriber-side ports in the range 5780 – 5784, packets bypass the policy engine and are mapped to CoS BE.

Table 1-1 Filter Rules (continued)

Flow Filter Name	Default State	Description
BGP Filter	Inactive	Applies to TCP packets, network-side port is equal to 179, packets bypass the policy engine and are mapped to CoS BE.
DHCP Filter	Inactive	Applies to UDP packets, network-side ports in the range 67 – 68, packets bypass the policy engine and are mapped to CoS BE.
OSPF Filter	Inactive	Applies to OSPFIGP packets, packets bypass the policy engine and are mapped to CoS BE.
IS-IS Filter	Inactive	Applies to IS-IS packets, packets bypass the policy engine and are mapped to CoS BE.
IGRP Filter	Inactive	Applies to IGP packets, packets bypass the policy engine and are mapped to CoS BE.
EIGRP Filter	Inactive	Applies to EIGRP packets, packets bypass the policy engine and are mapped to CoS BE.
HSRP Filter 1	Inactive	Applies to UDP packets, network-side IP is equal to 224.0.0.2, packets bypass the policy engine and are mapped to CoS BE.
HSRP Filter 2	Inactive	Applies to UDP packets, network-side port is equal to 1985, packets bypass the policy engine and are mapped to CoS BE.
HSRP Filter 3	Inactive	Applies to UDP packets, subscriber-side port is equal to 1985, packets bypass the policy engine and are mapped to CoS BE.
RIP Filter 1	Inactive	Applies to UDP packets, network-side IP is equal to 224.0.0.9, packets bypass the policy engine and are mapped to CoS BE.
RIP Filter 2	Inactive	Applies to UDP packets, network-side port is equal to 520, packets bypass the policy engine and are mapped to CoS BE.
RIP Filter 3	Inactive	Applies to UDP packets, subscriber-side port is equal to 520, packets bypass the policy engine and are mapped to CoS BE.
RADIUS Filter	Inactive	Applies to UDP packets, network-side port is equal to 1812, packets bypass the policy engine and are mapped to CoS BE.
RADIUS Filter (early deployment)	Inactive	Applies to UDP packets, network-side ports in the range 1645 – 1646, packets bypass the policy engine and are mapped to CoS BE.

Information About Protocols

Protocols are divided into four groups:

- Generic protocols—Protocols that are used for transactions not mapped to a service by one of the more specific protocol types.
- Signature-based protocols—Protocols that are classified according to a Layer 7 application signature. This group includes the most common protocols, such as HTTP and FTP, and a large group of popular Peer-to-Peer protocols.
- IP protocols—Protocols (such as ICMP), other than TCP and UDP protocols that are identified according to the IP protocol number of the transaction.
- Port-based protocols—TCP and UDP protocols that are classified according to their well-known ports. The default configuration includes more than 600 common port-based protocols.

  You may add new protocols (for example, to classify a new gaming protocol that uses a specific port) and edit or remove existing ones.

In Cisco SCA BB Console, protocols are listed in ASCII order.

The tables in the following sections list the protocols defined in the default service configuration:

- Generic Protocols, page 1-4
- Signature-Based Protocols, page 1-5
- IP Protocols, page 1-12
- Port-Based Protocols, page 1-16
- Protocols Identified on Unidirectional Flows, page 1-38

Generic Protocols

Three generic protocols (IP, TCP, and UDP) serve as default containers for classifying transactions of the relevant type (IP, TCP, or UDP) that are not classified as belonging to a more specific protocol.

A transaction is classified as belonging to one of the generic protocols if it meets both the following conditions:

- It was not classified as belonging to a signature-based protocol.
- It was not classified as belonging to an IP or port-based protocol that is mapped to a service.

Table 1-2 list the generic protocols.

Table 1-2 Generic Protocols

Protocol Name	ID	Description
Generic IPv6	1196	Any IPv6 traffic (TCP or UDP) that does not match the Signature-Based protocol, and where the related port-based protocol (if it exists) is not specifically mapped to a service.
Generic IP	10	Any non-TCP or non-UDP transaction where the related IP protocol is not specifically mapped to a service.

Table 1-2 Generic Protocols (continued)

Protocol Name	ID	Description
Generic TCP	0	Any TCP transaction that does not match any signature-based protocol, and where the related port-based protocol (if it exists) is not specifically mapped to a service.
Generic UDP	1	Any UDP transaction that does not match any signature-based protocol, and where the related port-based protocol (if it exists) is not specifically mapped to a service.

Signature-Based Protocols

A transaction is classified as belonging to one of the signature-based protocols if it is carried on the well-known port of the protocol or matches the signature of the protocol.

Note Table 1-3 lists only signature-based protocols that are not Peer-to-Peer, VoIP, or SIP protocols (these protocols are listed in the following tables). However, the Signature-Based Protocols Filter in the Console lists all signature-based protocols.

Table 1-3 Signature-Based Protocols

Protocol Name	ID	TCP Ports	UDP Ports
ActiveSync Gmail	1123	—	—
Apple iCloud	1204	—	—
Audio over HTTP	1041	—	—
Alicall	1169	—	—
Baidu Movie	1043	—	—
Bebo	1251	—	—
Behavioral Upload/Download See note on page 9.	127	—	—
Binary over HTTP	1042	—	—
Call Of Duty	1127	—	—
CCcam-Traffic	1129	—	—
CCTV_Video_Stream_UDP	1141	—	—
ChatON	1249	—	—
CloudMe	1255	—	—
CUWorld	117	—	—
Citrix	1104	—	—
Club Box	1038	—	—
Daum My People	1231	—	—
Dailymotion	1223	—	—
DHCP	33	—	—

Table 1-3 Signature-Based Protocols (continued)

Protocol Name	ID	TCP Ports	UDP Ports
DHCPv6	1300	—	—
DHT	106	—	—
Dial070 - Smartphone Login	1131	—	—
DNS	47	—	—
eBay	1257	—	—
DingoTel	42	—	—
Facebook HTTP	1262	—	—
Facebook Messenger Chat	1228	—	—
Facebook Over HTTPS	1245	—	—
Facebook Poke	1245	—	—
Facebook Video Record	1163	—	—
FIX	1113	—	—
FTP	4	21	—
Flash	2033	—	—
Flash MySpace	2035	—	—
Flash Yahoo	2036	—	—
Flash YouTube	2034	—	—
FourSquare	1254	—	—
Fring	1052	—	—
FunshionTCP	1144	—	—
FunshionUDP	1145	—	—
GaduGadu	1146	—	—
GBox-Traffic	1132	—	—
Generic P2PSuspected	1143	—	—
Generic Nonestablished TCP See note on page 9.	126	—	—
Gmail Video UDP	1152	—	—
Gmail Video SSL	1153	—	—
GoogleMaps	1258	—	—
Google Call Phone	1164	—	—
Google Talk	1030	—	—
Gmail Video TCP	1151	—	—
GoogleEarth	118	—	—
HootSuite	1261	—	—
GroupMe	1252	—	—
HTTP Browsing	2	80, 8080	—

Table 1-3 Signature-Based Protocols (continued)

Protocol Name	ID	TCP Ports	UDP Ports
HTTP Tunnel	55	—	—
Hopster	115	—	—
ICQ	119	—	—
iMessage	1188	—	—
imap	59	143	143
Instagram	1216	—	—
IRC	62	—	—
iTunes	30	—	—
JustVoIP	1167	—	—
LoveFilm	1212	—	—
IBM Lotus Domino	1198	—	—
Jabber	116	—	—
Kakao Talk	1226	9001	—
LogMeIn	1224	—	—
Minecraft-Gaming	1176	—	—
MMS	6	1755	—
MS Exchange Desktop	1111	—	—
MS Push Mail	1048	—	—
Mobile MMS	46	—	—
MyJabber	1056	—	—
MyPeople Video Call	1171	—	—
MyPeople Voice Over SIP	1170	—	—
Napster	32	—	—
Nateon	1077	—	—
NateonTalk	1234	—	—
NNTP	15	119	—
NetflixNetworking	1139	—	—
NexTV	1173	—	—
Newcamd-Traffic	1130	—	—
NTP	54	—	—
ooVoo	1114	—	—
OpenVPN	1098	—	—
Origin	1222	5222	—
POP3	9	110	—
Put.io	1253		—
QQ	52	—	—

Table 1-3 Signature-Based Protocols (continued)

Protocol Name	ID	TCP Ports	UDP Ports
radius	738	—	—
Rapidshare	1256	80	—
Rift_Tcp	1175	—	—
RTMPS	1103	443	—
RTSP Streaming	5	554, 1554, 7070	—
RayV	1112	—	—
Saavn	1229	—	—
SD Gundam Capsule Fighter Online	1197	—	—
SkyDrive	1225	—	—
SMTP	8	25	—
Soundcloud_HTTPS	1230	—	—
Snapchat	1271	—	—
SocialCam	1273	—	—
SSDP	53	—	—
SSL	1100	—	—
Steam	1097	—	—
STUN	114	—	—
Second Life	1060	—	—
Shareman-download	1172	—	—
SkeedReceiver	1109	—	—
Skype Video	1168	—	—
Sling	112	—	—
Starcraft2-Gaming	1174	—	—
Street Fighter IV	1101	—	—
SVTPlay	1140	—	—
Talkray	1266	—	—
Tango Video Calls	1166	—	—
Temp Gmail Video TCP	1161	—	—
Temp Gmail Video SSL	1162	—	—
Teredo	1210	—	—
tftp	60	69	69
Ubuntuone	1232	—	—
UC	48	—	—
Ustream	1136	—	—
Utagoe UGLive2	1108	—	—

Table 1-3 Signature-Based Protocols (continued)

Protocol Name	ID	TCP Ports	UDP Ports
UUSee	1177	—	—
Video over HTTP	1040	—	—
Vopium	1227	—	—
Watchitoo	1247	—	—
WazeGPS	1248	—	—
WebEx	1110	—	—
WeChat	1246	—	—
WhatsApp	1178	443 and 5222	—
WhatsApp Message Count	1301	443 and 5222	—
Windows Update	1107	—	—
WoW-Gaming	1133	—	—
xbox Call Of Duty	1127	—	—
Yahoo Messenger	40	5000–5001	5000–5010
Youku Video	1165	—	—

Note Behavioral Upload/Download—Transactions that have download packet flow characteristics and do not match a more specific signature are classified to this protocol. This protocol applies to downloads both from the network side and from the subscriber side.

Note Generic Non-Established TCP—IPv4 TCP flows that are not established properly (syn-ack is missing) are mapped to this protocol.

Table 1-4 lists the signature-based peer-to-peer protocols.

Table 1-4 Signature-Based Peer-to-Peer Protocols

Protocol Name	ID	TCP Ports	UDP Ports
Adobe Reader Cloud	1250	—	—
Amazon Cloud	1209	—	—
Android Market	1202	—	—
Angle Media	1063	—	—
AntsP2P	113	—	—
BBBroadcast	1058	—	—
BBC iPlayer	1057	—	—
BaiBao	43	—	—
Behavioral P2P	2044	—	—
BitTorrent	24	6881–6889	—

Table 1-4 Signature-Based Peer-to-Peer Protocols (continued)

Protocol Name	ID	TCP Ports	UDP Ports
Carbonite	1272	—	—
Cubby	1270	—	—
Dijjer	120	—	—
DirectConnect	19	411–413	—
Dropbox	1180		
Einy	1102	—	—
EmuleEncrypted	105	—	—
Entropy	125	—	—
Exosee	121	—	—
FastTrack KaZaA File Transfer	14	—	—
FastTrack KaZaA Networking	13	1214	—
Feidian	1037	—	—
Filetopia	31	—	—
Freenet	107	—	—
Furthur	123	—	—
Gnutella File Transfer	12	—	—
Gnutella Networking	11	6346–6349	—
Hotline	20	—	—
Hotspot Shield	1269	—	—
Joost	1046	—	—
Justcloud	1265	—	—
Kontiki	124	—	—
KuGoo	1050	—	—
LottoFile	1095	—	—
Manolito	22	—	—
MEGA	1268	—	—
Monkey3	1096	—	—
Mute	34	—	—
NeoNet	37	—	—
NodeZilla	35	—	—
POCO	51	—	—
PPLive	44	—	—
PPStream	49	—	—
PacketiX	1059	—	—
Pando	1049	—	—
Pandora	1138	—	—

Table 1-4 Signature-Based Peer-to-Peer Protocols (continued)

Protocol Name	ID	TCP Ports	UDP Ports
Pandora Audio	1137	—	—
PeerEnabler	122	—	—
QQ-Live	2032	—	—
Rodi	111	—	—
Share	27	—	—
SkeedReceiver	1109	—	—
SopCast	1064	—	—
Soulseek	29	—	—
TVAnts	109	—	—
Thunder	50	—	—
Utagoe UGLive2	1108	—	—
Warez/FileCroc	39	—	—
Waste	36	—	—
WebThunder	1055	—	—
WinMX/OpenNap	16	6257, 6699	6257
Winny	17	7742–7745, 7773	—
Zattoo	1047	—	—
eDonkey	18	4661–4665, 4672–4673, 4711, 5662, 5773, 5783	4661–4665, 4672–4673, 4711, 5662, 5773, 5783
guruguru	66	—	—
kuro	67	—	—
soribada	69	—	—
v-share	71	—	—

Table 1-5 lists the signature-based VoIP protocols.

Table 1-5 Signature-Based VoIP Protocols

Protocol Name	ID	TCP Ports	UDP Ports
Alicall Callback	1156	—	—
Alicall Control (TCP/UDP call)	1158	—	—
Alicall TCP Login	1155	—	—
Alicall UDP	1154	—	—
Behavioral VoIP	1062	—	—
DAUM	1150	—	—
Dial070 - Smartphone Voice	1118	—	—
Fring VoIP	1053	—	—

Table 1-5 Signature-Based VoIP Protocols (continued)

Protocol Name	ID	TCP Ports	UDP Ports
Gmail VoIP SSL	1160	—	—
Gmail VoIP TCP	1159	—	—
Google Voice	1099	—	—
Headcall	1142	—	—
H323	28	1720	—
Hyves	1200	—	—
ICQ VoIP	110	—	—
JaJah YahooPhoneOut	1126	—	—
MGCP	38	—	2427, 2727
MSN Messenger VoIP	1054	—	—
Mumble	1208	—	—
Net2phone	1135	—	—
ooVoo Voice	1115	—	—
PTT Winphoria	61	—	—
Primus	108	—	—
RTP	57	—	—
SIP	23	5060–5061	5060–5061
Skinny	41	—	—
Skype	25	—	—
Skype-IM (V5.8)	1199	—	—
UUCall	1134	—	—
Viber over TCP	1147	—	—
Viber over UDP	1148	—	—
Vivox	1061	—	—
Yahoo Messenger Call Setup	1149	—	—
Yahoo Messenger VoIP	45	—	—
Yahoo VoIP over SIP	2039	—	—

Note The protocols ICQ VoIP, Primus, SIP, and Yahoo VoIP over SIP are also signature-based SIP protocols.

IP Protocols

Table 1-6 lists the IP protocols supported by Cisco SCA BB.

Table 1-6 IP Protocols

IP Protocol Number	Protocol Name	Protocol ID
0	HOPOPT	756
1	ICMP	757
2	IGMP	758
3	GGP	759
4	IP	760
5	ST	761
6	Generic TCP	0
7	CBT	762
8	EGP	763
9	IGP	764
10	BBN-RCC-MON	765
11	NVP-II	766
12	PUP	767
13	ARGUS	768
14	EMCON	769
15	XNET	770
16	CHAOS	771
17	Generic UDP	1
18	MUX	772
19	DCN-MEAS	773
20	HMP	774
21	PRM	775
22	XNS-IDP	776
23	TRUNK-1	777
24	TRUNK-2	778
25	LEAF-1	779
26	LEAF-2	780
27	RDP	781
28	IRTP	782
29	ISO-TP4	783
30	NETBLT	784
31	MFE-NSP	785
32	MERIT-INP	786
33	SEP	787
34	3PC	788
35	IDPR	789

Table 1-6 IP Protocols (continued)

IP Protocol Number	Protocol Name	Protocol ID
36	XTP	790
37	DDP	791
38	IDPR-CMTP	792
39	TP++	793
40	IL	794
41	IPv6-Over-IPv4	795
42	SDRP	796
43	IPv6-Route	797
44	IPv6-Frag	798
45	IDRP	799
46	RSVP	800
47	GRE	801
48	MHRP	802
49	BNA	803
50	ESP	804
51	AH	805
52	I-NLSP	806
53	SWIPE	807
54	NARP	808
55	MOBILE	809
56	TLSP	810
57	SKIP	811
58	IPv6-ICMP	812
59	IPv6-NoNxt	813
60	IPv6-Opts	814
61	any host internal protocol	815
62	CFTP	816
63	any local network	817
64	SAT-EXPAK	818
65	KRYPTOLAN	819
66	RVD	820
67	IPPC	821
68	any distributed file system	822
69	SAT-MON	823
70	VISA	824
71	IPCV	825

Table 1-6 IP Protocols (continued)

IP Protocol Number	Protocol Name	Protocol ID
72	CPNX	826
73	CPHB	827
74	WSN	828
75	PVP	829
76	BR-SAT-MON	830
77	SUN-ND	831
78	WB-MON	832
79	WB-EXPAK	833
80	ISO-IP	834
81	VMTP	835
82	SECURE-VMTP	836
83	VINES	837
84	TTP	838
85	NSFNET-IGP	839
86	DGP	840
87	TCF	841
88	EIGRP	842
89	OSPFIGP	843
90	Sprite-RPC	844
91	LARP	845
92	MTP	846
93	AX.25	847
94	IPIP	848
95	MICP	849
96	SCC-SP	850
97	ETHERIP	851
98	ENCAP	852
99	any private encryption scheme	853
100	GMTP	854
101	IFMP	855
102	PNNI	856
103	PIM	857
104	ARIS	858
105	SCPS	859
106	QNX	860
107	A/N	861

Table 1-6 IP Protocols (continued)

IP Protocol Number	Protocol Name	Protocol ID
108	IPComp	862
109	SNP	863
110	Compaq-Peer	864
111	IPX-in-IP	865
112	VRRP	866
113	PGM	867
114	any 0-hop protocol	868
115	L2TP	869
116	DDX	870
117	IATP	871
118	STP	872
119	SRP	873
120	UTI	874
121	SMP	875
122	SM	876
123	PTP	877
124	ISIS	878
125	FIRE	879
126	CRTP	880

Port-Based Protocols

Table 1-7 lists the TCP/UDP port-based protocols defined in the Cisco SCA BB default service configuration.

Table 1-7 Port-Based Protocols

Protocol Name	ID	TCP Ports	UDP Ports
FTP	4	21	—
Gnutella Networking	11	6346–6349	—
FastTrack KaZaA Networking	13	1214	—
Bittorrent	24	6881–6889	—
NTP	54	123	123
epmap	128	135	135
profile	129	136	136
netbios-ns	130	137	137
netbios-dgm	131	138	138

Table 1-7 Port-Based Protocols (continued)

Protocol Name	ID	TCP Ports	UDP Ports
netbios-ssn	132	139	139
emfis-data	133	140	140
emfis-cntl	134	141	141
bl-idm	135	142	142
uma	137	144	144
uaac	138	145	145
iso-tp0	139	146	146
iso-ip	140	147	147
jargon	141	148	148
aed-512	142	149	149
sql-net	143	150	150
hems	144	151	151
bftp	145	152	152
sgmp	146	153	153
netsc-prod	147	154	154
netsc-dev	148	155	155
sqlsrv	149	156	156
knet-cmp	150	157	157
nss-routing	152	159	159
sgmp-traps	153	160	160
snmp	154	161	161
snmptrap	155	162	162
cmip-man	156	163	163
cmip-agent	157	164	164
xns-courier	158	165	165
s-net	159	166	166
namp	160	167	167
rsvd	161	168	168
send	162	169	169
print-srv	163	170	170
multiplex	164	171	171
cl/1	165	172	172
xyplex-mux	166	173	173
mailq	167	174	174
vmnet	168	175	175
genrad-mux	169	176	176

Table 1-7 Port-Based Protocols (continued)

Protocol Name	ID	TCP Ports	UDP Ports
xdmcp	170	177	177
nextstep	171	178	178
bgp	172	179	179
ris	173	180	180
unify	174	181	181
audit	175	182	182
ocserver	177	184	184
remote-kis	178	185	185
kis	179	186	186
aci	180	187	187
mumps	181	188	188
qft	182	189	189
gacp	183	190	190
prospero	184	191	191
osu-nms	185	192	192
srmp	186	193	193
IRC	187	194, 6665-6669	194, 6665-6669
dn6-nlm-aud	188	195	195
dn6-smm-red	189	196	196
dls	190	197	197
dls-mon	191	198	198
smux	192	199	199
src	193	200	200
at-rtmp	194	201	201
at-nbp	195	202	202
at-3	196	203	203
at-echo	197	204	204
at-5	198	205	205
at-zis	199	206	206
at-7	200	207	207
at-8	201	208	208
qmtp	202	209	209
z39.50	203	210	210
914c/g	204	211	211
anet	205	212	212
ipx	206	213	213

Table 1-7 Port-Based Protocols (continued)

Protocol Name	ID	TCP Ports	UDP Ports
vmpwscs	207	214	214
softpc	208	215	215
CAIlic	209	216	216
dbase	210	217	217
mpp	211	218	218
uarps	212	219	219
imap3	213	220	220
fln-spx	214	221	221
rsh-spx	215	222	222
cdc	216	223	223
masqdialer	217	224	224
direct	218	242	242
sur-meas	219	243	243
inbusiness	220	244	244
link	221	245	245
dsp3270	222	246	246
bhfhs	224	248	248
set	225	257	257
yak-chat	226	258	258
esro-gen	227	259	259
openport	228	260	260
nsiiops	229	261	261
arcisdms	230	262	262
hdap	231	263	263
bgmp	232	264	264
x-bone-ctl	233	265	265
sst	234	266	266
td-service	235	267	267
td-replica	236	268	268
http-mgmt	237	280	280
personal-link	238	281	281
cableport-ax	239	282	282
rescap	240	283	283
corerjd	241	284	284
fxp-1	242	286	286
k-block	243	287	287

Table 1-7 Port-Based Protocols (continued)

Protocol Name	ID	TCP Ports	UDP Ports
novastorbakcup	244	308	308
entrusttime	245	309	309
bhmds	246	310	310
asip-webadmin	247	311	311
vslmp	248	312	312
magenta-logic	249	313	313
opalis-robot	250	314	314
dpsi	251	315	315
decauth	252	316	316
zannet	253	317	317
pkix-timestamp	254	318	318
ptp-event	255	319	319
ptp-general	256	320	320
pip	257	321	321
rtsps	258	322	322
texar	259	333	333
pdap	260	344	344
pawserv	261	345	345
zserv	262	346	346
fatserv	263	347	347
csi-sgwp	264	348	348
mftp	265	349	349
matip-type-a	266	350	350
matip-type-b	267	351	351
dtag-ste-sb	268	352	352
ndsauth	269	353	353
bh611	270	354	354
datex-asn	271	355	355
cloanto-net-1	272	356	356
bhevent	273	357	357
shrinkwrap	274	358	358
nsrmp	275	359	359
scoi2odialog	276	360	360
semantix	277	361	361
srssend	278	362	362
rsvp_tunnel	279	363	363

Table 1-7 Port-Based Protocols (continued)

Protocol Name	ID	TCP Ports	UDP Ports
aurora-cmgr	280	364	364
dtk	281	365	365
odmr	282	366	366
mortgageware	283	367	367
qbikgdp	284	368	368
rpc2portmap	285	369	369
codaauth2	286	370	370
clearcase	287	371	371
ulistproc	288	372	372
legent-1	289	373	373
legent-2	290	374	374
hassle	291	375	375
nip	292	376	376
tnETOS	293	377	377
dsETOS	294	378	378
is99c	295	379	379
is99s	296	380	380
hp-collector	297	381	381
hp-managed-node	298	382	382
hp-alarm-mgr	299	383	383
arns	300	384	384
ibm-app	301	385	385
asa	302	386	386
aurp	303	387	387
unidata-ldm	304	388	388
ldap	305	—	389
uis	306	390	390
synotics-relay	307	391	391
synotics-broker	308	392	392
meta5	309	393	393
embl-ndt	310	394	394
netware-ip	311	396	396
mptn	312	397	397
kryptolan	313	398	398
iso-tsap-c2	314	399	399
work-sol	315	400	400

Table 1-7 Port-Based Protocols (continued)

Protocol Name	ID	TCP Ports	UDP Ports
ups	316	401	401
genie	317	402	402
decap	318	403	403
nced	319	404	404
ncld	320	405	405
imsp	321	406	406
timbuktu	322	407	407
prm-sm	323	408	408
prm-nm	324	409	409
decladebug	325	410	410
rmt	326	—	411
synoptics-trap	327	—	412
smsp	328	—	413
infoseek	329	414	414
bnet	330	415	415
silverplatter	331	416	416
onmux	332	417	417
hyper-g	333	418	418
ariel1	334	419	419
smpte	335	420	420
ariel2	336	421	421
ariel3	337	422	422
opc-job-start	338	423	423
opc-job-track	339	424	424
icad-el	340	425	425
smartsdp	341	426	426
svrloc	342	427	427
ocs_cmu	343	428	428
ocs_amu	344	429	429
utmpsd	345	430	430
utmpcd	346	431	431
iasd	347	432	432
nnsp	348	433	433
mobileip-agent	349	434	434
mobilip-mn	350	435	435
dna-cml	351	436	436

Table 1-7 Port-Based Protocols (continued)

Protocol Name	ID	TCP Ports	UDP Ports
comscm	352	437	437
dsfgw	353	438	438
dasp	354	439	439
sgcp	355	440	440
decvms-sysmgt	356	441	441
cvc_hostd	357	442	442
https	358	443	—
snpp	359	444	444
microsoft-ds	360	445	445
ddm-rdb	361	446	446
ddm-dfm	362	447	447
ddm-ssl	363	448	448
as-servermap	364	449	449
tserver	365	450	450
sfs-smp-net	366	451	451
sfs-config	367	452	452
creativeserver	368	453	453
contentserver	369	454	454
creativepartnr	370	455	455
scohelp	371	457	457
appleqtc	372	458	458
ampr-rcmd	373	459	459
skronk	374	460	460
datasurfsrv	375	461	461
datasurfsrvsec	376	462	462
alpes	377	463	463
kpasswd	378	464	464
url-rendezvous	379	465	465
digital-vrc	380	466	466
mylex-mapd	381	467	467
photuris	382	468	468
rcp	383	469	469
scx-proxy	384	470	470
mondex	385	471	471
ljk-login	386	472	472
hybrid-pop	387	473	473

Table 1-7 Port-Based Protocols (continued)

Protocol Name	ID	TCP Ports	UDP Ports
tn-tl-w1	388	474	
tn-tl-w2	389	—	474
tn-tl-fd1	390	476	476
ss7ns	391	477	477
spsc	392	478	478
iafserver	393	479	479
iafdbase	394	480	480
ph	395	481	481
bgs-nsi	396	482	482
ulpnet	397	483	483
integra-sme	398	484	484
powerburst	399	485	485
avian	400	486	486
saft	401	487	487
gss-http	402	488	488
nest-protocol	403	489	489
micom-pfs	404	490	490
go-login	405	491	491
ticf-1	406	492	492
ticf-2	407	493	493
pov-ray	408	494	494
intecourier	409	495	495
pim-rp-disc	410	496	496
dantz	411	497	497
siam	412	498	498
iso-ill	413	499	499
isakmp	414	500, 4500	500, 4500
stmf	415	501	501
asa-appl-proto	416	502	502
intrinsa	417	503	503
citadel	418	504	504
mailbox-lm	419	505	505
ohimsrv	420	506	506
crs	421	507	507
xvttp	422	508	508
snare	423	509	509

Table 1-7 Port-Based Protocols (continued)

Protocol Name	ID	TCP Ports	UDP Ports
fcp	424	510	510
passgo	425	511	511
exec	426	512	—
biff	427	—	512
login	428	513	—
who	429	—	513
shell	430	514	—
syslog	431	—	514
printer	432	515	515
videotex	433	516	516
talk	434	517	517
ntalk	435	518	518
utime	436	519	519
efs	437	520	—
router	438	—	520
ripng	439	521	521
ulp	440	522	522
ibm-db2	441	523	523
ncp	442	524	524
timed	443	525	525
tempo	444	526	526
stx	445	527	527
custix	446	528	528
irc-serv	447	529	529
courier	448	530	530
conference	449	531	531
netnews	450	432	432
netwall	451	533	533
mm-admin	452	534	534
iiop	453	535	535
opalis-rdv	454	536	536
nmsp	455	537	537
gdomap	456	538	538
apertus-ldp	457	539	539
uucp	458	540	540
uucp-rlogin	459	541	541

Table 1-7 Port-Based Protocols (continued)

Protocol Name	ID	TCP Ports	UDP Ports
commerce	460	542	542
klogin	461	543	543
kshell	462	544	544
appleqtcsrvr	463	545	545
dhcpv6-client	464	546	546
dhcpv6-server	465	547	547
idfp	466	549	549
new-rwho	467	550	550
cybercash	468	551	551
deviceshare	469	552	552
pirp	470	553	553
remotefs	471	556	556
openvms-sysipc	472	557	557
sdnskmp	473	558	558
teedtap	474	559	559
rmonitor	475	560	560
monitor	476	561	561
chshell	477	562	562
nntps	478	563	563
9pfs	479	564	564
whoami	480	565	565
streettalk	481	566	566
banyan-rpc	482	567	567
ms-shuttle	483	568	568
ms-rome	484	569	569
meter	485	570–571	570–571
sonar	486	572	572
banyan-vip	487	573	573
ftp-agent	488	574	574
vemmi	489	575	575
vnas	491	577	577
ipdd	492	578	578
decbsrv	493	579	579
sntp-heartbeat	494	580	580
bdp	495	581	581
scc-security	496	582	582

Table 1-7 Port-Based Protocols (continued)

Protocol Name	ID	TCP Ports	UDP Ports
philips-vc	497	583	583
keyserver	498	584	584
imap4-ssl	499	585	585
password-chg	500	586	586
submission	501	587	587
cal	502	588	588
eyelink	503	589	589
tns-cml	504	590	590
http-alt	505	591	591
eudora-set	506	592	592
http-rpc-epmap	507	593	593
tpip	508	594	594
cab-protocol	509	595	595
smsd	510	596	596
ptcnameservice	511	597	597
sco-websrvrmg3	512	598	598
acp	513	599	599
ipcserver	514	600	600
urm	515	606	606
nqs	516	607	607
sift-uft	517	608	608
npmp-trap	518	609	609
npmp-local	519	610	610
npmp-gui	520	611	611
hmmp-ind	521	612	612
hmmp-op	522	613	613
sshell	523	614	614
sco-inetmgr	524	615	615
sco-sysmgr	525	616	616
sco-dtmgr	526	617	617
dei-icda	527	618	618
digital-evm	528	619	619
sco-websrvrmgr	529	620	620
escp-ip	530	621	621
collaborator	531	622	622
aux_bus_shunt	532	623	623

Table 1-7 Port-Based Protocols (continued)

Protocol Name	ID	TCP Ports	UDP Ports
cryptoadmin	533	624	624
dec_dlm	534	625	625
asia	535	626	626
passgo-tivoli	536	627	627
qmqp	537	628	628
3com-amp3	538	629	629
rda	539	630	630
ipp	540	631	631
bmpp	541	632	632
servstat	542	633	633
ginad	543	634	634
rlzdbase	544	635	635
ldaps	545	636	636
lanserver	546	637	637
mcns-sec	547	638	638
msdp	548	639	639
entrust-sps	549	640	640
repcmd	550	641	641
esro-emsdp	551	642	642
sanity	552	643	643
dwr	553	644	644
pssc	554	645	645
ldp	555	646	646
dhcp-failover	556	647	647
rrp	557	648	648
aminet	558	649	659
obex	559	650	650
ieee-mms	560	651	651
hello-port	561	652	652
repscmd	562	653	653
aodv	563	654	654
tinc	564	655	655
spmp	565	656	656
rmc	566	657	657
tenfold	567	658	658
mac-srvr-admin	568	660	660

Table 1-7 Port-Based Protocols (continued)

Protocol Name	ID	TCP Ports	UDP Ports
hap	569	661	661
pftp	570	662	662
purenoise	571	663	663
secure-aux-bus	572	664	664
sun-dr	573	665	665
doom	574	666	666
disclose	575	667	667
mecomm	576	668	668
meregister	577	669	669
vacdsm-sws	578	670	670
vacdsm-app	579	671	671
vpps-qua	580	672	672
cimplex	581	673	673
acap	582	674	674
dctp	583	675	675
vpps-via	584	676	676
vpp	585	677	677
ggf-ncp	586	678	678
mrm	587	679	679
entrust-aaas	588	680	680
entrust-aams	589	681	681
xfr	590	682	682
corba-iiop	591	683	683
corba-iiop-ssl	592	684	684
mdc-portmapper	593	685	685
hcp-wismar	594	686	686
asipregistry	595	687	687
realm-rusd	596	688	688
nmap	597	689	689
vatp	598	690	690
msexch-routing	599	691	691
hyperwave-isp	600	692	692
connendp	601	693	693
ha-cluster	602	694	694
ieee-mms-ssl	603	695	695
rushd	604	696	696

Table 1-7 Port-Based Protocols (continued)

Protocol Name	ID	TCP Ports	UDP Ports
uuidgen	605	697	697
olsr	606	698	698
accessnetwork	607	699	699
elcsd	608	704	704
agentx	609	705	705
silc	610	706	706
borland-dsj	611	707	707
entrust-kmsh	612	709	709
entrust-ash	613	710	710
cisco-tdp	614	711	711
netviewdm1	615	729	729
netviewdm2	616	730	730
netviewdm3	617	731	731
netgw	618	741	741
netrcs619	619	742	742
flexlm	620	744	744
fujitsu-dev	621	747	747
ris-cm	622	748	748
kerberos-adm	623	749	749
rfile	624	750	—
kerberos-iv	625	—	750
pump	626	751	751
qrh	627	752	752
rrh	628	753	753
tell	629	754	754
nlogin	630	758	758
con	631	759	759
ns	632	760	760
rxe	633	761	761
quotad	634	762	762
cycleserv	635	763	763
omserv	636	764	764
webster	637	765	765
phonebook	638	767	767
vid	639	769	769
cadlock	640	770	770

Table 1-7 Port-Based Protocols (continued)

Protocol Name	ID	TCP Ports	UDP Ports
rtip	641	771	771
cycleserv2	642	772	772
submit	643	773	—
notify	644	—	773
rpasswd	645	774	—
acmaint_dbd	646	—	774
entomb	647	775	—
acmaint_transd	648	—	775
wpages	649	776	776
multiling-http	650	777	777
wpgs	651	780	780
concert	652	786	786
qsc	653	—	787
mdbs_daemon	654	800	800
device	655	801	801
itm-mcell-s	656	828	828
pkix-3-ca-ra	657	829	829
dhcp-failover2	658	847	847
rsync	659	873	873
iclcnet-locate	660	886	886
iclcnet_svinfo	661	887	887
accessbuilder	662	888	888
omginitialrefs	663	900	900
smpnameres	664	901	901
ideafarm-chat	665	902	902
ideafarm-catch	666	903	903
xact-backup	667	911	911
ftps-data	668	989	989
ftps	669	990	990
nas	670	991	991
telnets	671	992	992
imaps	672	993	993
ircs	673	994	994
pop3s	674	995	995
vsinet	675	996	996
maitrd	676	997	997

Table 1-7 Port-Based Protocols (continued)

Protocol Name	ID	TCP Ports	UDP Ports
busboy	677	998	—
puparp	678	—	998
garcon	679	999	—
applix	680	—	999
surf	681	1010	1010
rmiactivation	682	1098	1098
rmiregistry	683	1099	1099
ms-sql-s	684	1433	1433
oracle	690	1521	1521
orasrv	691	1525	1525
tlisrv	692	1527	1527
coauthor	693	1529	1529
rdb-dbs-disp	694	1571	1571
oraclenames	695	1575	1575
oraclenet8cman	696	1630	1630
net8-cman	697	1830	1830
ms-olap	686	2382–2383, 2393–2394	2382–2383, 2393–2394
msft-gc	687	3268	3268
msft-gc-ssl	688	3269	3269
citrixima	698	2512	2512
citrixadmin	699	2513	2513
citrix-rtmp	700	2897	2897
citriximaclient	701	2598	2598
micromuse-lm	702	1534	1534
orbixd	703	1570	1570
orbix-locator	704	3075	3075
orbix-config	705	3076	3076
orbix-loc-ssl	706	3077	3077
shockwave	707	1626	1626
sitaraserver	708	2629	2629
sitaramgmt	709	2630	2630
sitaradir	710	2631	2631
mysql	711	3306	3306
msnp	713	1836	1826
aim	714	5190–5193	—
groove	715	2492	2492

Table 1-7 Port-Based Protocols (continued)

Protocol Name	ID	TCP Ports	UDP Ports
directplay	716	2234	2234
directplay8	717	6073	6073
kali	718	2213	2213
worldfusion	719	2595–2596	2595–2596
directv-web	720	3334	3334
directv-soft	721	3335	3335
directv-tick	722	3336	3336
directv-catlg	723	3337	3337
wta-wsp-s	724	2805	2805
wap-push	725	2948	2948
wap-pushsecure	726	2949	2949
wap-push-http	727	4035	4035
wap-push-https	728	4036	4036
game-spy	755	6500, 28900	6515, 27900
ibprotocol	737	6714	6714
wap-wsp	729	9200	9200
wap-wsp-wtp	730	9201	9201
wap-wsp-s	731	9202	9202
wap-wsp-wtp-s	732	9203	9203
wap-vcard	733	9204	9204
wap-vcal	734	9205	9205
wap-vcard-s	735	9206	9206
wap-vcal-s	736	9207	9207
pptp	739	1723	1723
gtp-user	740	2152	2152
xdtp	741	3088	3088
l2tp	742	1701	1701
fsgs	743	6112	6112
parsec-game	744	6582	6582
UnReal_UT	745	—	7777-7783
SiN	746	22450	22450
halflife	747	—	27015
tribes	748	28001	28001
Heretic II	749	28910	—
starsiege	750	—	29001–29009
game-search	751	29001	—

Table 1-7 Port-Based Protocols (continued)

Protocol Name	ID	TCP Ports	UDP Ports
KingPin	752	31510	31510
runescape	753	43594	—
GLT Poliane	882	1201	—
MSN Messenger	883	1863	1863
xbox live	898	3074	3074
ps2	899	10070–10080	10070
compressnet	900	2–3	2–3
rje	901	5	5
echo	902	7	7
discard	903	9	9
systat	904	11	11
daytime	905	13	13
qotd	906	17	17
msp	907	18	18
chargen	908	19	19
ftp-data	909	20	20
ssh	910	22	22
telnet	911	23	23
nsw-fe	912	27	27
msg-icp	913	29	29
msg-auth	916	31	31
dsp	917	33	33
time	918	37	37
rap	919	38	38
rlp	920	39	39
graphics	921	41	41
name	922	42	42
nicname	923	43	43
mpm-flags	924	44	44
mpm	925	45	45
mpm-snd	926	46	46
ni-ftp	927	47	47
auditd	928	48	48
tacacs	929	49	49
re-mail-ck	930	50	50
la-maint	931	51	51

Table 1-7 Port-Based Protocols (continued)

Protocol Name	ID	TCP Ports	UDP Ports
xns-time	932	52	52
xns-ch	934	54	54
isi-gl	935	55	55
xns-auth	936	56	56
xns-mail	937	58	58
ni-mail	938	61	61
acas	939	62	62
whois	940	63	63
covia	941	64	64
tacacs-ds	942	65	65
sql*net	943	66	66
bootps	944	67	67
bootpc	945	68	68
gopher	947	70	70
netrjs-1	948	71	71
netrjs-2	949	72	72
netrjs-3	950	73	73
netrjs-4	951	74	74
deos	952	76	76
finger	953	79	79
hosts2-ns	954	81	81
xfer	955	82	82
mit-ml-dev	956	83, 85	83, 85
ctf	957	84	84
mfcobol	958	86	86
kerberos	959	88	88
su-mit-tg	960	89	89
dnsix	961	90	90
mit-dov	962	91	91
npp	963	92	92
dcp	964	93	93
objcall	965	94	94
supdup	966	95	95
dixie	967	96	96
swift-rvf	968	97	97
tacnews	969	98	98

Table 1-7 Port-Based Protocols (continued)

Protocol Name	ID	TCP Ports	UDP Ports
metagram	970	99	99
newacct	971	100	—
hostname	972	101	101
iso-tsap	973	102	102
gppitnp	974	103	103
acr-nema	975	104	104
csnet-ns	976	105	105
3com-tsmux	977	106	106
rtelnet	978	107	107
snagas	979	108	108
pop2	980	109	109
sunrpc	981	111	111
mcidas	982	112	112
auth	983	113	113
audionews	984	114	114
sftp	985	115	115
ansanotify	986	116	116
uucp-path	987	117	117
sqlserv	988	118	118
cfdptkt	989	120	120
erpc	990	121	121
smakynet	991	122	122
ansatrader	993	124	124
locus-map	994	125	125
nxedit	995	126	126
locus-con	996	127	127
gss-xlicen	997	128	128
pwdgen	998	129	129
cisco-fna	999	130	130
LapLink	1105	1547	—
SAP	1106	3200,3300,3600	—
cisco-tna	2000	131	131
cisco-sys	2001	132	132
statsrv	2002	133	133
ingres-net	2003	134	134
Anarchy	2004	7013, 7500–7501	7013, 7500–7501

Table 1-7 Port-Based Protocols (continued)

Protocol Name	ID	TCP Ports	UDP Ports
Asherons Call	2005	9000–9013	9000–9013
Black And White	2006	2611–2612	—
Counter strike	2007	27020–27039	1200, 27000–27018
Dark Reign	2008	26214	26214
Diablo	2009	6113–6119, 4000	6113–6119
Elite Force	2010	—	26000, 27500
F16	2011	—	3862, 3863
F22 Simulator (lightning 3)	2012	—	3874–3875, 4533, 4534
Hexen	2013	—	26900
Kohan Immortal Sovereigns	2014	3855, 17437	3855, 17437
Motorhead	2015	16000, 16010–16030	16000, 16010–16030
Myth	2016	3453	3453
Need For Speed	2017	9442	9442
Need For Speed 3	2018	1030	1030
Operation Flash Point	2019	47624	—
Outlaws	2020	5310	5310
Swat3	2021	16639	16638
Ultima	2022	5002–5010,7775–7777, 8888, 9999, 7875	—
Warcraft	2023	3724	3724
Znes	2024	—	7845
Delta Force	2025	3100, 3999	3100, 3999, 3568, 3569
Rainbox six	2026	2346	2346
Soldier of fortune	2027	—	28911–28915
Westwood Online	2028	1140, 1234	1140, 1234
Yahoo Games	2029	11999	—
Konspire2b	2031	6085	6085

Protocols Identified on Unidirectional Flows

When unidirectional classification is enabled, the protocols listed in Table 1-8 can be detected on unidirectional flows.

- When a unidirectional flow (inbound or outbound) passes through the SCE platform, it is matched against this set of protocol signatures.
- When a bidirectional flow passes through the SCE platform, the protocol library tries to match it to one of its standard (bidirectional) protocol signatures.

Table 1-8 Unidirectionally Detected Protocols

Protocol Name	Protocol ID
AntsP2P	113
Audio over HTTP	1041
BBC iPlayer	1057
BaiBao	43
Baidu Movie	1043
Behavioral Upload/Download	127
Binary over HTTP	1042
BitTorrent	24
Citrix	1104
CUWorld	117
Club Box	1038
Dijjer	120
Dial070 - Smartphone Login	1131
Dial070 - Smartphone Voice	1118
DingoTel	42
DirectConnect	19
EmuleEncrypted	105
Entropy	125
Exosee	121
FastTrack KaZaA File Transfer	14
Feidian	1037
Filetopia	31
Flash	2033
Flash MySpace	2035
Flash Yahoo	2036
Flash YouTube	2034
Fring	1052
FunshionTCP	1144
Furthur	123

Table 1-8 Unidirectionally Detected Protocols (continued)

Protocol Name	Protocol ID
Generic IPv6	1196
Generic TCP	0
Gnutella File Transfer	12
Gnutella Networking	11
Google Talk	1030
GoogleEarth	118
HTTP Browsing	2
HTTP Tunnel	55
Hopster	115
Hotline	20
ICQ	119
Jabber	116
Joost	1046
Kontiki	124
LapLink	1105
Location Free	1045
LottoFile	1095
MMS	6
Monkey3	1096
MS Push Mail	1048
MSN Messenger	883
Manolito	22
Mobile MMS	46
Mute	34
Napster	32
NeoNet	37
Net2phone	1135
NodeZilla	35
ooVoo	1114
Pandora	1138
POCO	51
POP3	9
PPLive	44
PPStream	49
Pando	1049
PeerEnabler	122

Table 1-8 Unidirectionally Detected Protocols (continued)

Protocol Name	Protocol ID
QQ-Live	2032
SMTP	8
Skype	25
Sling	112
TVAnts	109
Thunder	50
Tor and Orbot	1065
UC	48
Viber over TCP	1147
Video over HTTP	1040
Warez/FileCroc	39
WebThunder	1055
WinMX/OpenNap	16
Winny	17
Yahoo Messenger	40
Yahoo Messenger VoIP	45
Zattoo	1047
eDonkey	18
guruguru	66
iTunes	30
imap	59
soribada	69
v-share	71

Services

Services are the building blocks of service configurations. Classification of a transaction to a service determines the accounting and control that apply to the corresponding transaction. Services are organized in an hierarchal structure used for both accounting and control.

Table 1-9 lists the services defined in the default service configuration. Two service usage counters, Global Usage Counter and Subscriber Usage Counter, are used to accumulate information about the transactions classified under each service. Both these counter have the same name.

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

Table 1-9 Installed Services

Name	ID	Name of Parent Service	Global Usage Counter and Subscriber Usage Counter
Default Service	0		Default Service*
Browsing	7	Default Service	Global: Default Service*, Subscriber: Browsing*
ClickStream-New Page	118	Browsing	Global: HTTP, Subscriber: Browsing*
ClickStream-New Site	119	Browsing	Global: HTTP, Subscriber: Browsing*
HTTP	16	Browsing	Global: HTTP, Subscriber: Browsing*
HTTPS	17	Browsing	Global: HTTPS, Subscriber: Browsing*
Location Based Services	48	Browsing	Global: Location Based Services, Subscriber: Browsing*
Social Sites	104	Browsing	Default Service*
Facebook	105	Social Sites	Global: Default Service*, Subscriber: Browsing*
MySpace	107	Social Sites	Global: Default Service*, Subscriber: Browsing*
Twitter	106	Social Sites	Global: Default Service*, Subscriber: Browsing*
Other Social Sites	108	Social Sites	Global: Default Service*, Subscriber: Browsing*
E-Mail	4	Default Service	E-Mail*
IMAP	23	E-Mail	Global: IMAP, Subscriber: E-Mail*
MS Exchange Desktop	110	E-Mail	Global: MS Exchange Desktop , Subscriber: E-Mail*
MS Push Mail	47	E-Mail	Global: MS Push Mail, Subscriber: E-Mail*
POP3	21	E-Mail	Global: POP3, Subscriber: E-Mail*
SMTP	22	E-Mail	Global: SMTP, Subscriber: E-Mail*
Web-Based E-Mail	71	E-Mail	Global: Web-Based E-Mail, Subscriber: E-Mail*
File Sharing	49	Default Service	Default Service*

Table 1-9 Installed Services (continued)

Name	ID	Name of Parent Service	Global Usage Counter and Subscriber Usage Counter
Download over HTTP	44	File Sharing	Download over HTTP
FTP	32	File Sharing	FTP
IM File Transfer	51	File Sharing	Global: Default Service*, Subscriber: IM File Transfer*
Google Talk File Transfer	54	IM File Transfer	Global: Google Talk File Transfer, Subscriber: IM File Transfer*
ICQ File Transfer	55	IM File Transfer	Global: ICQ File Transfer, Subscriber: IM File Transfer*
QQ File Transfer	52	IM File Transfer	Global: QQ File Transfer, Subscriber: IM File Transfer*
Skype File Transfer	98	IM File Transfer	Global: Skype File Transfer, Subscriber: IM File Transfer*
Windows Live Messenger File Transfer	57	IM File Transfer	Global: Windows Live Messenger File Transfer, Subscriber: IM File Transfer*
Yahoo Messenger File Transfer	53	Global: Yahoo Messenger File	Global: Yahoo Messenger File Transfer, Subscriber: IM File Transfer*
Other IM File Transfer	56	IM File Transfer	Global: Other IM File Transfer, Subscriber: IM File Transfer*
One-Click Hosting	50	File Sharing	One-Click Hosting
P2P	9	File Sharing	Default Service*
Ares/Warez	58	P2P	Arez/Warez
Bittorrent	24	P2P	Global: Default Service*, Subscriber: Bittorrent*
Bittorrent Over IPv6	116	Bittorrent	Global: Bittorrent Over IPv6, Subscriber: Bittorrent*
Encrypted Bittorrent	62	Bittorrent	Global: Encrypted Bittorrent, Subscriber: Bittorrent*
Non-Encrypted Bittorrent	63	Bittorrent	Global: Non-Encrypted Bittorrent, Subscriber: Bittorrent*
Gnutella	30	P2P	Gnutella
Winny	27	P2P	Winny
eDonkey/eMule	14	P2P	Global: Default Service*, Subscriber: eDonkey/eMule*
Encrypted eMule	60	eDonkey/eMule	Global: Encrypted eMule, Subscriber: eDonkey/eMule*
Non-Encrypted eMule	61	eDonkey/eMule	Global: Non-Encrypted eMule, Subscriber: eDonkey/eMule*
Behavioral P2P	43	P2P	Behavioral P2P
Other P2P	59	P2P	Other P2P

Table 1-9 Installed Services (continued)

Name	ID	Name of Parent Service	Global Usage Counter and Subscriber Usage Counter
Behavioral Upload/Download	39	File Sharing	Behavioral Upload/Download
Gaming	29	Default Service	Global: Default Service*, Subscriber: Gaming*
Nintendo Wii	90	Gaming	Global: Nintendo Wii, Subscriber: Gaming*
PC Gaming	87	Gaming	Global: PC Gaming, Subscriber: Gaming*
Playstation	89	Gaming	Global: Playstation, Subscriber: Gaming*
Xbox	88	Gaming	Global: Xbox, Subscriber: Gaming*
Instant Messaging	28	Default Service	Global: Default Service*, Subscriber: Instant Messaging*
Facebook IM	101	Instant Messaging	Global: HTTP Browsing, Subscriber: Instant Messaging*
Google Talk	83	Instant Messaging	Global: Google Talk, Subscriber: Instant Messaging*
ICQ	85	Instant Messaging	Global: ICQ, Subscriber: Instant Messaging*
Windows Live Messenger	82	Instant Messaging	Global: Windows Live Messenger, Subscriber: Instant Messaging*
Yahoo Messenger	84	Instant Messaging	Global: Yahoo Messenger, Subscriber: Instant Messaging*
Other Instant Messaging	86	Instant Messaging	Global: Other Instant Messaging, Subscriber: Instant Messaging*
Internet Privacy	94	Default Service	Global: Default Service*, Subscriber: Internet Privacy*
Anonimity Networks	95	Internet Privacy	Global: Anonimity Networks, Subscriber: Internet Privacy*
Tunneling	38	Internet Privacy	Global: Tunneling, Subscriber: Internet Privacy*
VPN	41	Internet Privacy	Global: Default Service*, Subscriber: Internet Privacy*
IPSec VPN	42	VPN	Global: IPSec VPN, Subscriber: Internet Privacy*
Internet Video	70	Default Service	Default Service*
Audio and Video over HTTP	76	Internet Video	Audio and Video over HTTP
Commercial Media Distribution	26	Internet Video	Commercial Media Distribution

Table 1-9 Installed Services (continued)

Name	ID	Name of Parent Service	Global Usage Counter and Subscriber Usage Counter
Flash	45	Internet Video	Global: Default Service*, Subscriber: Flash*
Flash MySpace	73	Flash	Global: Flash MySpace, Subscriber: Flash*
Flash Yahoo	75	Flash	Global: Flash Yahoo, Subscriber: Flash*
Flash YouTube	74	Flash	Global: Flash YouTube, Subscriber: Flash*
Other Flash	72	Flash	Global: Other Flash, Subscriber: Flash*
P2P TV	77	Internet Video	Global: Default Service*, Subscriber: P2P TV*
Joost	81	P2P TV	Global: Joost, Subscriber: P2P TV*
PPLive	79	P2P TV	Global: PPLive, Subscriber: P2P TV*
PPStream	80	P2P TV	Global: PPStream, Subscriber: P2P TV*
Other P2P TV	78	P2P TV	Global: Other P2P TV, Subscriber: P2P TV*
Streaming	34	Internet Video	Global: Default Service*, Subscriber: Streaming*
MMS	20	Streaming	Global: MMS, Subscriber: Streaming*
RTMP	99	Streaming	Global: RTMP, Subscriber: Streaming*
RTSP	19	Streaming	Global: RTSP, Subscriber: Streaming*
Net Admin	33	Default Service	Global: Default Service*, Subscriber: Net Admin*
Naming Services	91	Net Admin	Global: Naming Services, Subscriber: Net Admin*
Terminals	92	Net Admin	Global: Terminals, Subscriber: Net Admin*
Other Net Admin	93	Net Admin	Global: Other Net Admin, Subscriber: Net Admin*
Newsgroups	8	Default Service	Newsgroups
Voice and Video Calls	12	Default Service	Global: Default Service*, Subscriber: Voice and Video Calls*
Google Talk VoIP	68	Voice and Video Calls	Global: Google Talk VoIP, Subscriber: Voice and Video Calls*
H323	11	Voice and Video Calls	Global: H323, Subscriber: Voice and Video Calls*
ICQ VoIP	40	Voice and Video Calls	Global: ICQ VoIP, Subscriber: Voice and Video Calls*
MGCP	5	Voice and Video Calls	Global: MGCP, Subscriber: Voice and Video Calls*

Table 1-9 Installed Services (continued)

Name	ID	Name of Parent Service	Global Usage Counter and Subscriber Usage Counter
QQ VoIP	69	Voice and Video Calls	Global: QQ VoIP, Subscriber: Voice and Video Calls*
SIP	10	Voice and Video Calls	Global: SIP, Subscriber: Voice and Video Calls*
Skype	25	Voice and Video Calls	Global: Default Service*, Subscriber: Voice and Video Calls*
Skype VoIP	97	Skype	Global: Skype VoIP, Subscriber: Voice and Video Calls*
SkypeIn	65	Skype	Global: SkypeIn, Subscriber: Voice and Video Calls*
SkypeOut	66	Skype	Global: SkypeOut, Subscriber: Voice and Video Calls*
Other Skype	67	Skype	Global: Other Skype, Subscriber: Voice and Video Calls*
Vonage	13	Voice and Video Calls	Global: Vonage, Subscriber: Voice and Video Calls*
Windows Live Messenger VoIP and Video	15	Voice and Video Calls	Global: Default Service*, Subscriber: Voice and Video Calls*
Windows Live Messenger Video	18	Windows Live Messenger VoIP and Video	Global: Windows Live Messenger Video, Subscriber: Voice and Video Calls*
Windows Live Messenger VoIP	46	Windows Live Messenger VoIP and Video	Global: Windows Live Messenger VoIP, Subscriber: Voice and Video Calls*
Yahoo Messenger VoIP and Video	31	Voice and Video Calls	Global: Default Service*, Subscriber: Voice and Video Calls*
Yahoo Messenger Video	35	Yahoo Messenger VoIP and Video	Global: Yahoo Messenger Video, Subscriber: Voice and Video Calls*
Yahoo Messenger VoIP	37	Yahoo Messenger VoIP and Video	Global: Yahoo Messenger VoIP, Subscriber: Voice and Video Calls*
Behavioral VoIP	64	Voice and Video Calls	Global: Behavioral VoIP, Subscriber: Voice and Video Calls*
Other VoIP	36	Voice and Video Calls	Global: Other VoIP, Subscriber: Voice and Video Calls*
Other	1	Default Service	Default Service*
Other IP	6	Other	Other IP
Other IPv6	128	Other	Global: Other IPv6, Subscriber: Other
Other TCP	2	Other	Other TCP

Table 1-9 Installed Services (continued)

Name	ID	Name of Parent Service	Global Usage Counter and Subscriber Usage Counter
Other UDP	3	Other	Other UDP
Other Well-Known Ports	96	Other	Other Well-Known Ports

RDR Settings

The Cisco SCE platforms generate and transmit Raw Data Records (RDRs) that contain a wide variety of information and statistics, depending on the configuration of the system.

Table 1-10 lists the RDR settings defined in the default service configuration.

Table 1-10 Default RDR Settings

RDR Family	RDR Name	State	Rate	Rate Limit	Notes
Usage	Generic	ON	Every 5 minutes	—	—
	Link	ON	Every 5 minutes	—	—
	Package	ON	Every 5 minutes	—	—
	Subscriber	ON	Every 10 minutes	200 per second	—
	Virtual Links	OFF	Every 10 minutes	—	Default is ON for service configurations created in Virtual Links mode.
Transaction	Transaction	ON	—	100 per second	All services have the same relative weight.
	Anonymized Transaction	ON	—	100 per second	All services have the same relative weight.

Table 1-10 Default RDR Settings (continued)

RDR Family	RDR Name	State	Rate	Rate Limit	Notes
Transaction Usage	Transaction Usage (TUR)	OFF	—	—	No threshold.
	Anonymized Transaction Usage (TUR)	OFF	—	—	No threshold.
	HTTP Transaction Usage	OFF	—	—	—
	Anonymized HTTP Transaction Usage	OFF	—	—	—
	RTSP Transaction Usage	OFF	—	—	—
	Anonymized RTSP Transaction Usage	OFF	—	—	—
	Video Transaction Usage	OFF	—	—	—
	Anonymized Video Transaction Usage	OFF	—	—	—
	VoIP Transaction Usage	OFF	—	—	—
	Anonymized VoIP Transaction Usage	OFF	—	—	—
Quota	Quota Breach	OFF	—	—	Generate RDR when bucket is breached.
	Quota Status	OFF	User configured	User configured	—
	Quota Threshold Breach	OFF	—	—	Generate RDR each time bucket exceeds threshold.
	Session Creation	OFF	—	—	Generated upon subscriber introduction or package switch.

Table 1-10 Default RDR Settings (continued)

RDR Family	RDR Name	State	Rate	Rate Limit	Notes
Log	Block	ON	—	20 per second	—
	Anonymized Block	ON	—	20 per second	—
Real-Time Subscriber	Real-Time Subscriber Usage	ON	Every 1 minutes	100 per second	Enable for each subscriber separately, using CLI.
Attack	Attack Start	OFF	—	—	—
	Attack Stop		—	—	—
Malicious Traffic	Malicious Traffic Periodic	ON	Every 60 seconds	—	Generated only during attack.
Spam	Spam	OFF	—	—	—
	Anonymized Spam RDR	OFF	—	—	—
DHCP	DHCP	OFF	—	—	—
DHCP	DHCPv6	OFF	—	—	—
RADIUS	RADIUS	OFF	—	—	—
Zone	Zone Usage RDR	ON	Every 5 minutes	100 per second	—
Flow	Flow Start RDR				
	Anonymized Flow Start RDR				
	Flow End RDR				
	Anonymized Flow End RDR				
	Flow ongoing RDR				
	Anonymized Flow ongoing RDR				
	Media Flow RDR				
	Anonymized Media Flow RDR				

Rules

Rules are a set of configurable instructions telling the application how to handle flows classified to a service.

The default service configuration contains a single rule for the default service. Until you create other rules, the default service rule applies to all traffic processed by the SCE platform.

The default service rule places no restrictions on traffic:

- Flows are routed through the default Bandwidth Controllers (BWCs), which have unlimited bandwidth (BW).
- No quota limitations are applied to the flows and external quota management mode is selected.

System Mode

The default System Operational Mode is Report Only, which means that the system is used for reporting but does not control traffic.

The default System Topological Mode is Duplex, which means that all inbound and outbound traffic go through the SCE platform.

Note When unidirectional classifications enabled, there are some changes to the default service configuration:
- There are no predefined flavors.
- No service elements include a specified flavor.
- Periodic quota management mode is selected.

Raw Data Records: Formats and Field Contents

Revised: January 31, 2014

Introduction

This chapter contains a list of the RDRs produced by the SCE platform and a full description of the fields contained in each RDR.

The chapter also contains field-content information for the fields that the Service Control components generates.

This chapter consists of these sections:

- Raw Data Records Overview, page 2-3
- Universal RDR Fields, page 2-4
- ADDITIONAL_INFO Field, page 2-6
- Transaction RDR, page 2-7
- Anonymized Transaction RDR, page 2-10
- Transaction Usage RDR, page 2-15
- Anonymized Transaction Usage RDR, page 2-19
- HTTP Transaction Usage RDR, page 2-24
- Anonymized HTTP Transaction Usage RDR, page 2-30
- RTSP Transaction Usage RDR, page 2-34
- Anonymized RTSP Transaction Usage RDR, page 2-38
- VoIP Transaction Usage RDR, page 2-42
- Anonymized VoIP Transaction Usage RDR, page 2-46
- Video Transaction Usage RDR, page 2-50
- Anonymized Video Transaction Usage RDR, page 2-55
- Generic Usage RDR, page 2-60
- Using the Generic Usage RDR to Report IPv6 Usage, page 2-63
- Subscriber Usage RDR, page 2-64
- Real-Time Subscriber Usage RDR, page 2-68

- Link Usage RDR, page 2-71
- Zone Usage RDR, page 2-75
- Package Usage RDR, page 2-77
- Virtual Links Usage RDR, page 2-81
- Blocking RDR, page 2-84
- Anonymized Blocking RDR, page 2-86
- Quota Breach RDR, page 2-89
- Quota Status RDR, page 2-92
- Quota Threshold Breach RDR, page 2-95
- Session Creation RDR, page 2-99
- DHCP RDR, page 2-101
- DHCPv6 RDR, page 2-102
- RADIUS RDR, page 2-104
- Flow Start RDR, page 2-105
- Anonymized Flow Start RDR, page 2-107
- Flow End RDR, page 2-109
- Anonymized Flow End RDR, page 2-111
- Flow Ongoing RDR, page 2-113
- Anonymized Flow Ongoing RDR, page 2-115
- Media Flow RDR, page 2-117
- Anonymized Media Flow RDR, page 2-126
- Attack Start RDR, page 2-135
- Attack End RDR, page 2-136
- Malicious Traffic Periodic RDR, page 2-137
- Spam RDR, page 2-139
- Anonymized Spam RDR, page 2-142
- Information About RDR Enumeration Fields, page 2-145
- RDR Tag Assignment Summary, page 2-149
- Periodic RDR Zero Adjustment Mechanism, page 2-152

Raw Data Records Overview

RDRs are the collection of fields that the Service Control Engine (SCE) platforms sent to the Cisco Service Control Management Suite (SCMS) Collection Manager (CM).

Fields that are common to many of the RDRs are described in the next section, before the individual RDRs are described.

Note On devices running Cisco SCOS Release 3.8.0, generic transaction usage RDRs or anonymized transaction usage RDRs are not generated for IPv6 if the anonymized transaction usage RDRs are enabled on the device.

Universal RDR Fields

This section contains descriptions of fields that are common to many RDRs. The first two fields, SUBSCRIBER_ID and PACKAGE_ID, appear in almost all the RDRs. The other fields are listed in alphabetical order.

- SUBSCRIBER_ID—Subscriber identification string, introduced through the subscriber management interfaces. It may contain up to 64 characters. For unknown subscribers, this field may contain an empty string.
- PACKAGE_ID—ID of the package assigned to the subscriber whose traffic is being reported. An assigned Package ID is an integer between 0 and 4999. The value 4999 is reserved for unknown subscribers, and this is the maximum_number_of_packages possible.
- ACCESS_STRING—Layer 7 property, extracted from the transaction. For possible values, see the "String Fields" section on page 2-145.
- BREACH_STATE—Indicates whether the quota allocated for the subscriber was breached:
  - 0—Not breached
  - 1—Breached
- CLIENT_IP—IP address of the client side of the reported session. (The client side is defined as the initiator of the networking session.) The IP address is in a 32-bit binary format, but the value is obtained in Decimal format in RDR.
- CLIENT_PORT—Port number of the client side (initiator) of the TCP/UDP-based networking session. For non-TCP/UDP sessions, this field has the value zero.
- CONFIGURED_DURATION—Configured period, in seconds, for periodic RDRs, between successive RDRs.
- END_TIME—Ending time stamp of this RDR. The field is in UNIX time_t format, which is the number of seconds since midnight of 1 January 1970.
- FLAVOR_ID—ID of the flavor associated with this session. This field is for protocol signatures that have flavors.
- INFO_STRING—Layer 7 property, extracted from the transaction. For possible values, see the "String Fields" section on page 2-145.
- INITIATING_SIDE—Side of the SCE platform on which the initiator of the transaction resides.
  - 0—Subscriber side
  - 1—Network side
- IP-TYPE—This value indicates whether the RDR is IPv4 or IPv6. Possible values are 0 and 1.
  - 0—IPv4
  - 1—IPv6
  - 3—DSLite
- PROTOCOL_ID—Unique ID of the protocol associated with the reported session.

Note PROTOCOL_ID is the Generic IP/Generic TCP/Generic UDP protocol ID Note value, according to the specific transport protocol of the transaction, unless a more specific protocol definition (such as a signature-based protocol or a port-based protocol), which matches the reported session, is assigned to a service.

- PROTOCOL_SIGNATURE—ID of the protocol signature associated with this session.
- REPORT_TIME—Ending time stamp of this RDR. The field is in UNIX time_t format, which is the number of seconds since midnight of 1 January 1970.
- SERVER_IP—Destination IP address of the reported session. (The destination is defined as the server or the listener of the networking session.) The IP address is in a 32-bit binary format, but the value is obtained in decimal format in RDR.
- SERVER_PORT—Destination port number of the TCP/UDP-based networking session. For non-TCP/UDP sessions, this field contains the IP protocol number of the session flow.
- SERVICE_ID—Service classification of the reported session. For example, in the Transaction RDR, this field indicates which service was accessed, and in the Breaching RDR, this field indicates which service was breached.
- TIME_FRAME—Time frame during which the RDR was generated. The value of this field can be in the range from 0 to 3, indicating which of the four time frames was used.The system supports time-dependent policies, by using different rules for different time frames.
- ZONE_ID—ID of the zone associated with this session.

Note All volumes in RDRs are reported in Layer 3 bytes.

Related Topics

- String Fields, page 2-145

ADDITIONAL_INFO Field

This bit map field supplies additional information about subscriber, event, or system configuration.

Table 2-1 ADDITIONAL_INFO Field Definitions

Bit Number (LSB = 0)	Bit Value	Description
0	1	Anonymous subscriber
0	0	Introduced subscriber
1	1	Tariff change report
1	0	No tariff change
2–4	1	Reauthorization
2–4	2	Quota Holding Time Expired
2–4	4	Quota Validity Time Expired
5	1	More RDRs follow
5	0	No RDRs follow
6	1	Final RDR
7–10	Volume units	Number of bytes of each unit. This number is a power of 2. For example, 0 indicates bytes, 10 (2^10) indicates kilo bytes.
11	0	Quota update in Cisco SCE is complete.
11	1	Quota update in Cisco SCE is not complete.
12–31	0	Reserved

Transaction RDR

This section contains descriptions of Transaction RDRs.

- RDR Purpose—Analyzes a sampling of network transactions to estimate the behavior of the network based on statistics.
- RDR Default destination—Sent to the Collection Manager, inserted into the database, and used by Cisco Insight tool for statistical reports, such as the Traffic Discovery report.
- RDR Content—Describes a single transaction; its connection attributes, extracted Layer 7 attributes, duration, and volume.
- RDR Generation Logic—Generated at the end of a session, according to a configurable sampling mechanism. You can configure number-of-transaction-RDRs-per-second, which sets the number of Transaction RDRs (TRs) generated during each second.

  The Transaction RDR is not generated for sessions that are blocked by a rule.

  You can disable TRs, which invalidate TR-based reports.

  A Sizing Tool helps you to calculate the appropriate sample rate; a sample rate which is too high may cause Collection Manager sizing problems. A sample rate which is too low reduces the accuracy of TR-based reports. You may contact the Cisco technical marketing expert to calculate the appropriate sample rate that suits your business needs.
- RDR tag— 0xf0f0f010 / 4042321936

Table 2-2 lists the Transaction RDR fields and their descriptions.

Table 2-2 Transaction RDR Fields

RDR Field Name	Type	Description	Example Value
SUBSCRIBER_ID	STRING	Subscriber identification string, introduced through the subscriber management interfaces. It may contain up to 64 characters. For unknown subscribers, this field may contain an empty string.	john
PACKAGE_ID	INT16	ID of the package assigned to the subscriber whose traffic is being reported. An assigned Package ID is an integer value between 0 and 4999. The value 4999 is reserved for unknown subscribers, and this is the maximum_number_of_packages possible.	0 [Default Package]
SERVICE_ID	INT32	Service classification of the reported session. For example, in the Transaction RDR, this field indicates which service was accessed, and in the Breaching RDR, this field indicates which service was breached.	16 [HTTP]
PROTOCOL_ID	INT16	Unique ID of the protocol associated with the reported session.	2 [HTTP]

Table 2-2 Transaction RDR Fields (continued)

RDR Field Name	Type	Description	Example Value
SKIPPED_SESSIONS	UINT32	Number of unreported sessions since the previous RDR *plus one*. The default value is 1. A value of 2 means that *one* RDR was unreported.	10
SERVER_IP	UINT32	Destination IP address of the reported session. (The destination is defined as the server or the listener of the networking session.) The IP address is in a 32-bit binary format, but the value is obtained in decimal format in RDR.	3330661145
SERVER_PORT	UINT16	Destination port number of the TCP/UDP-based networking session. For non-TCP/UDP sessions, this field contains the IP protocol number of the session flow.	80
ACCESS_STRING	STRING	Layer 7 property, extracted from the transaction.	www.cisco.com
INFO_STRING	STRING	Layer 7 property, extracted from the transaction.	/en/US/partner/
CLIENT_IP	UINT32	IP address of the client side of the reported session. (The client side is defined as the initiator of the networking session.) The IP address is in a 32-bit binary format, but the value is obtained in Decimal format in RDR.	3228978306
CLIENT_PORT	UINT16	Port number of the client side (initiator) of the TCP/UDP-based networking session. For non-TCP/UDP sessions, this field has the value zero.	3221
INITIATING_SIDE	INT8	Side of the SCE platform on which the initiator of the transaction resides: • 0—Subscriber side • 1—Network side	0 [subscriber-initiated]
REPORT_TIME	UINT32	Ending time stamp of this RDR. The field is in UNIX time_t format, which is the number of seconds since midnight of 1 January 1970.	—
MILLISEC_ DURATION	UINT32	Duration, in milliseconds, of the transaction reported in this RDR.	310

Table 2-2 Transaction RDR Fields (continued)

RDR Field Name	Type	Description	Example Value
TIME_FRAME	INT8	Time frame during which the RDR was generated. The value of the field is in the range 0–3, indicating which of the four time frames was used. The system supports time-dependent policies, by using different rules for different time frames.	0
SESSION_ UPSTREAM_ VOLUME	UINT32	Upstream volume of the transaction, in bytes. The volume refers to the aggregated upstream volume on both links of all the flows bundled in the transaction.	32
SESSION_ DOWNSTREAM_ VOLUME	UINT32	Downstream volume of the transaction, in bytes. The volume refers to the aggregated downstream volume on both links of all the flows bundled in the transaction.	117
SUBSCRIBER_ COUNTER_ID	UINT16	Counter to which each service is mapped. There are 48 subscriber usage counters.	1
GLOBAL_COUNTER_ ID	UINT16	Counter to which each service is mapped. There are 192 global usage counters.	9
PACKAGE_ COUNTER_ID	UINT16	Counter to which each package is mapped. There are 1024 package usage counters.	0
IP_PROTOCOL	UINT8	IP protocol type.	6 [TCP]
PROTOCOL_ SIGNATURE	INT32	ID of the protocol signature associated with this session.	0x3010000 [HTTP]
ZONE_ID	INT32	ID of the zone associated with this session.	0
FLAVOR_ID	INT32	ID of the flavor associated with this session.	0
FLOW_CLOSE_ MODE	UINT8	Reason for the end of flow: • 0 [TCP_NORMAL_CLOSE] • 2 [The aging mechanism closed the flow.]	0
IP_TYPE	UINT8	IP flow type of the respective RDR. For example, when the flow type is IPv6, the IPv4 address of the RDR will contain the value zero. However, the IPv6 address of the RDR will contain a white space for IPv4 flow type.	0—IPv4 1—IPv6

Table 2-2 Transaction RDR Fields (continued)

RDR Field Name	Type	Description	Example Value
SERVERIPv6ADDRESS	STRING	Destination IPv6 address of the reported session. The destination is defined as the server or the listener of the networking session.	2001:0db8:f0fd:a0bd:1234:98dc:cccc:aa24
CLIENTIPv6ADDRESS	STRING	IPv6 address of the client side of the reported session. The client side is defined as the initiator of the networking session.	2001:0db8:f0fd:a0bd:1234:98dc:cccc:aa24

Related Topics

- Universal RDR Fields, page 2-4
- Anonymized Transaction RDR, page 2-10

Anonymized Transaction RDR

This section contains descriptions of Anonymized Transaction RDRs.

- RDR Purpose—Analyzes a sampling of network transactions to estimate the behavior of the network based on statistics, without personal subscriber data.
- RDR Default destination—Sent to the Collection Manager, inserted into the database, and used by Cisco Insight tool for statistical reports, such as the Traffic Discovery report.
- RDR Content—Describes a single transaction; its connection attributes, extracted Layer 7 attributes, duration, and volume.
- RDR Generation Logic—Generated at the end of a session, according to a configurable sampling mechanism. You can configure the number-of-transaction-RDRs-per-second, which sets the number of Transaction RDRs (TRs) generated during each second.

  The Transaction RDR is not generated for sessions that are blocked by a rule.

  You can disable TRs, which invalidate TR-based reports.
- RDR tag— 0xf0f0f540 / 4042323264

Table 2-3 lists the Anonymized Transaction RDR fields and their descriptions.

Table 2-3 Anonymized Transaction RDR Fields

RDR Field Name	Type	Description	Example Value
HASHED_SUBSCRIBER_ID	STRING	Subscriber identification string introduced through the subscriber management interfaces. It may be passed through the hashing algorithm. It may contain up to 64 characters. For unknown subscribers, this field may contain an empty string.	da1c2d7c1e41147979e920fd56575077
PACKAGE_ID	INT16	ID of the package assigned to the subscriber whose traffic is being reported. An assigned Package ID is an integer value between 0 and 4999. The value 4999 is reserved for unknown subscribers, and this is the maximum_number_of_packages possible.	0 [Default Package]
SERVICE_ID	INT32	Service classification of the reported session. For example, in the Transaction RDR, this field indicates which service was accessed, and in the Breaching RDR, this field indicates which service was breached.	16 [HTTP]
PROTOCOL_ID	INT16	Unique ID of the protocol associated with the reported session.	2 [HTTP]
SKIPPED_SESSIONS	UINT32	Number of unreported sessions since the previous RDR *plus one*. The default value is 1. A value of 2 means that *one* RDR was unreported.	10
SERVER_IP	UINT32	Destination IP address of the reported session. (The destination is defined as the server or the listener of the networking session.) The IP address is in a 32-bit binary format, but the value is obtained in decimal format in RDR. If this is the subscriber IP, this field may contain the short-hash of the IP if configured.	3330661145
SERVER_PORT	UINT16	Destination port number of the TCP/UDP-based networking session. For non-TCP/UDP sessions, this field contains the IP protocol number of the session flow.	80

Table 2-3 Anonymized Transaction RDR Fields (continued)

RDR Field Name	Type	Description	Example Value
ACCESS_STRING	STRING	Layer 7 property, extracted from the transaction.	www.cisco.com
INFO_STRING	STRING	Layer 7 property, extracted from the transaction.	/en/US/partner/
CLIENT_IP	UINT32	IP address of the client side of the reported session. (The client side is defined as the initiator of the networking session.) The IP address is in a 32-bit binary format, but the value is obtained in Decimal format in RDR. If this is the subscriber IP, this field may contain the short-hash of the IP if configured.	3228978306
CLIENT_PORT	UINT16	Port number of the client side (initiator) of the TCP/UDP-based networking session. For non-TCP/UDP sessions, this field has the value zero.	3221
INITIATING_SIDE	INT8	Side of the SCE platform on which the initiator of the transaction resides: • 0—Subscriber side • 1—Network side	0 [subscriber-initiated]
REPORT_TIME	UINT32	Ending time stamp of this RDR. The field is in UNIX time_t format, which is the number of seconds since midnight of 1 January 1970.	—
MILLISEC_ DURATION	UINT32	Duration, in milliseconds, of the transaction reported in this RDR.	310
TIME_FRAME	INT8	Time frame during which the RDR was generated. The value of the field is in the range 0 – 3, indicating which of the four time frames was used. The system supports time-dependent policies, by using different rules for different time frames.	0
SESSION_ UPSTREAM_ VOLUME	UINT32	Upstream volume of the transaction, in bytes. The volume refers to the aggregated upstream volume on both links of all the flows bundled in the transaction.	32

Table 2-3 Anonymized Transaction RDR Fields (continued)

RDR Field Name	Type	Description	Example Value
SESSION_ DOWNSTREAM_ VOLUME	UINT32	Downstream volume of the transaction, in bytes. The volume refers to the aggregated downstream volume on both links of all the flows bundled in the transaction.	117
SUBSCRIBER_ COUNTER_ID	UINT16	Counter to which each service is mapped. There are 48 subscriber usage counters.	1
GLOBAL_COUNTER_ ID	UINT16	Counter to which each service is mapped. There are 192 global usage counters.	9
PACKAGE_ COUNTER_ID	UINT16	Counter to which each package is mapped. There are 1024 package usage counters.	0
IP_PROTOCOL	UINT8	IP protocol type.	6 [TCP]
PROTOCOL_ SIGNATURE	INT32	ID of the protocol signature associated with this session.	0x3010000 [HTTP]
ZONE_ID	INT32	ID of the zone associated with this session.	0
FLAVOR_ID	INT32	ID of the flavor associated with this session.	0
FLOW_CLOSE_ MODE	UINT8	Reason for the end of flow: • 0 [TCP_NORMAL_CLOSE] • 2 [The aging mechanism closed the flow.]	0
IP_TYPE	UINT8	IP flow type of the respective RDR. For example, when the flow type is IPv6, the IPv4 address of the RDR will contain the value zero. However, the IPv6 address of the RDR will contain a white space for IPv4 flow type.	0—IPv4 1—IPv6

Table 2-3 Anonymized Transaction RDR Fields (continued)

RDR Field Name	Type	Description	Example Value
SERVERIPv6ADDRESS	STRING	Destination IPv6 address of the reported session. The destination is defined as the server or the listener of the networking session. If this is the subscriber IP, this field may contain a 32-byte string hash, if configured.	2001:0db8:f0fd:a0bd:1234:98dc:cccc:aa24
CLIENTIPv6ADDRESS	STRING	IPv6 address of the client side of the reported session. The client side is defined as the initiator of the networking session. If this is the subscriber IP, this field may contain a 32-byte string hash, if configured.	2001:0db8:f0fd:a0bd:1234:98dc:cccc:aa24

Related Topics

- Universal RDR Fields, page 2-4
- Transaction RDR, page 2-7

Transaction Usage RDR

This section contains descriptions of Transaction Usage RDR.

- RDR Purpose—Log network transactions for transaction-based billing or offline data mining.
- RDR Default destination—Sent to the Collection Manager, and stored in comma-separated values (CSV) files.
- RDR Content—Describes a single transaction; its connection attributes, extracted Layer 7 attributes, duration, and volume.
- RDR Generation Logic—Generated at the end of a session, for all transactions on packages and services that are configured to generate such an RDR.

  This RDR is not generated for sessions that were blocked by a rule.
- RDR tag—0xf0f0f438 / 4042323000

By default, packages and services are disabled from generating Transaction Usage RDRs. They can be enabled for specific packages and services. You can disable generating Transaction Usage RDRs (TURs) for short flows by setting a volume threshold. You can enable generating interim TURs for long transactions.

Transaction Usage RDRs are designed for services and packages where specific, per-transaction RDRs are required (such as, transaction-level billing). It is easy to configure this RDR, in error, so that it is generated for every transaction, which may result in an excessive RDR rate.

Note Configure the generation scheme for this RDR with extra care.

Table 2-4 lists the Transaction Usage RDR fields and their descriptions.

Table 2-4 Transaction Usage RDR Fields

RDR Field Name	Type	Description	Example Value
SUBSCRIBER_ID	STRING	Subscriber identification string, introduced through the subscriber management interfaces. It may contain up to 64 characters. For unknown subscribers, this field may contain an empty string.	john
PACKAGE_ID	INT16	ID of the package assigned to the subscriber whose traffic is being reported. An assigned Package ID is an integer value between 0 and 4999. The value 4999 is reserved for unknown subscribers, and this is the maximum_number_of_packages possible.	0 [Default Package

Table 2-4 Transaction Usage RDR Fields (continued)

RDR Field Name	Type	Description	Example Value
SERVICE_ID	INT32	Service classification of the reported session. For example, in the Transaction RDR, this field indicates which service was accessed, and in the Breaching RDR, this field indicates which service was breached.	16 [HTTP]
PROTOCOL_ID	INT16	Unique ID of the protocol associated with the reported session.	2 [HTTP]
SKIPPED_SESSIONS	UINT32	Reason for RDR generation: • 0 (INTERIM)—Interim Transaction Usage RDR • 1 (SESSION_END)—Normal Transaction Usage RDR for a flow that had no interim Transaction Usage RDRs • 2 (LAST_TUR)—Last Transaction Usage RDR for a flow that had interim Transaction Usage RDRs	1 [SESSION_END]
SERVER_IP	UINT32	Contains the destination IP address of the reported session. (The destination is defined as the server or the listener of the networking session.) The IP address is in a 32-bit binary format, but the value is obtained in Decimal format in RDR.	3330661145
SERVER_PORT	UINT16	Destination port number of the TCP/UDP-based networking session. For non-TCP/UDP sessions, this field contains the IP protocol number of the session flow.	80
ACCESS_STRING	STRING	Layer 7 property, extracted from the transaction.	www.cisco.com
INFO_STRING	STRING	Layer 7 property, extracted from the transaction.	/en/US/partner/
CLIENT_IP	UNIT32	IP address of the client side of the reported session. The client side is defined as the initiator of the networking session. The IP address is in a 32-bit binary format, but the value is obtained in Decimal format in RDR.	3228978306

Table 2-4 Transaction Usage RDR Fields (continued)

RDR Field Name	Type	Description	Example Value
CLIENT_PORT	UINT16	Port number of the client side (initiator) of the TCP/UDP-based networking session. For non-TCP/UDP sessions, this field has the value zero.	3221
INITIATING_SIDE	INT8	Side of the SCE platform on which the initiator of the transaction resides: • 0—Subscriber side • 1—Network side	0 [subscriber-initiated]
REPORT_TIME	UINT32	Ending time stamp of this RDR. The field is in UNIX time_t format, which is the number of seconds since midnight of 1 January 1970.	—
MILLISEC_ DURATION	UINT32	Duration, in milliseconds, of the transaction reported in this RDR.	310
TIME_FRAME	INT8	Time frame during which the RDR was generated. The value of the field can be in the range 0 – 3, indicating which of the four time frames was used. The system supports time-dependent policies, by using different rules for different time frames.	0
SESSION_ UPSTREAM_ VOLUME	UINT32	Upstream volume of the transaction, in bytes. The volume refers to the aggregated upstream volume on both links of all the flows bundled in the transaction.	32
SESSION_ DOWNSTREAM_ VOLUME	UINT32	Downstream volume of the transaction, in bytes. The volume refers to the aggregated downstream volume on both links of all the flows bundled in the transaction.	117
SUBSCRIBER_ COUNTER_ID	UINT16	Counter to which each service is mapped. There are 48 subscriber usage counters.	1
GLOBAL_COUNTER_ ID	UINT16	Counter to which each service is mapped. There are 192 global usage counters.	9
PACKAGE_ COUNTER_ID	UINT16	Counter to which each package is mapped. There are 1024 package usage counters.	0
IP_PROTOCOL	UINT8	IP protocol type.	6 [TCP]

Table 2-4 Transaction Usage RDR Fields (continued)

RDR Field Name	Type	Description	Example Value
PROTOCOL_ SIGNATURE	INT32	ID of the protocol signature associated with this session.	0x3010000 [HTTP]
ZONE_ID	INT32	ID of the zone associated with this session.	0
FLAVOR_ID	INT32	ID of the flavor associated with this session.	0
FLOW_CLOSE_ MODE	UINT8	Reason for the end of flow: • 0 [TCP_NORMAL_CLOSE] • 2 [The aging mechanism closed the flow.]	0
SESSION_LINK_ID	INT8	The ID number of the link on which the session was initiated. Values are between 0-X, where X is the corresponding SCE link. X can have values of 0–7 if there is only one DPI module and 0–15 if there are two DPI modules.	0–15
IP_TYPE	UINT8	IP flow type of the respective RDR. For example, when the flow type is IPv6, the IPv4 address of the RDR will contain the value zero. However, the IPv6 address of the RDR will contain a white space for IPv4 flow type.	0—IPv4 1—IPv6
SERVERIPv6ADDRES S	STRING	Destination IPv6 address of the reported session. The destination is defined as the server or the listener of the networking session.	2001:0db8:f0fd:a0bd:1 234:98dc:cccc:aa24
CLIENTIPv6ADDRES S	STRING	IPv6 address of the client side of the reported session. The client side is defined as the initiator of the networking session.	2001:0db8:f0fd:a0bd:1 234:98dc:cccc:aa24

Related Topics

- Universal RDR Fields, page 2-4
- Anonymized Transaction Usage RDR, page 2-19

Anonymized Transaction Usage RDR

This section contains descriptions of Anonymized Transaction Usage RDR.

- RDR Purpose—Log network transactions for transaction-based billing or offline data mining, without personal subscriber data.
- RDR Default destination—Sent to the Collection Manager, and stored in CSV files.
- RDR Content—Describes a single transaction; its connection attributes, extracted Layer 7 attributes, duration, and volume.
- RDR Generation Logic—Generated at the end of a session, for all transactions on packages and services that are configured to generate such an RDR.

  This RDR is not generated for sessions that were blocked by a rule.
- RDR tag—0xf0f0f546 / 4042323270

By default, packages and services are disabled from generating Anonymized Transaction Usage RDRs. They can be enabled for specific packages and services. You can disable generating Transaction Usage RDRs (TURs) for short flows by setting a volume threshold. You can enable generating interim TURs for long transactions.

Anonymized Transaction Usage RDRs are designed for services and packages where specific, per-transaction RDRs are required (such as, transaction-level billing). It is easy to configure this RDR, in error, so that it is generated for every transaction, which may result in an excessive RDR rate.

Note Configure the generation scheme for this RDR with extra care.

Table 2-5 lists the Anonymized Transaction Usage RDR fields and their descriptions.

Table 2-5 Anonymized Transaction Usage RDR Fields

RDR Field Name	Type	Description	Example Value
HASHED_SUBSCRIBER_ID	STRING	Subscriber identification string introduced through the subscriber management interfaces. It may be passed through the hashing algorithm. It may contain up to 64 characters. For unknown subscribers, this field may contain an empty string.	da1c2d7c1e41147979e920fd56575077
PACKAGE_ID	INT16	ID of the package assigned to the subscriber whose traffic is being reported. An assigned Package ID is an integer value between 0 and 4999. The value 4999 is reserved for unknown subscribers, and this is the maximum_number_of_packages possible.	0 [Default Package

Table 2-5 Anonymized Transaction Usage RDR Fields (continued)

RDR Field Name	Type	Description	Example Value
SERVICE_ID	INT32	Service classification of the reported session. For example, in the Transaction RDR, this field indicates which service was accessed, and in the Breaching RDR this field indicates which service was breached.	16 [HTTP]
PROTOCOL_ID	INT16	Unique ID of the protocol associated with the reported session.	2 [HTTP]
SKIPPED_SESSIONS	UINT32	Reason for RDR generation: • 0 (INTERIM)—Interim Transaction Usage RDR • 1 (SESSION_END)—Normal Transaction Usage RDR for a flow that had no interim Transaction Usage RDRs • 2 (LAST_TUR)—Last Transaction Usage RDR for a flow that had interim Transaction Usage RDRs	1 [SESSION_END]
SERVER_IP	UINT32	Contains the destination IP address of the reported session. (The destination is defined as the server or the listener of the networking session.) The IP address is in a 32-bit binary format, but the value is obtained in decimal format in RDR. If this is the subscriber IP, this field may contain the short-hash of the IP if configured.	3330661145
SERVER_PORT	UINT16	Destination port number of the TCP/UDP-based networking session. For non-TCP/UDP sessions, this field contains the IP protocol number of the session flow.	80
ACCESS_STRING	STRING	Layer 7 property, extracted from the transaction.	www.cisco.com
INFO_STRING	STRING	Layer 7 property, extracted from the transaction.	/en/US/partner/

Table 2-5 Anonymized Transaction Usage RDR Fields (continued)

RDR Field Name	Type	Description	Example Value
CLIENT_IP	UNIT32	IP address of the client side of the reported session. The client side is defined as the initiator of the networking session. The IP address is in a 32-bit binary format, but the value is obtained in Decimal format in RDR. If this is the subscriber IP, this field may contain the short-hash of the IP if configured.	3228978306
CLIENT_PORT	UINT16	Port number of the client side (initiator) of the TCP/UDP-based networking session. For non-TCP/UDP sessions, this field has the value zero.	3221
INITIATING_SIDE	INT8	Side of the SCE platform on which the initiator of the transaction resides: • 0—Subscriber side • 1—Network side	0 [subscriber-initiated]
REPORT_TIME	UINT32	Ending time stamp of this RDR. The field is in UNIX time_t format, which is the number of seconds since midnight of 1 January 1970.	—
MILLISEC_ DURATION	UINT32	Duration, in milliseconds, of the transaction reported in this RDR.	310
TIME_FRAME	INT8	Time frame during which the RDR was generated. The value of the field can be in the range 0 – 3, indicating which of the four time frames was used. The system supports time-dependent policies, by using different rules for different time frames.	0
SESSION_ UPSTREAM_ VOLUME	UINT32	Upstream volume of the transaction, in bytes. The volume refers to the aggregated upstream volume on both links of all the flows bundled in the transaction.	32
SESSION_ DOWNSTREAM_ VOLUME	UINT32	Downstream volume of the transaction, in bytes. The volume refers to the aggregated downstream volume on both links of all the flows bundled in the transaction.	117

Table 2-5 Anonymized Transaction Usage RDR Fields (continued)

RDR Field Name	Type	Description	Example Value
SUBSCRIBER_ COUNTER_ID	UINT16	Counter to which each service is mapped. There are 48 subscriber usage counters.	1
GLOBAL_COUNTER_ ID	UINT16	Counter to which each service is mapped. There are 192 global usage counters.	9
PACKAGE_ COUNTER_ID	UINT16	Counter to which each package is mapped. There are 1024 package usage counters.	0
IP_PROTOCOL	UINT8	IP protocol type.	6 [TCP]
PROTOCOL_ SIGNATURE	INT32	ID of the protocol signature associated with this session.	0x3010000 [HTTP]
ZONE_ID	INT32	ID of the zone associated with this session.	0
FLAVOR_ID	INT32	ID of the flavor associated with this session.	0
FLOW_CLOSE_ MODE	UINT8	Reason for the end of flow: • 0 [TCP_NORMAL_CLOSE] • 2 [The aging mechanism closed the flow.]	0
SESSION_LINK_ID	INT8	The ID number of the link on which the session was initiated. Values are between 0–X, where X is the corresponding SCE link. X can have values of 0–7 if there is only one DPI module and 0–15 if there are two DPI modules.	0–7
IP_TYPE	UINT8	IP flow type of the respective RDR. For example, when the flow type is IPv6, the IPv4 address of the RDR will contain the value zero. However, the IPv6 address of the RDR will contain a white space for IPv4 flow type.	0—IPv4 1—IPv6

Table 2-5 Anonymized Transaction Usage RDR Fields (continued)

RDR Field Name	Type	Description	Example Value
SERVERIPv6ADDRESS	STRING	Destination IPv6 address of the reported session. The destination is defined as the server or the listener of the networking session. If this is the subscriber IP, this field may contain a 32-byte string hash, if configured.	2001:0db8:f0fd:a0bd:1234:98dc:cccc:aa24
CLIENTIPv6ADDRESS	STRING	IPv6 address of the client side of the reported session. The client side is defined as the initiator of the networking session. If this is the subscriber IP, this field may contain a 32-byte string hash, if configured.	2001:0db8:f0fd:a0bd:1234:98dc:cccc:aa24

Related Topics

- Universal RDR Fields, page 2-4
- Transaction Usage RDR, page 2-15

HTTP Transaction Usage RDR

The HTTP_TRANSACTION_USAGE_RDR is a TUR specifically used for HTTP transactions.

- RDR Purpose—Log HTTP network transactions for transaction-based billing or offline data mining.
- RDR Default destination—Sent to the Collection Manager, and stored in CSV files.
- RDR Content—Describes a single HTTP transaction; its connection attributes, extracted Layer 7 attributes, duration, and volume.
- RDR Generation Logic—Generated at the end of an HTTP session, for all transactions on packages and services that are configured to generate a Transaction Usage RDR.

  This RDR is not generated for sessions that were blocked by a rule.
- RDR tag—0xf0f0f43C / 4042323004

By default, packages and services are disabled from generating this RDR. You can enable them for specific packages and services.

This RDR is designed for services and packages where specific, per-transaction RDRs are required (such as, transaction-level billing). It is easy to configure this RDR, in error, so that it is generated for every transaction, which may result in an excessive RDR rate.

Note Configure the generation scheme for this RDR with extra care.

Table 2-6 lists the HTTP Transaction Usage RDR fields and their descriptions.

Table 2-6 HTTP Transaction Usage RDR Fields

RDR Field Name	Type	Description	Example Value
SUBSCRIBER_ID	STRING	Subscriber identification string, introduced through the subscriber management interfaces. It may contain up to 64 characters. For unknown subscribers, this field may contain an empty string.	john
PACKAGE_ID	INT16	ID of the package assigned to the subscriber whose traffic is being reported. An assigned Package ID is an integer value between 0 and 4999. The value 4999 is reserved for unknown subscribers, and this is the maximum_number_of_packages possible.	0 [Default Package]
SERVICE_ID	INT32	Service classification of the reported session. For example, in the Transaction RDR, this field indicates which service was accessed, and in the Breaching RDR, this field indicates which service was breached.	16 [HTTP]

Table 2-6 HTTP Transaction Usage RDR Fields (continued)

RDR Field Name	Type	Description	Example Value
PROTOCOL_ID	INT16	Unique ID of the protocol associated with the reported session.	2 [HTTP]
SKIPPED_SESSIONS	UINT32	Number of unreported sessions since the previous RDR. Because an HTTP Transaction Usage RDR is generated only at the end of a flow, this field always has the value 1.	1 [SESSION_END]
SERVER_IP	UINT32	Destination IP address of the reported session. (The destination is defined as the server or the listener of the networking session.) The IP address is in a 32-bit binary format, but the value is obtained in decimal format in RDR.	3330661145
SERVER_PORT	UINT16	Destination port number of the TCP/UDP-based networking session. For non-TCP/UDP sessions, this field contains the IP protocol number of the session flow.	80
ACCESS_STRING	STRING	Layer 7 property, extracted from the transaction.	www.cisco.com
INFO_STRING	STRING	Layer 7 property, extracted from the transaction.	/en/US/partner/
CLIENT_IP	UINT32	IP address of the client side of the reported session. The client side is defined as the initiator of the networking session. The IP address is in a 32-bit binary format, but the value is obtained in Decimal format in RDR.	3228978306
CLIENT_PORT	UINT16	Port number of the client side (initiator) of the TCP/UDP-based networking session. For non-TCP/UDP sessions, this field has the value zero.	3221
INITIATING_SIDE	INT8	Side of the SCE platform on which the initiator of the transaction resides: • 0—Subscriber side • 1—Network side	0 [subscriber-initiated]
REPORT_TIME	UINT32	Ending time stamp of this RDR. The field is in UNIX time_t format, which is the number of seconds since midnight of 1 January 1970.	—

Table 2-6 HTTP Transaction Usage RDR Fields (continued)

RDR Field Name	Type	Description	Example Value
MILLISEC_ DURATION	UINT32	Duration, in milliseconds, of the transaction reported in this RDR.	310
TIME_FRAME	INT8	Time frame during which the RDR was generated. The value of the field can be in the range 0–3, indicating which of the four time frames was used. The system supports time-dependent policies, by using different rules for different time frames.	0
SESSION_ UPSTREAM_ VOLUME	UINT32	Upstream volume of the transaction, in bytes. The volume refers to the aggregated upstream volume on both links of all the flows bundled in the transaction.	32
SESSION_ DOWNSTREAM_ VOLUME	UINT32	Downstream volume of the transaction, in bytes. The volume refers to the aggregated downstream volume on both links of all the flows bundled in the transaction.	117
SUBSCRIBER_ COUNTER_ID	UINT16	Counter to which each service is mapped. There are 48 subscriber usage counters.	1
GLOBAL_COUNTER_ ID	UINT16	Counter to which each service is mapped. There are 192 global usage counters.	9
PACKAGE_ COUNTER_ID	UINT16	Counter to which each package is mapped. There are 1024 package usage counters.	0
IP_PROTOCOL	UINT8	IP protocol type.	6 [TCP]
PROTOCOL_ SIGNATURE	INT32	ID of the protocol signature associated with this session.	0x3010000 [HTTP]
ZONE_ID	INT32	ID of the zone associated with this session.	0
FLAVOR_ID	INT32	ID of the flavor associated with this session.	0
FLOW_CLOSE_ MODE	UINT8	Reason for the end of flow: • 0 [TCP_NORMAL_CLOSE] • 2 [The aging mechanism closed the flow.]	0
USER_AGENT	STRING	User agent field extracted from the HTTP transaction.	Moselle
HTTP_REFERER	STRING	REFERER extracted from the HTTP transaction.	http://addition.cnn.com

Table 2-6 HTTP Transaction Usage RDR Fields (continued)

RDR Field Name	Type	Description	Example Value
HTTP_COOKIE	STRING	COOKIE extracted from the HTTP transaction.	SelectedAddition= Addition;CNNid= 3459286729-09
SESSION_LINK_ID	INT8	The ID number of the link on which the session was initiated. Values are between 0-X, where X is the corresponding SCE link. X can have values of 0–7 if there is only one DPI module and 0–15 if there are two DPI modules.	0–15
IP_TYPE	UINT8	Defines the IP flow type of the respective RDR. For example, when the flow type is IPv6, the IPv4 address of the RDR will contain the value zero. However, the IPv6 address of the RDR will contain a white space for IPv4 flow type.	0—IPv4 1—IPv6
SERVERIPv6ADDRES S	STRING	Destination IPv6 address of the reported session. The destination is defined as the server or the listener of the networking session.	2001:0db8:f0fd:a0bd:1 234:98dc:cccc:aa24
CLIENTIPv6ADDRESS	STRING	IPv6 address of the client side of the reported session. The client side is defined as the initiator of the networking session.	2001:0db8:f0fd:a0bd:1 234:98dc:cccc:aa24
ATTRIBUTE INDICATOR	UINT32	Generated if the VSA Fields option is enabled. Identifies the valid attributes from the RDR.	2047 all fields are valid
ACCT-MULTI-SESSIO N-ID	STRING	Generated if the VSA Fields option is enabled. A unique accounting ID used to link multiple related sessions.	Subscriber1
ACCT-SESSION-ID	STRING	Generated if the VSA Fields option is enabled. A unique accounting ID used to match the start and stop records in a log file. The start and stop records for a given session contains the same ID. All accounting request packet contains an accounting session ID.	lkjhgfdsa

Table 2-6 HTTP Transaction Usage RDR Fields (continued)

RDR Field Name	Type	Description	Example Value
FRAMED-IP-ADDRESS	UINT32	Generated if the VSA Fields option is enabled. Provides the IPv4 address allocated to the subscriber.	10.1.2.3
CALLED-STATION-ID	STRING	Generated if the VSA Fields option is enabled. Provides the ID of station to which the subscriber is connected for the GPRS access.	abcdefg
3GPP-IMEISV	STRING	Generated if the VSA Fields option is enabled. Provides the international mobility equipment identity (IMEI) of the subscriber. IMEI is a unique identity associated with all the GSM and CDMA subscribers.	000000000000
3GPP-IMSI	STRING	Generated if the VSA Fields option is enabled. Provides the international mobile subscriber identity (IMSI) of the subscriber. IMSI is a unique ID associated with all the GSM and UMTS network mobile phone subscribers.	000000100000
3GPP-RAT-TYPE	STRING	Generated if the VSA Fields option is enabled. Indicates the radio access technology (RAT) serving the subscriber equipment.	700300100050
3GPP-SGSN-ADDRESS	UINT32	Generated if the VSA Fields option is enabled. Indicates the IPv4 address of the serving GPRS support node (SGSN)	10.1.1.1
3GPP-SGSN-MCC-MNC	STRING	Generated if the VSA Fields option is enabled. Indicates the mobile country code (MCC) and mobile network code (MNC) of the SGSN.	mhutexcfvkli
3GPP-USER-LOCATION-INFO	STRING	Generated if the VSA Fields option is enabled. Indicates the location of the equipment.	abc

Table 2-6 HTTP Transaction Usage RDR Fields (continued)

RDR Field Name	Type	Description	Example Value
WIMAX-BSID	STRING	Generated if the VSA Fields option is enabled. Indicates the base station identifier (BSID) of the WiMax network.	3p3p3
3GPP2-MEID	STRING	Generated if the VSA Fields option is enabled. The 3G mobile equipment identifier of a CDMA mobile station equipment.	A0000020D92AAA
3GPP2-ESN	STRING	Generated if the VSA Fields option is enabled. The unique electronic serial number of the mobile station equipment assigned by the mobile station manufacturer.	80dc47ed
3GPP2-PCF-IP-Address	UINT32	Generated if the VSA Fields option is enabled. The packet control function IP address.	10.222.202.5
3GPP2-Home-Agent-IP-Address	UINT32	Generated if the VSA Fields option is enabled. The IP address of the home agent connected to the mobile station.	68.28.57.76
Framed-IPv6-Prefix	STRING	This field is supported only on Cisco SCE 8000. The field appears in Cisco SCE 2000, but is a reserved field. Generated if the VSA Fields option is enabled. The IPv6 address prefix allocated to the corresponding subscriber.	—

Related Topics

- Universal RDR Fields, page 2-4

Anonymized HTTP Transaction Usage RDR

The ANONYMIZED_HTTP_TRANSACTION_USAGE_RDR is a TUR specifically used for HTTP transactions.

- RDR Purpose—Log HTTP network transactions for transaction-based billing or offline data mining without personal subscriber data.
- RDR Default destination—Sent to the Collection Manager, and stored in CSV files.
- RDR Content—Describes a single HTTP transaction; its connection attributes, extracted Layer 7 attributes, duration, and volume.
- RDR Generation Logic—Generated at the end of an HTTP session, for all transactions on packages and services that are configured to generate a Transaction Usage RDR.

  This RDR is not generated for sessions that were blocked by a rule.
- RDR tag—0xf0f0f53C / 4042323260

By default, packages and services are disabled from generating this RDR. You can enable them for specific packages and services.

This RDR is designed for services and packages where specific, per-transaction RDRs are required (such as, transaction-level billing). It is easy to configure this RDR, in error, so that it is generated for every transaction, which may result in an excessive RDR rate.

Note Configure the generation scheme for this RDR with extra care.

Table 2-7 lists the Anonymized HTTP Transaction Usage RDR fields and their descriptions.

Table 2-7 Anonymized HTTP Transaction Usage RDR Fields

RDR Field Name	Type	Description
HASHED_SUBSCRIBER_ID	STRING	Subscriber identification string, may be passed through hashing algorithm.
PACKAGE_ID	INT16	ID of the package assigned to the subscriber whose traffic is being reported.
SERVICE_ID	INT32	Service classification of the reported session.
PROTOCOL_ID	INT16	Unique ID of the protocol associated with the reported session.
SKIPPED_SESSIONS	UINT32	Always 1.
SERVER_IP	UINT32	HTTP server IP. If this is the subscriber IP, this field may contain the short hash of the IP, if configured.
SERVER_PORT	UINT16	Destination port number of the networking session.
HOST	STRING	Host extracted from the HTTP transaction.
URL	STRING	URL extracted from the HTTP transaction.
CLIENT_IP	UINT32	HTTP client IP. If this is the subscriber IP, this field may contain the short-hash of the IP if configured.

Table 2-7 Anonymized HTTP Transaction Usage RDR Fields (continued)

RDR Field Name	Type	Description
CLIENT_PORT	UINT16	Port number of the client side (initiator) of the networking session.
INITIATING_SIDE	INT8	Side of the SCE platform on which the initiator of the transaction resides: • 0–Subscriber side • 1–Network side
REPORT_TIME	UINT32	Ending time stamp of this RDR.
MILLISEC_DURATION	UINT32	Duration, in milliseconds, of the transaction reported in this RDR.
TIME_FRAME	INT8	Time frame during which the RDR was generated. The value of the field can be in the range 0–3, indicating which of the four time frames was used. The system supports time-dependent policies, by using different rules for different time frames.
SESSION_UPSTREAM_ VOLUME	UINT32	Upstream volume of the transaction, in bytes. The volume refers to the aggregated upstream volume on both links of all the flows bundled in the transaction.
SESSION_DOWNSTREAM_ VOLUME	UINT32	Downstream volume of the transaction, in bytes. The volume refers to the aggregated stream volume on both links of all the flows bundled in the transaction.
SUBSCRIBER_COUNTER_ID	UINT16	Counter to which each service is mapped. There are 48 subscriber usage counters.
GLOBAL_COUNTER_ID	UINT16	Counter to which each service is mapped. There are 192 global usage counters.
PACKAGE_COUNTER_ID	UINT16	Counter to which each package is mapped. There are 1024 package usage counters.
IP_PROTOCOL	UINT8	IP protocol type.
PROTOCOL_SIGNATURE	UINT32	ID of the protocol signature associated with this session.
ZONE_ID	UINT32	ID of the zone associated with this session.
FLAVOR_ID	UINT32	ID of the flavor associated with this session.
FLOW_CLOSE_MODE	UINT8	Reason for the end of flow.
HASHED_SUBSCRIBER_IP	STRING	Subscriber IP, may be hashed if configured.
USER_AGENT	STRING	User agent field extracted from the HTTP transaction.
HTTP_REFERER	STRING	REFERER extracted from the HTTP transaction.
HTTP_COOKIE	STRING	COOKIE extracted from the HTTP transaction.
SESSION_LINK_ID	INT8	The ID number of the link on which the session was initiated. Values are between 0-X, where X is the corresponding SCE link. X can hav values of 0–7 if there is only one DPI module and 0–15 if there are two DPI modules.

Table 2-7 Anonymized HTTP Transaction Usage RDR Fields (continued)

RDR Field Name	Type	Description
IP_TYPE	UINT8	Defines the IP flow type of the respective RDR. For example, when the flow type is IPv6, the IPv4 address of the RDR will contain the value zero. However, the IPv6 address of the RDR will contain a white space for IPv4 flow type.
SERVERIPv6ADDRESS	STRING	Destination IPv6 address of the reported session. The destination is defined as the server or the listener of the networking session. If this is the subscriber IP, this field may contain a 32-byte string hash, if configured.
CLIENTIPv6ADDRESS	STRING	IPv6 address of the client side of the reported session. The client side is defined as the initiator of the networking session. If this is the subscriber IP, this field may contain a 32-byte string hash, if configured.
ATTRIBUTE INDICATOR	UINT32	Generated if the VSA Fields option is enabled. Identifies the valid attributes from the RDR.
ACCT-MULTI-SESSION-ID	STRING	Generated if the VSA Fields option is enabled. A unique accounting ID used to link multiple related sessions.
ACCT-SESSION-ID	STRING	Generated if the VSA Fields option is enabled. A unique accounting ID used to match the start and stop records in a log file. The start and stop records for a given session contains the same ID. All accounting request packet contains an accounting session ID.
FRAMED-IP-ADDRESS	UINT32	Generated if the VSA Fields option is enabled. Provides the IPv4 address allocated to the subscriber. If this is the subscriber IP, this field may contain a 32-byte string hash, if configured.
CALLED-STATION-ID	STRING	Generated if the VSA Fields option is enabled. Provides the ID of station to which the subscriber is connected for the GPRS access.
3GPP-IMEISV	STRING	Generated if the VSA Fields option is enabled. Provides the international mobility equipment identity (IMEI) of the subscriber. IMEI is a unique identity associated with all the GSM and CDMA subscribers.
3GPP-IMSI	STRING	Generated if the VSA Fields option is enabled. Provides the international mobile subscriber identity (IMSI) of the subscriber. IMSI is a unique ID associated with all the GSM and UMTS network mobile phone subscribers.

Table 2-7 Anonymized HTTP Transaction Usage RDR Fields (continued)

RDR Field Name	Type	Description
3GPP-RAT-TYPE	STRING	Generated if the VSA Fields option is enabled. Indicates the radio access technology (RAT) serving the subscriber equipment.
3GPP-SGSN-ADDRESS	UINT32	Generated if the VSA Fields option is enabled. Indicates the IPv4 address of the serving GPRS support node (SGSN)
3GPP-SGSN-MCC-MNC	STRING	Generated if the VSA Fields option is enabled. Indicates the mobile country code (MCC) and mobile network code (MNC) of the SGSN.
3GPP-USER-LOCATION-INFO	STRING	Generated if the VSA Fields option is enabled. Indicates the location of the equipment.
WIMAX-BSID	STRING	Generated if the VSA Fields option is enabled. Indicates the base station identifier (BSID) of the WiMax network.
3GPP2-MEID	STRING	Generated if the VSA Fields option is enabled. The 3G mobile equipment identifier of a CDMA mobile station equipment.
3GPP2-ESN	STRING	Generated if the VSA Fields option is enabled. The unique electronic serial number of the mobile station equipment assigned by the mobile station manufacturer.
3GPP2-PCF-IP-Address	UINT32	Generated if the VSA Fields option is enabled. The packet control function IP address.
3GPP2-Home-Agent-IP-Addres s	UINT32	Generated if the VSA Fields option is enabled. The IP address of the home agent connected to the mobile station.
Framed-IPv6-Prefix	STRING	This field is supported only on Cisco SCE 8000. The field appears in Cisco SCE 2000, but is a reserved field. Generated if the VSA Fields option is enabled. The IPv6 address prefix allocated to the corresponding subscriber. If this is the subscriber IP, this field may contain a 32-byte string hash, if configured.

RTSP Transaction Usage RDR

The *RTSP_TRANSACTION_USAGE_RDR* is a TUR specifically used for RTSP Transactions.

- RDR Purpose—Log RTSP network transactions for transaction-based billing or offline data mining.
- RDR Default destination—Sent to the Collection Manager, and stored in CSV files.
- RDR Content—Describes a single RTSP transaction; its connection attributes, extracted Layer 7 attributes, duration, and volume.
- RDR Generation Logic—Generated at the end of a session, for all RTSP transactions on packages and services that are configured to generate a Transaction Usage RDR.

  This RDR is not generated for sessions that were blocked by a rule.
- RDR tag—0xf0f0f440 / 4042323008

By default, packages and services are *disabled* from generating this RDR.

This RDR is designed for services and packages where specific, per-transaction RDRs are required (such as, transaction-level billing). It is easy to configure this RDR in error, so that it is generated for every transaction, which may result in an excessive RDR rate.

Note Configure the generation scheme for this RDR with extra care.

Table 2-8 lists the RTSP Transaction Usage RDR fields and their descriptions.

Table 2-8 RTSP Transaction Usage RDR Fields

RDR Field Name	Type	Description
SUBSCRIBER_ID	STRING	Subscriber identification string, introduced through the subscriber management interfaces. It may contain up to 64 characters. For unknown subscribers, this field may contain an empty string.
PACKAGE_ID	INT16	ID of the package assigned to the subscriber whose traffic is being reported. An assigned Package ID is an integer value between 0 and 4999. The value 4999 is reserved for unknown subscribers, and this is the maximum_number_of_packages possible.
SERVICE_ID	INT32	Service classification of the reported session. For example, in the Transaction RDR, this field indicates which service was accessed, and in the Breaching RDR, this field indicates which service was breached.
PROTOCOL_ID	INT16	Unique ID of the protocol associated with the reported session.
SKIPPED_SESSIONS	UINT32	Number of unreported sessions since the previous RDR. Because an RTSP Transaction Usage RDR is generated only at the end of a flow, this field always has the value 1.

Table 2-8 RTSP Transaction Usage RDR Fields (continued)

RDR Field Name	Type	Description
SERVER_IP	UINT32	Destination IP address of the reported session. (The destination is defined as the server or the listener of the networking session.) The IP address is in a 32-bit binary format, but the value is obtained in decimal format in RDR.
SERVER_PORT	UINT16	Destination port number of the TCP/UDP-based networking session. For non-TCP/UDP sessions, this field contains the IP protocol number of the session flow.
ACCESS_STRING	STRING	Layer 7 property, extracted from the transaction.
INFO_STRING	STRING	Layer 7 property, extracted from the transaction.
CLIENT_IP	UINT32	IP address of the client side of the reported session. (The client side is defined as the initiator of the networking session.) The IP address is in a 32-bit binary format, but the value is obtained in decimal format in RDR.
CLIENT_PORT	UINT16	Port number of the client side (initiator) of the TCP/UDP-based networking session. For non-TCP/UDP sessions, this field has the value zero.
INITIATING_SIDE	INT8	Side of the SCE platform on which the initiator of the transaction resides: • 0—Subscriber side • 1—Network side
REPORT_TIME	UINT32	Ending time stamp of this RDR. The field is in UNIX time_t format, which is the number of seconds since midnight of 1 January 1970.
MILLISEC_DURATION	UINT32	Duration, in milliseconds, of the transaction reported in this RDR.
TIME_FRAME	INT8	System supports time-dependent policies, by using different rules for different time frames. This field indicates the time frame during which the RDR was generated. The value of the field can be in the range 0 – 3, indicating which of the four time frames was used.
SESSION_UPSTREAM_ VOLUME	UINT32	Upstream volume of the transaction, in bytes. The volume refers to the aggregated upstream volume on both links of all the flows bundled in the transaction.
SESSION_DOWNSTREAM_ VOLUME	UINT32	Downstream volume of the transaction, in bytes. The volume refers to the aggregated downstream volume on both links of all the flows bundled in the transaction.
SUBSCRIBER_COUNTER_ID	UINT16	Counter to which each service is mapped. There are 48 subscriber usage counters.

Table 2-8 RTSP Transaction Usage RDR Fields (continued)

RDR Field Name	Type	Description
GLOBAL_COUNTER_ID	UINT16	Counter to which each service is mapped. There are 192 global usage counters.
PACKAGE_COUNTER_ID	UINT16	Counter to which each package is mapped. There are 1024 package usage counters.
IP_PROTOCOL	UNIT8	IP protocol type.
PROTOCOL_SIGNATURE	INT32	ID of the protocol signature associated with this session.
ZONE_ID	INT32	ID of the zone associated with this session.
FLAVOR_ID	INT32	ID of the protocol signature with flavor associated with this session.
FLOW_CLOSE_MODE	UINT8	The reason for the end of flow: • 0—TCP_NORMAL_CLOSE • 2—The aging mechanism closed the flow.
RTSP_SESSION_ID	STRING	RTSP session ID as seen on an RTSP SETUP request.
RESPONSE_DATE	STRING	RTSP DESCRIBE date.
TOTAL_ENCODING_RATE	UINT32	Sum of encoding rates of data flows.
NUMBER_OF_VIDEO_ STREAMS	UINT8	Number of video streams for this RTSP session.
NUMBER_OF_AUDIO_ STREAMS	UINT8	Number of audio streams for this RTSP session.
SESSION_TITLE	STRING	Title for this RTSP stream.
SERVER_NAME	STRING	Name of the RTSP server.
SESSION_LINK_ID	INT8	The ID number of the link on which the session was initiated. Values are between 0-X, where X is the corresponding SCE link. X can have values of 0–7 if there is only one DPI module and 0–15 if there are two DPI modules.
IP_TYPE	UINT8	Defines the IP flow type of the respective RDR. For example, when the flow type is IPv6, the IPv4 address of the RDR will contain the value zero. However, the IPv6 address of the RDR will contain a white space for IPv4 flow type.
SERVERIPv6ADDRESS	STRING	Destination IPv6 address of the reported session. The destination is defined as the server or the listener of the networking session.
CLIENTIPv6ADDRESS	STRING	IPv6 address of the client side of the reported session. The client side is defined as the initiator of the networking session.

Related Topics

- Universal RDR Fields, page 2-4

- Anonymized RTSP Transaction Usage RDR, page 2-38

Anonymized RTSP Transaction Usage RDR

The ANONYMIZED_RTSP_TRANSACTION_USAGE_RDR is a TUR specifically used for RTSP Transactions.

- RDR Purpose—Log RTSP network transactions for transaction-based billing or offline data mining, without personal subscriber data.
- RDR Default destination—Sent to the Collection Manager, and stored in CSV files.
- RDR Content—Describes a single RTSP transaction; its connection attributes, extracted Layer 7 attributes, duration, and volume.
- RDR Generation Logic—Generated at the end of a session, for all RTSP transactions on packages and services that are configured to generate a Transaction Usage RDR.

  This RDR is not generated for sessions that were blocked by a rule.
- RDR tag—0xf0f0f542 / 4042323266

By default, packages and services are *disabled* from generating this RDR.

This RDR is designed for services and packages where specific, per-transaction RDRs are required (such as, transaction-level billing). It is easy to configure this RDR in error, so that it is generated for every transaction, which may result in an excessive RDR rate.

Note Configure the generation scheme for this RDR with extra care.

Table 2-9 lists the Anonymized RTSP Transaction Usage RDR fields and their descriptions.

Table 2-9 Anonymized RTSP Transaction Usage RDR Fields

RDR Field Name	Type	Description
HASHED_SUBSCRIBER_ID	STRING	Subscriber identification string, introduced through the subscriber management interfaces, may be passed through hashing algorithm. It may contain up to 64 characters. For unknown subscribers, this field may contain an empty string.
PACKAGE_ID	INT16	ID of the package assigned to the subscriber whose traffic is being reported. An assigned Package ID is an integer value between 0 and 4999. The value 4999 is reserved for unknown subscribers, and this is the maximum_number_of_packages possible.
SERVICE_ID	INT32	Service classification of the reported session. For example, in the Transaction RDR, this field indicates which service was accessed, and in the Breaching RDR, this field indicates which service was breached.
PROTOCOL_ID	INT16	Unique ID of the protocol associated with the reported session.
SKIPPED_SESSIONS	UINT32	Number of unreported sessions since the previous RDR. Because an RTSP Transaction Usage RDR is generated only at the end of a flow, this field always has the value 1.

Table 2-9 Anonymized RTSP Transaction Usage RDR Fields (continued)

RDR Field Name	Type	Description
SERVER_IP	UINT32	Destination IP address of the reported session. (The destination is defined as the server or the listener of the networking session.) The IP address is in a 32-bit binary format, but the value is obtained in decimal format in RDR. If this is the subscriber IP, this field may contain the short-hash of the IP if configured.
SERVER_PORT	UINT16	Destination port number of the TCP/UDP-based networking session. For non-TCP/UDP sessions, this field contains the IP protocol number of the session flow.
ACCESS_STRING	STRING	Layer 7 property, extracted from the transaction.
INFO_STRING	STRING	Layer 7 property, extracted from the transaction.
CLIENT_IP	UINT32	IP address of the client side of the reported session. The client side is defined as the initiator of the networking session. The IP address is in a 32-bit binary format, but the value is obtained in decimal format in RDR. If this is the subscriber IP, this field may contain the short-hash of the IP if configured.
CLIENT_PORT	UINT16	Port number of the client side (initiator) of the TCP/UDP-based networking session. For non-TCP/UDP sessions, this field has the value zero.
INITIATING_SIDE	INT8	Side of the SCE platform on which the initiator of the transaction resides: • 0—Subscriber side • 1—Network side
REPORT_TIME	UINT32	Ending time stamp of this RDR. The field is in UNIX time_t format, which is the number of seconds since midnight of 1 January 1970.
MILLISEC_DURATION	UINT32	Duration, in milliseconds, of the transaction reported in this RDR.
TIME_FRAME	INT8	System supports time-dependent policies, by using different rules for different time frames. This field indicates the time frame during which the RDR was generated. The value of the field can be in the range 0–3, indicating which of the four time frames was used.
SESSION_UPSTREAM_ VOLUME	UINT32	Upstream volume of the transaction, in bytes. The volume refers to the aggregated upstream volume on both links of all the flows bundled in the transaction.

Table 2-9 Anonymized RTSP Transaction Usage RDR Fields (continued)

RDR Field Name	Type	Description
SESSION_DOWNSTREAM_ VOLUME	UINT32	Downstream volume of the transaction, in bytes. The volume refers to the aggregated downstream volume on both links of all the flows bundled in the transaction.
SUBSCRIBER_COUNTER_ID	UINT16	Counter to which each service is mapped. There are 48 subscriber usage counters.
GLOBAL_COUNTER_ID	UINT16	Counter to which each service is mapped. There are 192 global usage counters.
PACKAGE_COUNTER_ID	UINT16	Counter to which each package is mapped. There are 1024 package usage counters.
IP_PROTOCOL	UNIT8	IP protocol type.
PROTOCOL_SIGNATURE	INT32	ID of the protocol signature associated with this session.
ZONE_ID	INT32	ID of the zone associated with this session.
FLAVOR_ID	INT32	ID of the protocol signature with flavor associated with this session.
FLOW_CLOSE_MODE	UINT8	The reason for the end of flow. • 0—TCP_NORMAL_CLOSE • 2—The aging mechanism closed the flow.
RTSP_SESSION_ID	STRING	RTSP session ID as seen on an RTSP SETUP request.
RESPONSE_DATE	STRING	RTSP DESCRIBE date.
TOTAL_ENCODING_RATE	UINT32	Sum of encoding rates of data flows.
NUMBER_OF_VIDEO_ STREAMS	UINT8	Number of video streams for this RTSP session.
NUMBER_OF_AUDIO_ STREAMS	UINT8	Number of audio streams for this RTSP session.
SESSION_TITLE	STRING	Title for this RTSP stream.
SERVER_NAME	STRING	Name of the RTSP server.
SESSION_LINK_ID	INT8	The ID number of the link on which the session was initiated. Values are between 0-X, where X is the corresponding SCE link. X can have values of 0–7 if there is only one DPI module and 0–15 if there are two DPI modules.
IP_TYPE	UINT8	Defines the IP flow type of the respective RDR. For example, when the flow type is IPv6, the IPv4 address of the RDR will contain the value zero. However, the IPv6 address of the RDR will contain a white space for IPv4 flow type.

Table 2-9 Anonymized RTSP Transaction Usage RDR Fields (continued)

RDR Field Name	Type	Description
SERVERIPv6ADDRESS	STRING	Destination IPv6 address of the reported session. The destination is defined as the server or the listener of the networking session. If this is the subscriber IP, this field may contain a 32-byte string hash, if configured.
CLIENTIPv6ADDRESS	STRING	IPv6 address of the client side of the reported session. The client side is defined as the initiator of the networking session. If this is the subscriber IP, this field may contain a 32-byte string hash, if configured.

Related Topics

- Universal RDR Fields, page 2-4
- RTSP Transaction Usage RDR, page 2-34

VoIP Transaction Usage RDR

The VOIP_TRANSACTION_USAGE_RDR is a TUR specifically used for VoIP transactions.

- RDR Purpose—Log VoIP network transactions for transaction-based billing or offline data mining.
- RDR Default destination—Sent to the Collection Manager, and stored in CSV files.
- RDR Content—Describes a single RTSP transaction; its connection attributes, extracted Layer 7 attributes, duration, and volume.
- RDR Generation Logic—Generated at the end of a session, for all transactions on packages and services that are configured to generate such an RDR.

  This RDR is not generated for sessions that were blocked by a rule.
- RDR tag—0xf0f0f46a / 4042323050

By default, packages and services are *disabled* from generating this RDR. You can enable them for specific packages and services.

The VoIP Transaction Usage RDR is enabled automatically when the Transaction Usage RDR is enabled; both RDRs are generated when the session ends. Currently, the VoIP Transaction Usage RDR is generated for H323, Skinny, SIP, and MGCP sessions.

This RDR is designed for services and packages where specific, per-transaction RDRs are required (for example, transaction-level billing). It is easy to configure this RDR, in error, so that it is generated for every transaction, which may result in an excessive RDR rate.

Note Configure the generation scheme for this RDR with extra care.

Table 2-10 lists the VoIP Transaction Usage RDR fields and their descriptions.

Table 2-10 VoIP Transaction Usage RDR Fields

RDR Field Name	Type	Description
SUBSCRIBER_ID	STRING	Subscriber identification string, introduced through the subscriber management interfaces. It may contain up to 64 characters. For unknown subscribers, this field may contain an empty string.
PACKAGE_ID	INT16	ID of the package assigned to the subscriber whose traffic is being reported. An assigned Package ID is an integer value between 0 and 4999. The value 4999 is reserved for unknown subscribers, and this is the maximum_number_of_packages possible.
SERVICE_ID	INT32	Service classification of the reported session. For example, in the Transaction RDR, this field indicates which service was accessed, and in the Breaching RDR, this field indicates which service was breached.
PROTOCOL_ID	INT16	Unique ID of the protocol associated with the reported session.
SKIPPED_SESSIONS	UINT32	Number of unreported sessions since the previous RDR. Because a VoIP Transaction Usage RDR is generated only at the end of a flow, this field always has the value 1.

Table 2-10 VoIP Transaction Usage RDR Fields (continued)

RDR Field Name	Type	Description
SERVER_IP	UINT32	Destination IP address of the reported session. (The destination is defined as the server or the listener of the networking session.) The IP address is in a 32-bit binary format, but the value is obtained in decimal format in RDR.
SERVER_PORT	UINT16	Destination port number of the TCP/UDP-based networking session. For non-TCP/UDP sessions, this field contains the IP protocol number of the session flow.
ACCESS_STRING	STRING	Layer 7 property, extracted from the transaction.
INFO_STRING	STRING	Layer 7 property, extracted from the transaction.
CLIENT_IP	UINT32	IP address of the client side of the reported session. (The client side is defined as the initiator of the networking session.) The IP address is in a 32-bit binary format, but the value is obtained in decimal format in RDR.
CLIENT_PORT	UINT16	Port number of the client side (initiator) of the TCP/UDP-based networking session. For non-TCP/UDP sessions, this field has the value zero.
INITIATING_SIDE	INT8	Side of the SCE platform on which the initiator of the transaction resides: • 0—Subscriber side • 1—Network side
REPORT_TIME	UINT32	Ending time stamp of this RDR. The field is in UNIX time_t format, which is the number of seconds since midnight of 1 January 1970.
MILLISEC_DURATION	UINT32	Duration, in milliseconds, of the transaction reported in this RDR.
TIME_FRAME	INT8	Time frame during which the RDR was generated. The value of the field can be in the range 0 - 3, indicating which of the four time frames was used. The system supports time-dependent policies, by using different rules for different time frames.
SESSION_UPSTREAM_ VOLUME	UINT32	Upstream volume of the transaction, in bytes. The volume refers to the aggregated upstream volume on both links of all the flows bundled in the transaction.
SESSION_DOWNSTREAM_ VOLUME	UINT32	Downstream volume of the transaction, in bytes. The volume refers to the aggregated downstream volume on both links of all the flows bundled in the transaction.
SUBSCRIBER_COUNTER_ID	UINT16	Counter to which each service is mapped. There are 48 subscriber usage counters.
GLOBAL_COUNTER_ID	UINT16	Counter to which each service is mapped. There are 192 global usage counters.

Table 2-10 VoIP Transaction Usage RDR Fields (continued)

RDR Field Name	Type	Description
PACKAGE_COUNTER_ID	UINT16	Counter to which each package is mapped. There are 1024 package usage counters.
IP_PROTOCOL	UINT8	IP protocol type.
PROTOCOL_SIGNATURE	INT32	ID of the protocol signature associated with this session.
ZONE_ID	INT32	ID of the zone associated with this session.
FLAVOR_ID	INT32	ID of the protocol signatures with flavor associated with this session.
FLOW_CLOSE_MODE	UINT8	The ITU-U vendor ID of the application. A value of 0xFFFFFFFF indicates that this field was not found in the traffic.
APPLICATION_ID	UINT32	ITU-U vendor ID of the application. A value of 0xFFFFFFFF indicates that this field was not found in the traffic.
UPSTREAM_PACKET_LOSS (see Note, page 45)	UINT16	Average fractional upstream packet loss for the session, taken from the RTCP flow. (See the note following this table for an explanation of this value.) A value of 0xFFFF indicates that this field is undefined (no RTCP flows were opened).
DOWNSTREAM_PACKET_ LOSS (see Note, page 45)	UINT16	Average fractional downstream packet loss for the session, taken from the RTCP flow. A value of 0xFFFF indicates that this field is undefined (no RTCP flows were opened).
UPSTREAM_AVERAGE_ JITTER (see Note, page 45)	UINT32	Average upstream jitter for the session in units of 1/65 milliseconds, taken from the RTCP flow. A value of 0xFFFFFFFF indicates that this field is undefined (no RTCP flows were opened).
DOWNSTREAM_AVERAGE_ JITTER (see Note, page 45)	UINT32	Average downstream jitter for the session in units of 1/65 milliseconds, taken from the RTCP flow. A value of 0xFFFFFFFF indicates that this field is undefined (no RTCP flows were opened).
CALL_DESTINATION	STRING	Q931 Alias address of the session destination. A value of N/A indicates that this field was not found in the traffic.
CALL_SOURCE	STRING	Q931 Alias address of the session source. A value of N/A indicates that this field was not found in the traffic.
UPSTREAM_PAYLOAD_ TYPE	UINT8	Upstream RTP payload type for the session. A value of 0xFF indicates that this field was not available (no RTP flows were opened).
DOWNSTREAM_PAYLOAD_ TYPE	UINT8	Downstream RTP payload type for the session. A value of 0xFF indicates that this field is undefined (no RTP flows were opened).

Table 2-10 VoIP Transaction Usage RDR Fields (continued)

RDR Field Name	Type	Description
CALL_TYPE	UINT8	Call type (taken from H225 packet). A value of 0xFF indicates that this field is undefined (no RTP flows were opened).
MEDIA_CHANNELS	UINT8	Number of data flows that were opened during the session.
SESSION_LINK_ID	INT8	The ID number of the link on which the session was initiated. Values are between 0-X, where X is the corresponding SCE link. X can have values of 0–7 if there is only one DPI module and 0–15 if there are two DPI modules.
IP_TYPE	UINT8	Defines the IP flow type of the respective RDR. For example, when the flow type is IPv6, the IPv4 address of the RDR will contain the value zero. However, the IPv6 address of the RDR will contain a white space for IPv4 flow type.
SERVERIPv6ADDRESS	STRING	Destination IPv6 address of the reported session. The destination is defined as the server or the listener of the networking session.
CLIENTIPv6ADDRESS	STRING	IPv6 address of the client side of the reported session. The client side is defined as the initiator of the networking session.

Note **Packet Loss**
This field is taken from the RTCP field “fraction lost”. It is the average value of all RTCP packets seen during the flow life for the specified direction. The value is the numerator of a fraction whose denominator is 256. To get the packet loss value as percentage, divide this value by 2.56.

Note **Average Jitter**
This field is taken from the RTCP field “interval jitter”. The reported value is the average value of all RTCP packets seen during the flow life for the specified direction. This value is multiplied by the NTP time-stamp delta (middle 32 bits) and divided by the RTCP time-stamp delta to convert it to normal time units. These two time stamps are also taken from the RTCP packet. The reported value is the average jitter in units of 1/65536 second. To convert to milliseconds, divide by 65.536.

For more information about the RCP/RTCP standard, see RFC 1889.

Related Topics

- Universal RDR Fields, page 2-4
- Anonymized VoIP Transaction Usage RDR, page 2-46

Anonymized VoIP Transaction Usage RDR

The ANONYMIZED_VOIP_TRANSACTION_USAGE_RDR is a TUR specifically used for VoIP transactions.

- RDR Purpose—Log VoIP network transactions for transaction-based billing or offline data mining, without personal subscriber data.
- RDR Default destination—Sent to the Collection Manager, and stored in CSV files.
- RDR Content—Describes a single RTSP transaction; its connection attributes, extracted Layer 7 attributes, duration, and volume.
- RDR Generation Logic—Generated at the end of a session, for all transactions on packages and services that are configured to generate such an RDR.

  This RDR is not generated for sessions that were blocked by a rule.
- RDR tag—0xf0f0f544 / 4042323268

By default, packages and services are *disabled* from generating this RDR. You can enable them for specific packages and services.

The VoIP Transaction Usage RDR is enabled automatically when the Transaction Usage RDR is enabled; both RDRs are generated when the session ends. Currently, the VoIP Transaction Usage RDR is generated for H323, Skinny, SIP, and MGCP sessions.

This RDR is designed for services and packages where specific, per-transaction RDRs are required (for example, transaction-level billing). It is easy to configure this RDR, in error, so that it is generated for every transaction, which may result in an excessive RDR rate.

Note Configure the generation scheme for this RDR with extra care.

Table 2-11 lists the Anonymized VoIP Transaction Usage RDR fields and their descriptions.

Table 2-11 Anonymized VoIP Transaction Usage RDR Fields

RDR Field Name	Type	Description
HASHED_SUBSCRIBER_ID	STRING	Subscriber identification string, introduced through the subscriber management interfaces, may be passed through hashing algorithm. It may contain up to 64 characters. For unknown subscribers, this field may contain an empty string.
PACKAGE_ID	INT16	ID of the package assigned to the subscriber whose traffic is being reported. An assigned Package ID is an integer value between 0 and 4999. The value 4999 is reserved for unknown subscribers, and this is the maximum_number_of_packages possible.
SERVICE_ID	INT32	Service classification of the reported session. For example, in the Transaction RDR, this field indicates which service was accessed, and in the Breaching RDR, this field indicates which service was breached.
PROTOCOL_ID	INT16	Unique ID of the protocol associated with the reported session.

Table 2-11 Anonymized VoIP Transaction Usage RDR Fields (continued)

RDR Field Name	Type	Description
SKIPPED_SESSIONS	UINT32	Number of unreported sessions since the previous RDR. Because a VoIP Transaction Usage RDR is generated only at the end of a flow, this field always has the value 1.
SERVER_IP	UINT32	Destination IP address of the reported session. (The destination is defined as the server or the listener of the networking session.) The IP address is in a 32-bit binary format, but the value is obtained in decimal format in RDR. If this is the subscriber IP, this field may contain the short-hash of the IP if configured.
SERVER_PORT	UINT16	Destination port number of the TCP/UDP-based networking session. For non-TCP/UDP sessions, this field contains the IP protocol number of the session flow.
ACCESS_STRING	STRING	Layer 7 property, extracted from the transaction.
INFO_STRING	STRING	Layer 7 property, extracted from the transaction.
CLIENT_IP	UINT32	IP address of the client side of the reported session. The client side is defined as the initiator of the networking session. The IP address is in a 32-bit binary format, but the value is obtained in decimal format in RDR. If this is the subscriber IP, this field may contain the short-hash of the IP if configured.
CLIENT_PORT	UINT16	Port number of the client side (initiator) of the TCP/UDP-based networking session. For non-TCP/UDP sessions, this field has the value zero.
INITIATING_SIDE	INT8	Side of the SCE platform on which the initiator of the transaction resides: • 0—Subscriber side • 1—Network side
REPORT_TIME	UINT32	Ending time stamp of this RDR. The field is in UNIX time_t format, which is the number of seconds since midnight of 1 January 1970.
MILLISEC_DURATION	UINT32	Duration, in milliseconds, of the transaction reported in this RDR.
TIME_FRAME	INT8	Time frame during which the RDR was generated. The value of the field can be in the range 0 – 3, indicating which of the four time frames was used. The system supports time-dependent policies, by using different rules for different time frames.
SESSION_UPSTREAM_VOLUME	UINT32	Upstream volume of the transaction, in bytes. The volume refers to the aggregated upstream volume on both links of all the flows bundled in the transaction.

Table 2-11 Anonymized VoIP Transaction Usage RDR Fields (continued)

RDR Field Name	Type	Description
SESSION_DOWNSTREAM_VOLUME	UINT32	Downstream volume of the transaction, in bytes. The volume refers to the aggregated downstream volume on both links of all the flows bundled in the transaction.
SUBSCRIBER_COUNTER_ID	UINT16	Counter to which each service is mapped. There are 48 subscriber usage counters.
GLOBAL_COUNTER_ID	UINT16	Counter to which each service is mapped. There are 192 global usage counters.
PACKAGE_COUNTER_ID	UINT16	Counter to which each package is mapped. There are 1024 package usage counters.
IP_PROTOCOL	UINT8	IP protocol type.
PROTOCOL_SIGNATURE	INT32	ID of the protocol signature associated with this session.
ZONE_ID	INT32	ID of the zone associated with this session.
FLAVOR_ID	INT32	ID of the protocol signatures with flavor associated with this session.
FLOW_CLOSE_MODE	UINT8	The ITU-U vendor ID of the application. A value of 0xFFFFFFFF indicates that this field was not found in the traffic.
APPLICATION_ID	UINT32	ITU-U vendor ID of the application. A value of 0xFFFFFFFF indicates that this field was not found in the traffic.
UPSTREAM_PACKET_LOSS (see Note, page 45)	UINT16	Average fractional upstream packet loss for the session, taken from the RTCP flow. A value of 0xFFFF indicates that this field is undefined (no RTCP flows were opened).
DOWNSTREAM_PACKET_LOSS (see Note, page 45)	UINT16	Average fractional downstream packet loss for the session, taken from the RTCP flow. A value of 0xFFFF indicates that this field is undefined (no RTCP flows were opened).
UPSTREAM_AVERAGE_JITTER (see Note, page 45)	UINT32	Average upstream jitter for the session in units of 1/65 milliseconds, taken from the RTCP flow. A value of 0xFFFFFFFF indicates that this field is undefined (no RTCP flows were opened).
DOWNSTREAM_AVERAGE_JITTER (see Note, page 45)	UINT32	Average downstream jitter for the session in units of 1/65 milliseconds, taken from the RTCP flow. A value of 0xFFFFFFFF indicates that this field is undefined (no RTCP flows were opened).
CALL_DESTINATION	STRING	Q931 Alias address of the session destination. A value of N/A indicates that this field was not found in the traffic.
CALL_SOURCE	STRING	Q931 Alias address of the session source. A value of N/A indicates that this field was not found in the traffic.

Table 2-11 Anonymized VoIP Transaction Usage RDR Fields (continued)

RDR Field Name	Type	Description
UPSTREAM_PAYLOAD_TYPE	UINT8	Upstream RTP payload type for the session. A value of 0xFF indicates that this field was not available (no RTP flows were opened).
DOWNSTREAM_PAYLOAD_TYPE	UINT8	Downstream RTP payload type for the session. A value of 0xFF indicates that this field is undefined (no RTP flows were opened).
CALL_TYPE	UINT8	Call type (taken from H225 packet). A value of 0xFF indicates that this field is undefined (no RTP flows were opened).
MEDIA_CHANNELS	UINT8	Number of data flows that were opened during the session.
SESSION_LINK_ID	INT8	The ID number of the link on which the session was initiated. Values are between 0-X, where X is the corresponding SCE link. X can have values of 0–7 if there is only one DPI module and 0–15 if there are two DPI modules.
IP_TYPE	UINT8	Defines the IP flow type of the respective RDR. For example, when the flow type is IPv6, the IPv4 address of the RDR will contain the value zero. However, the IPv6 address of the RDR will contain a white space for IPv4 flow type.
SERVERIPv6ADDRESS	STRING	Destination IPv6 address of the reported session. The destination is defined as the server or the listener of the networking session.
CLIENTIPv6ADDRESS	STRING	IPv6 address of the client side of the reported session. The client side is defined as the initiator of the networking session. If this is the subscriber IP, this field may contain a 32-byte string hash, if configured.

For more information about the RCP/RTCP standard, see RFC 1889.

Related Topics

- Universal RDR Fields, page 2-4
- VoIP Transaction Usage RDR, page 2-42

Video Transaction Usage RDR

The VIDEO_TRANSACTION_USAGE_RDR is a TUR used specifically for video transactions.

- RDR Default destination—Sent to the Collection Manager and stored in CSV format.
- RDR Content—Describes a single video transaction.
- RDR Generation Logic—Generated at the end of a session, for all transactions on all packages and all services if:
  - Packages and services are configured to generate VIDEO_TRANSACTION_USAGE_RDR.
  - VIDEO_TRANSACTION_USAGE_RDRs are enabled.

  This RDR is not generated for sessions that were blocked by a rule.
- RDR tag—0xf0f0f480 / 4042323072

By default, packages and services are disabled from generating this RDR. You can enable them for specific packages and services.

This RDR is designed for services and packages where specific, per-transaction RDRs are required (for example, transaction-level billing). It is easy to configure this RDR in error, so that it is generated for every transaction, which may result in an excessive RDR rate.

Note Configure the generation scheme for this RDR with extra care.

Table 2-12 lists the VIDEO_TRANSACTION_USAGE_RDR fields and their descriptions.

Table 2-12 Video Transaction Usage RDR Fields

RDR Field Name	Type	Description
SUBSCRIBER_ID	STRING	Subscriber identification string, introduced through the subscriber management interfaces. It may contain up to 64 characters. For unknown subscribers, this field may contain an empty string.
PACKAGE_ID	INT16	ID of the package assigned to the subscriber whose traffic is being reported. An assigned Package ID is an integer value between 0 and 4999. The value 4999 is reserved for unknown subscribers, and this is the maximum_number_of_packages possible.
SERVICE_ID	INT32	Service classification of the reported session. For example, in the Transaction RDR, this field indicates which service was accessed, and in the Breaching RDR, this field indicates which service was breached.
PROTOCOL_ID	INT16	Unique ID of the protocol associated with the reported session.
SKIPPED_SESSIONS	UINT32	Number of unreported sessions since the previous RDR. Because an RTSP Transaction Usage RDR is generated only at the end of a flow, this field always has the value 1.

Table 2-12 Video Transaction Usage RDR Fields (continued)

RDR Field Name	Type	Description
SERVER_IP	UINT32	Destination IP address of the reported session. (The destination is defined as the server or the listener of the networking session.) The IP address is in a 32-bit binary format, but the value is obtained in decimal format in RDR.
SERVER_PORT	UINT16	Destination port number of the TCP/UDP-based networking session. For non-TCP/UDP sessions, this field contains the IP protocol number of the session flow.
ACCESS_STRING	STRING	Layer 7 property, extracted from the transaction.
INFO_STRING	STRING	Layer 7 property, extracted from the transaction.
CLIENT_IP	UINT32	IP address of the client side of the reported session. The client side is defined as the initiator of the networking session. The IP address is in a 32-bit binary format, but the value is obtained in decimal format in RDR.
CLIENT_PORT	UINT16	Port number of the client side (initiator) of the TCP/UDP-based networking session. For non-TCP/UDP sessions, this field has the value zero.
INITIATING_SIDE	INT8	Side of the SCE platform on which the initiator of the transaction resides: • 0—Subscriber side • 1—Network side
REPORT_TIME	UINT32	Ending time stamp of this RDR. The field is in UNIX time_t format, which is the number of seconds since midnight of 1 January 1970.
MILLISEC_DURATION	UINT32	Duration, in milliseconds, of the transaction reported in this RDR.
TIME_FRAME	INT8	Time frame during which the RDR was generated. The value of the field can be in the range 0 – 3, indicating which of the four time frames was used. The system supports time-dependent policies, by using different rules for different time frames.
SESSION_UPSTREAM_ VOLUME	UINT32	Upstream volume of the transaction, in bytes. The volume refers to the aggregated upstream volume on both links of all the flows bundled in the transaction.
SESSION_DOWNSTREAM_ VOLUME	UINT32	Downstream volume of the transaction, in bytes. The volume refers to the aggregated downstream volume on both links of all the flows bundled in the transaction.
SUBSCRIBER_COUNTER_ID	UINT16	Counter to which each service is mapped. There are 48 subscriber usage counters.
GLOBAL_COUNTER_ID	UINT16	Counter to which each service is mapped. There are 192 global usage counters.

Table 2-12 Video Transaction Usage RDR Fields (continued)

RDR Field Name	Type	Description
PACKAGE_COUNTER_ID	UINT16	Counter to which each package is mapped. There are 1024 package usage counters.
IP_PROTOCOL	UNIT8	IP protocol type.
PROTOCOL_SIGNATURE	INT32	ID of the protocol signature associated with this session.
ZONE_ID	INT32	ID of the zone associated with this session.
FLAVOR_ID	INT32	ID of the protocol signatures with flavor associated with this session.
FLOW_CLOSE_MODE	UINT8	ITU-U vendor ID of the application. A value of 0xFFFFFFFF indicates that this field was not found in the traffic.
TITLE	STRING	Unique ID of the video.
DURATION	UINT32	Duration of the video in seconds.
ENCODING_RATE	UINT32	Bitrate of the video in bits per second.
RESOLUTION	UINT16	Resolution of the video in seconds.
REFERER	STRING	Not supported.
SESSION_LINK_ID	INT8	The ID number of the link on which the session was initiated. Values are between 0-X, where X is the corresponding SCE link. X can have values of 0–7 if there is only one DPI module and 0–15 if there are two DPI modules.
IP_TYPE	UINT8	Defines the IP flow type of the respective RDR. For example, when the flow type is IPv6, the IPv4 address of the RDR will contain the value zero. However, the IPv6 address of the RDR will contain a white space for IPv4 flow type.
SERVERIPv6ADDRESS	STRING	Destination address of the reported session. The destination is defined as the server or the listener of the networking session.
CLIENTIPv6ADDRESS	STRING	IPv6 address of the client side of the reported session. The client side is defined as the initiator of the networking session.
ATTRIBUTE INDICATOR	UINT32	Generated if the VSA Fields option is enabled. Identifies the valid attributes from the RDR.
ACCT-MULTI-SESSION-ID	STRING	Generated if the VSA Fields option is enabled. A unique accounting ID used to link multiple related sessions.

Table 2-12 Video Transaction Usage RDR Fields (continued)

RDR Field Name	Type	Description
ACCT-SESSION-ID	STRING	Generated if the VSA Fields option is enabled. A unique accounting ID used to match the start and stop records in a log file. The start and stop records for a given session contains the same ID. All accounting request packet contains an accounting session ID.
FRAMED-IP-ADDRESS	UINT32	Generated if the VSA Fields option is enabled. Provides the IPv4 address allocated to the subscriber.
CALLED-STATION-ID	STRING	Generated if the VSA Fields option is enabled. Provides the ID of station to which the subscriber is connected for the GPRS access.
3GPP-IMEISV	STRING	Generated if the VSA Fields option is enabled. Provides the international mobility equipment identity (IMEI) of the subscriber. IMEI is a unique identity associated with all the GSM and CDMA subscribers.
3GPP-IMSI	STRING	Generated if the VSA Fields option is enabled. Provides the international mobile subscriber identity (IMSI) of the subscriber. IMSI is a unique ID associated with all the GSM and UMTS network mobile phone subscribers.
3GPP-RAT-TYPE	STRING	Generated if the VSA Fields option is enabled. Indicates the radio access technology (RAT) serving the subscriber equipment.
3GPP-SGSN-ADDRESS	UINT32	Generated if the VSA Fields option is enabled. Indicates the IPv4 address of the serving GPRS support node (SGSN)
3GPP-SGSN-MCC-MNC	STRING	Generated if the VSA Fields option is enabled. Indicates the mobile country code (MCC) and mobile network code (MNC) of the SGSN.
3GPP-USER-LOCATION-INFO	STRING	Generated if the VSA Fields option is enabled. Indicates the location of the equipment.
WIMAX-BSID	STRING	Generated if the VSA Fields option is enabled. Indicates the base station identifier (BSID) of the WiMax network.
3GPP2-MEID	STRING	Generated if the VSA Fields option is enabled. The 3G mobile equipment identifier of a CDMA mobile station equipment.
3GPP2-ESN	STRING	Generated if the VSA Fields option is enabled. The unique electronic serial number of the mobile station equipment assigned by the mobile station manufacturer.

Table 2-12 Video Transaction Usage RDR Fields (continued)

RDR Field Name	Type	Description
3GPP2-PCF-IP-Address	UINT32	Generated if the VSA Fields option is enabled. The packet control function IP address.
3GPP2-Home-Agent-IP-Address	UINT32	Generated if the VSA Fields option is enabled. The IP address of the home agent connected to the mobile station.
Framed-IPv6-Prefix	STRING	This field is supported only on Cisco SCE 8000. The field appears in Cisco SCE 2000, but is a reserved field. Generated if the VSA Fields option is enabled. Provides the IPv6 address prefix allocated to the subscriber.

Anonymized Video Transaction Usage RDR

The ANONYMIZED_VIDEO_TRANSACTION_USAGE_RDR is a TUR used specifically for video transactions.

- RDR Default destination—Sent to the Collection Manager and stored in CSV format.
- RDR Content—Describes a single video transaction.
- RDR Generation Logic—Generated at the end of a session, for all transactions on all packages and all services if:
  - Packages and services are configured to generate ANONYMIZED_VIDEO_TRANSACTION_USAGE_RDR.
  - ANONYMIZED_VIDEO_TRANSACTION_USAGE_RDRs are enabled.

  This RDR is not generated for sessions that were blocked by a rule.
- RDR tag-0xf0f0f541 / 4042323265

By default, packages and services are disabled from generating this RDR. You can enable them for specific packages and services.

This RDR is designed for services and packages where specific, per-transaction RDRs are required (for example, transaction-level billing). It is easy to configure this RDR in error, so that it is generated for every transaction, which may result in an excessive RDR rate.

Note Configure the generation scheme for this RDR with extra care.

Table 2-13 lists the Anonymized Video Transaction Usage RDR fields and their descriptions.

Table 2-13 Anonymized Video Transaction Usage RDR Fields

RDR Field Name	Type	Description
HASHED_SUBSCRIBER_ID	STRING	Subscriber identification string, introduced through the subscriber management interfaces, may be passed through hashing algorithm. It may contain up to 64 characters. For unknown subscribers, this field may contain an empty string.
PACKAGE_ID	INT16	ID of the package assigned to the subscriber whose traffic is being reported. An assigned Package ID is an integer value between 0 and 4999. The value 4999 is reserved for unknown subscribers, and this is the maximum_number_of_packages possible.
SERVICE_ID	INT32	Service classification of the reported session. For example, in the Transaction RDR, this field indicates which service was accessed, and in the Breaching RDR, this field indicates which service was breached.
PROTOCOL_ID	INT16	Unique ID of the protocol associated with the reported session.

Table 2-13 Anonymized Video Transaction Usage RDR Fields (continued)

RDR Field Name	Type	Description
SKIPPED_SESSIONS	UINT32	Number of unreported sessions since the previous RDR. Because an RTSP Transaction Usage RDR is generated only at the end of a flow, this field always has the value 1.
SERVER_IP	UINT32	Destination IP address of the reported session. The destination is defined as the server or the listener of the networking session. The IP address is in a 32-bit binary format, but the value is obtained in decimal format in RDR. If this is the subscriber IP, this field may contain the short-hash of the IP if configured.
SERVER_PORT	UINT16	Destination port number of the TCP/UDP-based networking session. For non-TCP/UDP sessions, this field contains the IP protocol number of the session flow.
ACCESS_STRING	STRING	Layer 7 property, extracted from the transaction.
INFO_STRING	STRING	Layer 7 property, extracted from the transaction.
CLIENT_IP	UINT32	IP address of the client side of the reported session. The client side is defined as the initiator of the networking session. The IP address is in a 32-bit binary format, but the value is obtained in decimal format in RDR. If this is the subscriber IP, this field may contain the short-hash of the IP if configured.
CLIENT_PORT	UINT16	Port number of the client side (initiator) of the TCP/UDP-based networking session. For non-TCP/UDP sessions, this field has the value zero.
INITIATING_SIDE	INT8	Side of the SCE platform on which the initiator of the transaction resides: • 0—Subscriber side • 1—Network side
REPORT_TIME	UINT32	Ending time stamp of this RDR. The field is in UNIX time_t format, which is the number of seconds since midnight of 1 January 1970.
MILLISEC_DURATION	UINT32	Duration, in milliseconds, of the transaction reported in this RDR.
TIME_FRAME	INT8	Time frame during which the RDR was generated. The value of the field can be in the range 0 – 3, indicating which of the four time frames was used. The system supports time-dependent policies, by using different rules for different time frames.
SESSION_UPSTREAM_ VOLUME	UINT32	Upstream volume of the transaction, in bytes. The volume refers to the aggregated upstream volume on both links of all the flows bundled in the transaction.

Table 2-13 Anonymized Video Transaction Usage RDR Fields (continued)

RDR Field Name	Type	Description
SESSION_DOWNSTREAM_VOLUME	UINT32	Downstream volume of the transaction, in bytes. The volume refers to the aggregated downstream volume on both links of all the flows bundled in the transaction.
SUBSCRIBER_COUNTER_ID	UINT16	Counter to which each service is mapped. There are 48 subscriber usage counters.
GLOBAL_COUNTER_ID	UINT16	Counter to which each service is mapped. There are 192 global usage counters.
PACKAGE_COUNTER_ID	UINT16	Counter to which each package is mapped. There are 1024 package usage counters.
IP_PROTOCOL	UNIT8	IP protocol type.
PROTOCOL_SIGNATURE	INT32	ID of the protocol signature associated with this session.
ZONE_ID	INT32	ID of the zone associated with this session.
FLAVOR_ID	INT32	ID of the protocol signatures with flavor associated with this session.
FLOW_CLOSE_MODE	UINT8	ITU-U vendor ID of the application. A value of 0xFFFFFFFF indicates that this field was not found in the traffic.
TITLE	STRING	Not supported.
DURATION	UINT32	Not supported.
ENCODING_RATE	UINT32	Not supported.
RESOLUTION	UINT32	Not supported.
REFERER	STRING	Not supported.
SESSION_LINK_ID	INT8	The ID number of the link on which the session was initiated. Values are between 0-X, where X is the corresponding SCE link. X can have values of 0–7 if there is only one DPI module and 0–15 if there are two DPI modules.
IP_TYPE	UINT8	Defines the IP flow type of the respective RDR. For example, when the flow type is IPv6, the IPv4 address of the RDR will contain the value zero. However, the IPv6 address of the RDR will contain a white space for IPv4 flow type.
SERVERIPv6ADDRESS	STRING	Destination IPv6 address of the reported session. The destination is defined as the server or the listener of the networking session. If this is the subscriber IP, this field may contain a 32-byte string hash, if configured.

Table 2-13 Anonymized Video Transaction Usage RDR Fields (continued)

RDR Field Name	Type	Description
CLIENTIPv6ADDRESS	STRING	IPv6 address of the client side of the reported session. The client side is defined as the initiator of the networking session. If this is the subscriber IP, this field may contain a 32-byte string hash, if configured.
ATTRIBUTE INDICATOR	UINT32	Generated if the VSA Fields option is enabled. Identifies the valid attributes from the RDR.
ACCT-MULTI-SESSION-ID	STRING	Generated if the VSA Fields option is enabled. A unique accounting ID used to link multiple related sessions.
ACCT-SESSION-ID	STRING	Generated if the VSA Fields option is enabled. A unique accounting ID used to match the start and stop records in a log file. The start and stop records for a given session contains the same ID. All accounting request packet contains an accounting session ID.
FRAMED-IP-ADDRESS	UINT32	Generated if the VSA Fields option is enabled. Provides the IPv4 address allocated to the subscriber. If this is the subscriber IP, this field may contain a 32-byte string hash, if configured.
CALLED-STATION-ID	STRING	Generated if the VSA Fields option is enabled. Provides the ID of station to which the subscriber is connected for the GPRS access.
3GPP-IMEISV	STRING	Generated if the VSA Fields option is enabled. Provides the international mobility equipment identity (IMEI) of the subscriber. IMEI is a unique identity associated with all the GSM and CDMA subscribers.
3GPP-IMSI	STRING	Generated if the VSA Fields option is enabled. Provides the international mobile subscriber identity (IMSI) of the subscriber. IMSI is a unique ID associated with all the GSM and UMTS network mobile phone subscribers.
3GPP-RAT-TYPE	STRING	Generated if the VSA Fields option is enabled. Indicates the radio access technology (RAT) serving the subscriber equipment.
3GPP-SGSN-ADDRESS	UINT32	Generated if the VSA Fields option is enabled. Indicates the IPv4 address of the serving GPRS support node (SGSN)
3GPP-SGSN-MCC-MNC	STRING	Generated if the VSA Fields option is enabled. Indicates the mobile country code (MCC) and mobile network code (MNC) of the SGSN.

Table 2-13 Anonymized Video Transaction Usage RDR Fields (continued)

RDR Field Name	Type	Description
3GPP-USER-LOCATION-INFO	STRING	Generated if the VSA Fields option is enabled. Indicates the location of the equipment.
WIMAX-BSID	STRING	Generated if the VSA Fields option is enabled. Indicates the base station identifier (BSID) of the WiMax network.
3GPP2-MEID	STRING	Generated if the VSA Fields option is enabled. The 3G mobile equipment identifier of a CDMA mobile station equipment.
3GPP2-ESN	STRING	Generated if the VSA Fields option is enabled. The unique electronic serial number of the mobile station equipment assigned by the mobile station manufacturer.
3GPP2-PCF-IP-Address	UINT32	Generated if the VSA Fields option is enabled. The packet control function IP address.
3GPP2-Home-Agent-IP-Addres s	UINT32	Generated if the VSA Fields option is enabled. The IP address of the home agent connected to the mobile station.
Framed-IPv6-Prefix	STRING	This field is supported only on Cisco SCE 8000. The field appears in Cisco SCE 2000, but is a reserved field. Generated if the VSA Fields option is enabled. Provides the IPv6 address prefix allocated to the subscriber. If this is the subscriber IP, this field may contain a 32-byte string hash, if configured.

Generic Usage RDR

GENERIC_USAGE_RDR has a fixed structure with a unique tag, which allows the one-time creation of a database table to be used for various future RDRs.

The Generic Usage RDR is composed of universal fields like any other RDR, generic fields for all GUR RDRs, and fields for future use.

- RDR Purpose—Provides a generic template from which other Usage RDRs can be created.
- RDR Default destination—Varies depending on the specific Usage RDR created from this template
- RDR Content—Varies depending on the specific Usage RDR created from this template.
- RDR Generation Logic—Not generated, is provided as a template for creating other RDRs.
- RDR tag—0xf0f0f090 / 4042322064

Table 2-14 lists the Generic Usage RDR fields and their descriptions.

Table 2-14 Generic Usage RDR Fields

Key/Data	RDR Field Name	Type	Description
Key	GUR_TYPE	INT32	Type of the GUR—defines the usage of the rest of the fields.
Key	LINK_ID	INT8	Numeric value associated with the reported network link. Possible values are 0 and 1 (referring to physical links 1 and 2, respectively). For future use.
Key	GENERATOR_ID	INT8	Numeric value identifying the processor generating the RDR. Possible values are 0 – 3.
Key	GLOBAL_COUNTER_ID	UINT16	Counter to which each service is mapped. There are 192 global usage counters
Key	SUBSCRIBER_COUNTER_ID	UINT16	Counter to which each service is mapped. There are 48 subscriber usage counters.
Key	PACKAGE_COUNTER_ID	UINT16	Counter to which each package is mapped. There are 1024 package usage counters.
Key	SUBSCRIBER_ID	STRING	Subscriber identification string, introduced through the subscriber management interfaces. It may contain up to 64 characters. For unknown subscribers, this field may contain an empty string.
Key	PACKAGE_ID	INT16	ID of the package assigned to the subscriber whose traffic is being reported. An assigned Package ID is an integer value between 0 and 4999. The value 4999 is reserved for unknown subscribers, and this is the maximum_number_of_packages possible.
Key	SERVICE_ID	INT32	Service classification of the reported session. For example, in the Transaction RDR, this field indicates which service was accessed, and in the Breaching RDR, this field indicates which service was breached.
Key	PROTOCOL_ID	INT16	Unique ID of the protocol associated with the reported session.
Key	SIGNATURE_ID	INT32	ID of the protocol signature associated with this session.

Table 2-14 Generic Usage RDR Fields (continued)

Key/Data	RDR Field Name	Type	Description
Key	DESTINATION_IP	UINT32	• SIP—Destination IP address of RTP flow. • Skype—Destination IP address of Skype flow.
Key	DESTINATION_PORT	UINT16	• SIP—Destination port of RTP flow. • Skype—Destination port of Skype flow.
Key	SOURCE_IP	UINT32	• SIP—Source IP address of RTP flow. • Skype—Source IP address of Skype flow.
Key	SOURCE_PORT	UINT16	• SIP—Source port of RTP flow. • Skype—Source port of Skype flow.
Key	INITIATING_SIDE	INT8	Side of the SCE platform on which the initiator of the transaction resides: • 0—Subscriber side • 1—Network side For Skype, this value indicates the initiating side of the flow, and not necessarily the initiating side of the voice call.
Key	ZONE_ID	INT32	ID of the zone associated with this session.
Key	FLAVOR_ID	INT32	ID of protocol signatures with flavor associated with this session.
Key	SESSION_ID	UINT32	• SIP—Flow-context ID of the control flow. • Skype—Flow-context ID of the flow.
Key	START_TIME	UINT32	Flow start time.
Key	END_TIME	UINT32	Ending time stamp of this RDR. The field is in UNIX time_t format, which is the number of seconds since midnight of 1 January 1970.
Key	ACCESS_STRING	STRING	Layer 7 property, extracted from the transaction.
Key	INFO_STRING	STRING	Layer 7 property, extracted from the transaction.
Key	For future use	INT32	—
Key	For future use	INT32	—
Key	For future use	INT32	—
Key	For future use	INT32	—
Key	For future use	STRING	—
Key	For future use	STRING	—
Data	UPSTREAM_VOLUME	UINT32	Aggregated upstream volume of all sessions, in kilobytes, for the current reporting period.
Data	DOWNSTREAM_VOLUME	UINT32	Aggregated downstream volume of all sessions, in kilobytes, for the current reporting period.
Data	TOTAL_VOLUME	UINT32	Aggregated total volume of all sessions, in kilobytes, for the current reporting period.

Table 2-14 Generic Usage RDR Fields (continued)

Key/Data	RDR Field Name	Type	Description
Data	SESSIONS	UINT32	Aggregated number of sessions for the reported service for the current reporting period.
Data	SECONDS	UINT32	Aggregated number of session seconds for the reported service for the current reporting period.
Data	CONCURRENT_SESSIONS	UINT32	Number of sessions using the reported service now.
Data	ACTIVE_SUBSCRIBERS	UINT32	Number of subscribers using the reported service now.
Data	TOTAL_ACTIVE_SUBSCRIBERS	UINT32	Number of subscribers in the system now.
Data	CONFIGURED_DURATION	UINT32	Configured period for periodic RDRs, in seconds, between successive RDRs.
Data	DURATION	UINT32	• This release—Not implemented (always the same as CONFIGURED_DURATION). • Future releases—Indicates the number of seconds that have passed since the previous SUBSCRIBER_USAGE_RDR.
Data	For future use	INT32	—
Data	For future use	INT32	—
Data	For future use	INT32	—
Data	For future use	INT32	—

Using the Generic Usage RDR to Report IPv6 Usage

The Generic Usage RDR (GUR) is used to report both pure IPv6 and tunneled IPv6. The former is reported per device, and the latter per RUC.

Both reports use the GUR type "1". RDR Generation Logic is based on the user-defined configuration of the Link Usage Report.

Note Effective with Cisco SCE Release 4.1.0, the GENERIC_USAGE_RDR supports L2TP IPv6 over IPv4 tunneling protocol along with other tunneling protocols such as, 6to4, 6rd, and so on, on Cisco SCE 8000 devices.

Table 2-15 describes the specific fields of the pure-IPv6 and tunneled-IPv6 reports. (Any GUR fields not listed in the table are not used.)

Table 2-15 Generic Usage RDR Fields for IPv6 Usage

GUR Fields	Fields for Pure IPv6	Fields for Tunneled IPv6
GUR_TYPE	IPV6_TYPE (0x00000001)	IPV6_TYPE (0x00000001)
LINK_ID	—	LINK_ID
GENERATOR_ID	GENERATOR_ID	GENERATOR_ID
GLOBAL_COUNTER_ID	—	GLOBAL_COUNTER_ID
END_TIME	END_TIME	END_TIME
For future use	PURE_IPV6 (0x00000001)	TUNNELED_IPV6 (0x00000002)
UPSTREAM_VOLUME	—	UPSTREAM_VOLUME
DOWNSTREAM_VOLUME	—	DOWNSTREAM_VOLUME
TOTAL_VOLUME	TOTAL_VOLUME	TOTAL_VOLUME
SESSIONS	—	SESSIONS
SECONDS	—	SECONDS
CONCURRENT_SESSIONS	—	CONCURRENT_SESSIONS
ACTIVE_SUBSCRIBERS	—	ACTIVE_SUBSCRIBERS
TOTAL_ACTIVE_ SUBSCRIBERS	—	TOTAL_ACTIVE_ SUBSCRIBERS
CONFIGURED_DURATION	CONFIGURED_DURATION	CONFIGURED_DURATION
DURATION	DURATION	DURATION

Subscriber Usage RDR

The SUBSCRIBER_USAGE_RDR summarizes the activity of a single subscriber on a specific service for the last user-configured number of minutes.

- RDR Purpose—Compare subscribers for the Top Subscribers report, and create daily subscriber usage summary records.
- RDR Default destination—Sent to the Collection Manager, and processed by the Topper Adapter, which stores the processing results in the database and in CSV files. The Cisco Insight tool uses the database records for creating the Top Subscribers reports.
- RDR Content—Summary of the activity of a single subscriber on a defined service for the last user-configured number of minutes. This summary includes the aggregated number of flows, the total volume, and duration.
- RDR Generation Logic—Generated periodically, at user-configured intervals, for each subscriber. A separate RDR is generated for each service usage counter. The RDR is generated only if the subscriber consumed resources associated with the service usage counter during the current reporting period.

  At fixed, user-configurable intervals (for example, every 30 minutes), there is a periodic SUBSCRIBER_USAGE_RDR generation point. Whether a Subscriber Usage RDR for a particular subscriber is generated depends on the following:

  - If the subscriber consumed resources associated with a service usage counter since the previous RDR generation point, a Subscriber Usage RDR is generated.
  - If the subscriber did not consume resources associated with a service usage counter since the previous RDR generation point, no Subscriber Usage RDR is generated.

Note Unlike other Usage RDRs, the generation logic for Subscriber Usage RDRs does not use the zeroing methodology.

Subscriber Usage RDRs may also be generated in the following situations:

- The subscriber performed a logout in a subscriber-integrated installation or was unintroduced from the SCE platform:
  - If the subscriber consumed resources associated with a service usage counter since the previous Subscriber Usage RDR, a Subscriber Usage RDR is generated.
  - If the subscriber did not consume resources since the previous RDR, no RDR is generated for that service usage counter.
- RDR tag—0xf0f0f000 / 4042321920

The Subscriber Usage RDRs are enabled by default. Disabling the RDRs disables Top Subscriber reports.

The default interval for SUR is every 10 minutes and the default total rate is 200 SURs per second.

Table 2-16 lists the Subscriber Usage RDR fields and their descriptions.

Table 2-16 Subscriber Usage RDR Fields

RDR Field Name	Type	Description
SUBSCRIBER_ID	STRING	The subscriber identification string, introduced through the subscriber management interfaces. It may contain up to 64 characters. For unknown subscribers, this field may contain an empty string.
PACKAGE_ID	INT16	The ID of the package assigned to the subscriber whose traffic is being reported. An assigned Package ID is an integer value between 0 and 4999. The value 4999 is reserved for unknown subscribers, and this is the maximum_number_of_packages possible.
SERVICE_USAGE_ COUNTER_ID_	UINT16	Counter to which each service is mapped. There are 32 counters in the subscriber scope.
BREACH_STATE	UINT8	Indicates whether the quota allocated to the subscriber was breached: • 0—Not breached • 1—Breached Holds the breach state of a service. However, this RDR reports usage counters, which cannot be breached, so the value is always zero.
REASON	UINT8	Reason for RDR generation: • 0—Period time passed • 1—Subscriber logout • 3—Wraparound • 5—Subscriber VLink change • 7—Subscriber package change
CONFIGURED_DURATION	UINT32	Configured period for periodic RDRs, in seconds, between successive RDRs.
DURATION	UINT32	Indicates the number of seconds that have passed since the previous Subscriber Usage RDR.
END_TIME	UINT32	Ending time stamp of this RDR. The field is in UNIX time_t format, which is the number of seconds since midnight of 1 January 1970.
UPSTREAM_VOLUME	UINT32	Aggregated upstream volume on both links of all sessions, in kilobytes, for the current reporting period. If the volume is less than one kilobyte, the RDR shows the volume as zero.
DOWNSTREAM_VOLUME	UINT32	Aggregated downstream volume on both links of all sessions, in kilobytes, for the current reporting period.
SESSIONS	UINT32	Aggregated number of sessions for the reported service, for the current reporting period.
SECONDS	UINT32	Aggregated number of session seconds for the reported service, for the current reporting period.

Table 2-16 Subscriber Usage RDR Fields (continued)

RDR Field Name	Type	Description
UP_VLINK	INT16	Up VLINK the subscriber is mapped to. (Is valid only in CMTS-aware mode.
DOWN_VLINK	INT16	Down VLINK the subscriber is mapped to. (Is valid only in CMTS-aware mode.)
OS_FINGER_PRINTING	STRING	Aggregated Operating Systems of the subscriber.
IP_TYPE	UINT8	Defines the IP version of the flows for which the report is generated. Possible values are 0, 1, and 3 where 0 means IPv4, 1 means IPv6, and 3 means DS-Lite.
RESERVED_2	UINT32	Reserved for future compatibility.
ATTRIBUTE INDICATOR	UINT32	Generated if the VSA Fields option is enabled. Identifies the valid attributes from the RDR.
ACCT-MULTI-SESSION-ID	STRING	Generated if the VSA Fields option is enabled. A unique accounting ID used to link multiple related sessions.
ACCT-SESSION-ID	STRING	Generated if the VSA Fields option is enabled. A unique accounting ID used to match the start and stop records in a log file. The start and stop records for a given session contains the same ID. All accounting request packet contains an accounting session ID.
FRAMED-IP-ADDRESS	UINT32	Generated if the VSA Fields option is enabled. Provides the IPv4 address allocated to the subscriber.
CALLED-STATION-ID	STRING	Generated if the VSA Fields option is enabled. Provides the ID of station to which the subscriber is connected for the GPRS access.
3GPP-IMEISV	STRING	Generated if the VSA Fields option is enabled. Provides the international mobility equipment identity (IMEI) of the subscriber. IMEI is a unique identity associated with all the GSM and CDMA subscribers.
3GPP-IMSI	STRING	Generated if the VSA Fields option is enabled. Provides the international mobile subscriber identity (IMSI) of the subscriber. IMSI is a unique ID associated with all the GSM and UMTS network mobile phone subscribers.
3GPP-RAT-TYPE	STRING	Generated if the VSA Fields option is enabled. Indicates the radio access technology (RAT) serving the subscriber equipment.
3GPP-SGSN-ADDRESS	UINT32	Generated if the VSA Fields option is enabled. Indicates the IPv4 address of the serving GPRS support node (SGSN)

Table 2-16 Subscriber Usage RDR Fields (continued)

RDR Field Name	Type	Description
3GPP-SGSN-MCC-MNC	STRING	Generated if the VSA Fields option is enabled. Indicates the mobile country code (MCC) and mobile network code (MNC) of the SGSN.
3GPP-USER-LOCATION-INFO	STRING	Generated if the VSA Fields option is enabled. Indicates the location of the equipment.
WIMAX-BSID	STRING	Generated if the VSA Fields option is enabled. Indicates the base station identifier (BSID) of the WiMax network.
3GPP2-MEID	STRING	Generated if the VSA Fields option is enabled. The 3G mobile equipment identifier of a CDMA mobile station equipment.
3GPP2-ESN	STRING	Generated if the VSA Fields option is enabled. The unique electronic serial number of the mobile station equipment assigned by the mobile station manufacturer.
3GPP2-PCF-IP-Address	UINT32	Generated if the VSA Fields option is enabled. The packet control function IP address.
3GPP2-Home-Agent-IP-Address	UINT32	Generated if the VSA Fields option is enabled. The IP address of the home agent connected to the mobile station.
Framed-IPv6-Prefix	STRING	This field is supported only on Cisco SCE 8000. The field appears in Cisco SCE 2000, but is a reserved field. Generated if the VSA Fields option is enabled. Provides the IPv6 address prefix allocated to the subscriber.

Related Topics

- Periodic RDR Zero Adjustment Mechanism, page 2-152

Real-Time Subscriber Usage RDR

The REALTIME_SUBSCRIBER_USAGE_RDR summarizes the activity of a single subscriber on a specific service for the last user-configured number of minutes.

- RDR Purpose—Create detailed subscriber-level reports of network usage per service.
- RDR Default destination—Sent to the Collection Manager, stored in the database, and used by the Cisco Insight tool for subscriber usage reports such as the Subscriber Bandwidth per Service report.
- RDR Content—Summary of the activity of a single subscriber on a specific service for the last user-configured number of minutes, including aggregated number of flows, total volume, and duration.
- RDR Generation Logic—Generated periodically, at user-configured intervals, for each subscriber that has real-time monitoring enabled. A separate RDR is generated for each service usage counter. The RDR is generated only if the subscriber consumed resources associated with the service usage counter during the current reporting period.

Note A Real-Time Subscriber Usage RDR is generated only for those subscribers with real-time monitoring enabled. For information about enabling real-time monitoring, see the "Additional Management Tools and Interfaces" chapter of *Cisco Service Control Application for Broadband User Guide*.

At fixed, user-configurable intervals (for example, every 5 minutes), there is a periodic REALTIME_SUBSCRIBER_USAGE_RDR generation point. The REALTIME_SUBSCRIBER_USAGE_RDR reports the same usage information as the SUBSCRIBER_USAGE_RDR, but is generated more frequently to provide a more detailed picture of subscriber activity. Cisco Insight uses this RDR to generate reports on the activities of single subscribers over time.

Whether a Real-Time Subscriber Usage RDR for a particular subscriber is generated depends on the following:

- If the subscriber consumed resources associated with a service usage counter since the previous RDR generation point, a Real-Time Subscriber Usage RDR is generated.
- If the subscriber did not consume resources associated with a service usage counter since the previous RDR generation point, no Real-Time Subscriber Usage RDR is generated now.

  However, the generation logic for Subscriber Usage RDRs uses the zeroing methodology (as described in the "Periodic RDR Zero Adjustment Mechanism" section on page 2-152). If the subscriber consumes resources associated with the service usage counter at some later time, this causes the immediate generation of either one or two zero-consumption Real-Time Subscriber Usage RDRs (in addition to the eventual generation of the Real-Time Subscriber Usage RDR associated with this latest consumption of resources).

  - If there was only one interval (for example, 0805–0810) for which there was no subscriber consumption of resources, only one zero-consumption Real-Time Subscriber Usage RDR is generated.
  - If there were multiple consecutive intervals (for example, 0805–0810, 0810–0815, 0815–0820, 0820–0825) for which there was no subscriber consumption of resources, two zero-consumption Real-Time Subscriber Usage RDRs are generated—one for the first such time interval (0805–0810) and one for the last (0820–0825).

Real-Time Subscriber Usage RDRs may also be generated in the following situations:

- The subscriber performed a logout in a subscriber-integrated installation or was unintroduced from the SCE platform:
  - If the subscriber consumed resources associated with a service usage counter since the previous Real-Time Subscriber Usage RDR, a Real-Time Subscriber Usage RDR is generated and then a zero-consumption Real-Time Subscriber Usage RDR is generated.
  - If the subscriber consumed resources associated with a service usage counter since the previous Real-Time Subscriber Usage RDR, a Real-Time Subscriber Usage RDR is generated and then a zero-consumption Real-Time Subscriber Usage RDR is generated.

A zero-consumption Real-Time Subscriber Usage RDR is also generated for a subscriber in the following situations:

- The subscriber performed a login in a subscriber-integrated installation or was introduced from the SCE platform:
  - Before the first Real-Time Subscriber Usage RDRs reporting actual consumption are generated, a zero-consumption Real-Time Subscriber Usage RDR is generated.
- RDR tag—0xf0f0f002 / 4042321922

Real-Time Subscriber Usage RDRs (RTSUR) are generated only for those subscribers with real-time monitoring enabled. By default, it is disabled for all subscribers. The default interval is RTSUR every 1 minute. The default total rate is 100 RTSURs per second.

Table 2-17 lists the Real-Time Subscriber Usage RDR fields and their descriptions.

Table 2-17 Real-Time Subscriber Usage RDR Fields

RDR Field Name	Type	Description
SUBSCRIBER_ID	STRING	The subscriber identification string, introduced through the subscriber management interfaces. It may contain up to 64 characters. For unknown subscribers, this field may contain an empty string.
PACKAGE_ID	INT16	The ID of the package assigned to the subscriber whose traffic is being reported. An assigned Package ID is an integer value between 0 and 4999. The value 4999 is reserved for unknown subscribers, and this is the maximum_number_of_packages possible.
SERVICE_USAGE_ COUNTER_ID	UINT16	Counter to which each service is mapped. There are 32 counters in the subscriber scope.
AGGREGATION_OBJECT_ ID	INT16	Externally assigned: • 0—Offline subscriber • 1—Online subscriber
BREACH_STATE	UINT8	Indicates whether the quota allocated for the subscriber was breached: • 0—Not breached • 1—Breached Holds the breach state of a service. However, this RDR reports usage counters, which cannot be breached, so the value is always zero.

Table 2-17 Real-Time Subscriber Usage RDR Fields (continued)

RDR Field Name	Type	Description
REASON	UINT8	Reason for RDR generation: • 0—Period time passed • 1—Subscriber logout • 3—Wraparound • 5—Subscriber VLink change • 7—Subscriber Package Change
CONFIGURED_DURATION	UINT32	Configured period for periodic RDRs, in seconds, between successive RDRs.
DURATION	UINT32	Indicates the number of seconds that have passed since the previous Real-Time Subscriber Usage RDR. **Note** This field is not valid for zeroing RDR.
END_TIME	UINT32	Ending time stamp of this RDR. The field is in UNIX time_t format, which is the number of seconds since midnight of 1 January 1970.
UPSTREAM_VOLUME	UINT32	Aggregated upstream volume on both links of all sessions, in kilobytes, for the current reporting period.
DOWNSTREAM_VOLUME	UINT32	Aggregated downstream volume on both links of all sessions, in kilobytes, for the current reporting period.
SESSIONS	UINT32	Aggregated number of sessions for the reported service, for the current reporting period.
SECONDS	UINT32	Aggregated number of session seconds for the reported service, for the current reporting period.
OS_FINGER_PRINTING	STRING	Aggregated Operating Systems of the subscriber.
IP_TYPE	UINT8	Defines the IP version of the flows for which the report is generated. Possible values are 0, 1, and 3 where 0 means IPv4, 1 means IPv6, and 3 means DS-Lite.

Related Topics

- Periodic RDR Zero Adjustment Mechanism, page 2-152

Link Usage RDR

The LINK_USAGE_RDR summarizes the activity on one of the SCE links for a specific service for the last user-configured number of minutes.

- RDR Purpose—Create link-level reports of network usage per service.
- RDR Default destination—Sent to the Collection Manager, stored in the database, and used by Cisco Insight for global usage reports such as the Global Bandwidth per Service report, and subscriber demographics reports, such as the Active Subscribers per Service report.
- RDR Content—Summary of the activity on one of the SCE links for a specific service for the last user-configured minutes, including aggregated number of flows, total volume, duration, and active subscribers.
- RDR Generation Logic—Generated periodically, at user-configured intervals, for each link. A separate RDR is generated for each service usage counter. The RDR is generated only if resources associated with the service usage counter were consumed during the current reporting period.

  At fixed, user-configurable intervals (for example, every 30 minutes), there is a periodic LINK_USAGE_RDR generation point. Whether a Link Usage RDR is generated depends on the following:

  - If network resources associated with a service usage counter were consumed since the previous RDR generation point, a Link Usage RDR is generated.
  - If network resources associated with a service usage counter were not consumed since the previous RDR generation point, no Link Usage RDR is generated.

    However, the generation logic for Link Usage RDRs uses the zeroing methodology (as described in the "Periodic RDR Zero Adjustment Mechanism" section on page 2-152). If network resources associated with the service are again consumed at some later time, this causes the immediate generation of either one or two zero-consumption Link Usage RDRs (in addition to the eventual generation of the Link Usage RDR associated with this latest consumption of network resources).
  - If there was only one interval (for example, 0830–0900) for which there was no consumption of network resources, only one zero-consumption Link Usage RDR is generated.
  - If there were multiple consecutive intervals (for example, 0830–0900, 0900–0930, 0930–1000, 1000–1030) for which there was no consumption of network resources, two zero-consumption Link Usage RDR are generated—one for the first such time interval (0830–0900) and one for the last (1000–1030).

Note A separate RDR is generated for each link (on a single traffic processor) in the SCE platform, where each RDR represents the total traffic processed and analyzed by that processor (for the specified service usage counter). To compute the total traffic in any given time frame, take the sum of traffic of the RDRs of all the processors.

- RDR tag—0xf0f0f005 / 4042321925

Link Usage RDRs (LUR) are enabled by default. Disabling LURs eliminates global usage reports as well as subscriber demographics reports. Default interval for LURs is every 5 minutes. Increasing this interval can enhance the time granularity of LUR-based reports.

Table 2-18 lists the Link Usage RDR fields and their descriptions.

Table 2-18 Link Usage RDR Fields

RDR Field Name	Type	Description
LINK_ID	INT8	A numeric value associated with the reported network link. Possible values are 0 and 1 (referring to physical links 1 and 2, respectively). For future use.
GENERATOR_ID	INT8	A numeric value identifying the processor generating the RDR. **Cisco SCE 2000** 0—RDR aggregation is enabled. 1 to 3—RDR aggregation is disabled. These numbers identify the processor generating the RDR. RDR aggregation is disabled by default on Cisco SCE 2000 devices. **Cisco SCE 8000** 0—RDR aggregation is enabled. 1 to 12—RDR aggregation is disabled. These numbers identify the processor generating the RDR if the Cisco SCE has one Service Control Module. 1 to 24—RDR aggregation is disabled. These numbers identify the processor generating the RDR if the Cisco SCE has two Service Control Modules. RDR aggregation is enabled by default on Cisco SCE 8000 devices. **Note** To disable RDR aggregation, use the **no periodic-records aggregate-by-cpu all** command from the management interface configuration mode.
SERVICE_USAGE_ COUNTER_ID	UINT16	Counter to which each service is mapped. There are 64 global usage counters.
CONFIGURED_DURATION	UINT32	Configured period for periodic RDRs, in seconds, between successive RDRs.
DURATION	UINT32	• This release—Not implemented (always the same as CONFIGURED_DURATION). • Future release—Indicates the number of seconds that have passed since the previous SUBSCRIBER_USAGE_RDR.
END_TIME	UINT32	Ending time stamp of this RDR. The field is in UNIX time_t format, which is the number of seconds since midnight of 1 January 1970.

Table 2-18 Link Usage RDR Fields (continued)

RDR Field Name	Type	Description
UPSTREAM_VOLUME	UINT32	Aggregated upstream volume of all sessions, in kilobytes, for the current reporting period.
DOWNSTREAM_VOLUME	UINT32	Aggregated downstream volume of all sessions, in kilobytes, for the current reporting period.
SESSIONS	UINT32	Aggregated number of sessions for the reported service, for the current reporting period. The session count is reported in the RDR when the session gets initiated within the reporting period.
SECONDS	UINT32	Aggregated number of session seconds for the reported service, for the current reporting period.
CONCURRENT_SESSIONS	UINT32	Number of sessions using the reported service now. The session count is reported in the RDR if the session is active at the end of the reporting period. A value 0 is reported for all links except *link 0*. Although the values are not reported in the respective links, a cumulative value is reported in *link 0*.
ACTIVE_SUBSCRIBERS	UINT32	Number of subscribers using the reported service now irrespetive of the IP type. Dual-stack subscribers are counted only once. A value 0 is reported for all links except *link 0*. Although the values are not reported in the respective links, a cumulative value is reported in *link 0*.
TOTAL_ACTIVE_ SUBSCRIBERS	UINT32	Total subscribers having active bidirectional flows in the system irrespetive of the IP type. Dual-stack subscribers are counted only once. A value 0 is reported for all links except *link 0*. Although the values are not reported in the respective links, a cumulative value is reported in *link 0*.
IP_TYPE	UINT8	Defines the IP version of the flows for which the report is generated. Possible values are 0, 1, and 3 where 0 means IPv4, 1 means IPv6, and 3 means DS-Lite.
IP_TYPE_ACTIVE_SUBSCRI BERS	UINT32	Number of subscribers using the reported service per IP type. A value 0 is reported for all links except *link 0*. Although the values are not reported in the respective links, a cumulative value is reported in *link 0*.
IP_TYPE_TOTAL_ACTIVE_ SUBSCRIBERS	UINT32	All subscribers having active bidirectional flows in the system per IP type. A value 0 is reported for all links except *link 0*. Although the values are not reported in the respective links, a cumulative value is reported in *link 0*.

Example Scenario

The following is an example scenario in which there are 3 active IPv4 subscribers, one active IPv6 subscriber, and one active dual stack subscriber in Cisco SCE and all these subscribers use the same service and fall under same service usage counter in link 0.

The value of the ACTIVE_SUBSCRIBERS and TOTAL_ACTIVE_SUBSCRIBERS fields is 5 for both IPv4 and IPv6.

The values of IP_TYPE_ACTIVE_SUBSCRIBERS and IP_TYPE_TOTAL_ACTIVE_SUBSCRIBERS are 4 for IPv4 and 2 for IPv6.

Link Usage RDR Example

```
PPC: 255; SIP: x.0; DIP: x.0; SP: 0; DP: 0; FCID: 0;
 #4042321925:0 0 0 60 60 1359056160 0 0 0 0 0 0 5 0 0 4

PPC: 255; SIP: x.0; DIP: x.0; SP: 0; DP: 0; FCID: 0;
 #4042321925:0 0 91 60 60 1359056160 0 0 100 0 100 5 5 0 4 4

PPC: 255; SIP: x.0; DIP: x.0; SP: 0; DP: 0; FCID: 0;
 #4042321925:0 0 0 60 60 1359056160 0 0 0 0 0 0 5 1 0 2

PPC: 255; SIP: x.0; DIP: x.0; SP: 0; DP: 0; FCID: 0;
 #4042321925:0 0 91 60 60 1359056160 0 0 101 0 101 5 5 1 2 2
```

Related Topics

- Periodic RDR Zero Adjustment Mechanism, page 2-152

Zone Usage RDR

The ZONE_USAGE_RDR summarizes the activity on one of the SCE zones for a specific service for the last user-configured number of minutes.

- RDR Purpose—Create zone-level reports of network usage per service.
- RDR Default destination—Sent to the Collection Manager, stored in the database, and used by Cisco Insight for global usage reports such as the Global Bandwidth per Service report, and subscriber demographics reports such as the Active Subscribers per Service report.
- RDR Content—Summary of the activity on one of the SCE zones for a specific service for the last user-configured minutes, including aggregated number of flows, total volume, duration, and active subscribers.
- RDR Generation Logic—Generated periodically, at user-configured intervals, for each zone. A separate RDR is generated for each service usage counter. The RDR is generated only if resources associated with the service usage counter were consumed during the current reporting period.

  At fixed, user-configurable intervals (for example, every 30 minutes), there is a periodic ZONE_USAGE_RDR generation point. Whether or not a Zone Usage RDR is generated depends on the following:

  - If network resources associated with a service usage counter were consumed since the previous RDR generation point, a Zone Usage RDR is generated.
  - If network resources associated with a service usage counter were not consumed since the previous RDR generation point, no Zone Usage RDR is generated.

    However, the generation logic for Zone Usage RDRs uses the zeroing methodology (as described in the "Periodic RDR Zero Adjustment Mechanism" section on page 2-152). If network resources associated with the service are again consumed at some later time, this causes the immediate generation of either one or two zero-consumption Zone Usage RDRs (in addition to the eventual generation of the Zone Usage RDR associated with this latest consumption of network resources).
  - If there was only one interval (for example, 0830–0900) for which there was no consumption of network resources, only one zero-consumption Zone Usage RDR is generated.
  - If there were multiple consecutive intervals (for example, 0830–0900, 0900–0930, 0930–1000, 1000–1030) for which there was no consumption of network resources, two zero-consumption Zone Usage RDRs are generated—one for the first such time interval (0830–0900) and one for the last (1000–1030).

Note A separate RDR is generated for each Zone (on a single traffic processor) in the SCE platform, where each RDR represents the total traffic processed and analyzed by that processor (for the specified service usage counter). To compute the total traffic in any given time frame, take the sum of traffic of the RDRs of all the processors.

- RDR tag—4042321928

Zone Usage RDRs (ZUR) are enabled by default. Disabling ZURs eliminates global usage reports as well as subscriber demographics reports. The default interval for ZURs is every 5 minutes. Increasing this interval can enhance the time granularity of ZUR-based reports.

Table 2-19 lists the Zone Usage RDR fields and their descriptions.

Table 2-19 Zone Usage RDR Fields

RDR Field Name	Type	Description
ZONE_COUNTER_ID	UINT16	ID of the zone associated with this session.
GENERATOR_ID	INT8	Numeric value identifying the processor generating the RDR. Possible values are 0–3.
SERVICE_USAGE_ COUNTER_ID	UINT16	Counter to which each service is mapped. There are 64 global usage counters.
CONFIGURED_DURATION	UINT32	Configured period for periodic RDRs, in seconds, between successive RDRs.
DURATION	UINT32	• This release—Not implemented (always the same as CONFIGURED_DURATION). • Future release—Indicates the number of seconds that have passed since the previous SUBSCRIBER_USAGE_RDR.
END_TIME	UINT32	Ending time stamp of this RDR. The field is in UNIX time_t format, which is the number of seconds since midnight of 1 January 1970.
UPSTREAM_VOLUME	UINT32	Aggregated upstream volume of all sessions, in kilobytes, for the current reporting period.
DOWNSTREAM_VOLUME	UINT32	Aggregated downstream volume of all sessions, in kilobytes, for the current reporting period.
SESSIONS	INT32	Aggregated number of sessions for the reported service, for the current reporting period. The session count is reported in the RDR when the session gets initiated within the reporting period.
SECONDS	INT32	Aggregated number of session seconds for the reported service, for the current reporting period.
CONCURRENT_SESSIONS	UINT32	Number of sessions using the reported service now. The session count is reported in the RDR if the session is active at the end of the reporting period. Currently not supported in Release 4.0.0, so counter always returns 0.
ACTIVE_SUBSCRIBERS	UINT32	Number of subscribers using the reported service now. Currently not supported in Release 4.0.0, so counter always returns 0.
TOTAL_ACTIVE_ SUBSCRIBERS	UINT32	Number of subscribers in the system now. Currently not supported in Release 4.0.0, so counter always returns 0.
IP_TYPE	UNIT8	Defines the IP version of the flows for which the report is generated. Possible values are 0 and 1. Value 0 indicates IPv4 RDR and value 1 indicates IPv6 RDR.

Related Topics

- Periodic RDR Zero Adjustment Mechanism, page 2-152

Package Usage RDR

The PACKAGE_USAGE_RDR summarizes the activity of a specific group of subscribers (belonging to the same package) for a specific service in the last user-configured number of minutes.

- RDR Purpose—Create reports about network usage per service for a group of subscribers.
- RDR Default destination—Sent to the Collection Manager, stored in the database, and used by Cisco Insight for package usage reports such as the Package Bandwidth per Service report.
- RDR Content—Summary of the activity of a specific group of subscribers (belonging to the same package) for a specific service for the last user-configured number of minutes, including aggregated number of flows, total volume, and duration.
- RDR Generation Logic—Generated periodically, at user-configured intervals, for each package usage counter. A separate RDR is generated for each service usage counter. The RDR is generated only if resources associated with the service usage counter were consumed during the current reporting period. The RDR contains aggregated network usage information for all subscribers to the package or group of packages represented by the package usage counter.

  At fixed, user-configurable intervals (for example, every 5 minutes), there is a periodic PACKAGE_USAGE_RDR generation point. Whether or not a Package Usage RDR is actually generated depends on the following:

  - If network resources associated with a service usage counter were consumed by a subscriber of the package since the previous RDR generation point, a Package Usage RDR is generated.
  - If a subscriber of the package has not consumed network resources associated with a service usage counter since the previous RDR generation point, no Package Usage RDR is generated.

    However, the generation logic for Package Usage RDRs uses the zeroing methodology (as described in the "Periodic RDR Zero Adjustment Mechanism" section on page 2-152). If network resources associated with the service usage counter are again consumed by any subscriber of the package at some later time, this causes the immediate generation of either one or two zero-consumption Package Usage RDRs (in addition to the eventual generation of the Package Usage RDR associated with this latest consumption of network resources).
  - If there was only one interval (for example, 0805–0810) for which there was no consumption of network resources by any subscriber of the package, only one zero-consumption Package Usage RDR is generated.
  - If there were multiple consecutive intervals (for example, 0805–0810, 0810–0815, 0815–0820, 0820–0825) for which there was no consumption of network resources by any subscriber of the package, two zero-consumption Package Usage RDR are generated—one for the first such time interval (0805–0810) and one for the last (0820–0825).

Note Each traffic processor in the SCE platform generates a separate RDR, where each RDR represents the total traffic processed and analyzed by that processor (for the specified service usage counter). To compute the total traffic (for a package) in any given time frame, take the sum of the traffic of the RDRs of all the processors.

- RDR tag—0xf0f0f004 / 4042321924

Package Usage RDRs (PURs) are enabled by default. Disabling LURs eliminates package usage reports. The default interval for PURs is every 5 minutes. Increasing this interval can enhance the time granularity of PUR-based reports.

Table 2-20 lists the Package Usage RDR fields and their descriptions.

Table 2-20 Package Usage RDR Fields

RDR Field Name	Type	Description
PACKAGE_COUNTER_ID	UINT16	Counter to which each service is mapped. There are 1024 package usage counters.
GENERATOR_ID	INT8	Numeric value identifying the processor generating the RDR.
SERVICE_USAGE_ COUNTER_ID	UINT16	Counter to which each service is mapped. There are 64 global usage counters.
CONFIGURED_DURATION	UINT32	Configured period for periodic RDRs, in seconds, between successive RDRs.
DURATION	UINT32	• This release—Not implemented (always the same as CONFIGURED_DURATION). • Future release—Indicates the number of seconds that have passed since the previous SUBSCRIBER_USAGE_RDR.
END_TIME	UINT32	Ending time stamp of this RDR. The field is in UNIX time_t format, which is the number of seconds since midnight of 1 January 1970.
UPSTREAM_VOLUME	UINT32	Aggregated upstream volume on both links (for a single processor) of all sessions, in kilobytes, for the current reporting period.
DOWNSTREAM_VOLUME	UINT32	Aggregated downstream volume on both links (for a single processor) of all sessions, in kilobytes, for the current reporting period.
SESSIONS	UINT32	Aggregated number of sessions for the reported service, for the current reporting period. The session count is reported in the RDR when the session gets initiated within the reporting period.
SECONDS	UINT32	Aggregated number of session seconds for the reported service, for the current reporting period.
CONCURRENT_SESSIONS	UINT32	Number of sessions using the reported service in the reported package now. The session count is reported in the RDR if the session is active at the end of the reporting period.
ACTIVE_SUBSCRIBERS	UINT32	Number of subscribers using the reported service in the reported package now irrespetive of the IP type. Dual-stack subscribers are counted only once.
TOTAL_ACTIVE_ SUBSCRIBERS	UINT32	Total subscribers having active flows in the package irrespetive of the IP type. Dual-stack subscribers are counted only once.
IP_TYPE	INT8	Possible values are 0, 1, and 3. Value 0 indicates IPv4 RDR, value 1 indicates IPv6 RDR, and value 3 indicates DSLite RDR.

Table 2-20 Package Usage RDR Fields (continued)

RDR Field Name	Type	Description
IP_TYPE_ACTIVE_SUBSCRIBERS	UINT32	Number of subscribers using the reported service in the reported package per IP type.
IP_TYPE_TOTAL_ACTIVE_SUBSCRIBERS	UINT32	All subscribers having active flows in the in the reported package per IP type.

Example Scenario

The following is an example scenario in which there are 3 active IPv4 subscribers, one active IPv6 subscriber, and one active dual stack subscriber in Cisco SCE and all these subscribers use the same service and fall under same service usage counter in package 0.

The value of the ACTIVE_SUBSCRIBERS and TOTAL_ACTIVE_SUBSCRIBERS fields is 5 for both IPv4 and IPv6.

The values of IP_TYPE_ACTIVE_SUBSCRIBERS and IP_TYPE_TOTAL_ACTIVE_SUBSCRIBERS are 4 for IPv4 and 2 for IPv6.

Package Usage RDR Example

```
PPC: 255; SIP: x.0; DIP: x.0; SP: 0; DP: 0; FCID: 0;
 #4042321924:1 0 0 60 60 1359056165 0 0 0 0 0 0 5 0 0 4

PPC: 255; SIP: x.0; DIP: x.0; SP: 0; DP: 0; FCID: 0;
 #4042321924:1 0 91 60 60 1359056165 0 0 4 0 4 5 5 0 4 4

PPC: 255; SIP: x.0; DIP: x.0; SP: 0; DP: 0; FCID: 0;
 #4042321924:1 0 0 60 60 1359056165 0 0 0 0 0 0 5 1 0 2


PPC: 255; SIP: x.0; DIP: x.0; SP: 0; DP: 0; FCID: 0;
 #4042321924:1 0 91 60 60 1359056165 0 0 101 0 101 5 5 1 2 2
```

Related Topics

- Periodic RDR Zero Adjustment Mechanism, page 2-152

Virtual Links Usage RDR

The VIRTUAL_LINKS_USAGE_RDR summarizes the activity on one of the virtual links for a specific service for the last user-configured number of minutes. For information on virtual links, see the *Cisco Service Control Application for Broadband User Guide*.

- RDR Purpose—Create reports relating to network usage per service for a specific virtual link.
- RDR Default destination—Sent to the Collection Manager, stored in the database, and used by Cisco Insight for virtual link reports such as the Virtual Link Bandwidth per Service report.
- RDR Content—Summary of the activity on one of the virtual links for a specific service for the last user-configured number of minutes, including aggregated number of flows, total volume, and duration.
- RDR Generation Logic—Generated periodically, at user-configured intervals, for each service usage counter. A separate RDR is generated for each virtual link. The RDR is generated only if resources associated with the virtual link were consumed during the current reporting period. The RDR contains aggregated network usage information for all subscribers to the same virtual link.

  At fixed, user-configurable intervals (for example, every 5 minutes), there is a periodic VIRTUAL_LINKS_USAGE_RDR generation point. Whether or not a Virtual Links Usage RDR is actually generated depends on the following:

  - If network resources associated with the service usage counter were consumed by any subscriber of the virtual link since the previous RDR generation point, a Virtual Links Usage RDR is generated.
  - If no subscriber of the virtual link has consumed network resources associated with the service usage counter since the previous RDR generation point, no Virtual Links Usage RDR is generated.

    However, the generation logic for Virtual Links Usage RDRs uses the zeroing methodology (as described in the "Periodic RDR Zero Adjustment Mechanism" section on page 2-152). If network resources associated with the service usage counter are again consumed by subscribers of the virtual link at some later time, this causes the immediate generation of either one or two zero-consumption Virtual Links Usage RDRs (in addition to the eventual generation of the Virtual Links Usage RDR associated with this latest consumption of network resources by subscribers of the virtual link).
  - If there was only one interval (for example, 0805–0810) for which there was no consumption of network resources by any subscriber of the virtual link, only one zero-consumption Virtual Links Usage RDR is generated.
  - If there were multiple consecutive intervals (for example, 0805–0810, 0810–0815, 0815–0820, 0820–0825) for which there was no consumption of network resources by any subscriber of the virtual link, two zero-consumption Virtual Links Usage RDR are generated—one for the first such time interval (0805–0810) and one for the last (0820–0825).

  Note Each traffic processor in the SCE platform generates a separate RDR, where each RDR represents the total traffic processed and analyzed by that processor (for the specified service usage counter and the specified virtual link). To compute the total traffic (for a virtual link) in any given time frame, take the sum of the traffic of the RDRs of all the processors.

- RDR tag—0xf0f0f006 / 4042321926

Virtual Link Usage RDRs (VLURs) are disabled by default. You can enable VLURs when working with virtual links to facilitate virtual link usage reports. The recommended value for intervals between VLURs is 5 minutes.

Table 2-21 lists the Virtual Links Usage RDR fields and their descriptions.

Table 2-21 Virtual Links Usage RDR Fields

RDR Field Name	Type	Description
VLINK_ID	INT16	Virtual link ID
VLINK_DIRECTION	INT8	Virtual link direction: • 0—Upstream • 1—Downstream
GENERATOR_ID	INT8	Numeric value identifying the processor generating the RDR.
SERVICE_USAGE_ COUNTER_ID	UINT16	Counter to which each service is mapped. There are 1024 global usage counters.
CONFIGURED_DURATION	UINT32	Configured period for periodic RDRs, in seconds, between successive RDRs.
DURATION	UINT32	Not implemented (always the same as CONFIGURED_DURATION).
END_TIME	UINT32	Ending time stamp of this RDR. The field is in UNIX time_t format, which is the number of seconds since midnight of 1 January 1970.
UPSTREAM_VOLUME	UINT32	Aggregated upstream volume on the virtual link (for a single processor) of all sessions, in kilobytes, for the current reporting period.
DOWNSTREAM_VOLUME	UINT32	Aggregated downstream volume on the virtual link (for a single processor) of all sessions, in kilobytes, for the current reporting period.
SESSIONS	UINT32	Aggregated number of sessions for the reported service, for the current reporting period. The session count is reported in the RDR when the session gets initiated within the reporting period.
SECONDS	UINT32	Reserved for future use.
CONCURRENT_SESSIONS	UINT32	Number of sessions using the reported service now. The session count is reported in the RDR if the session is active at the end of the reporting period.
ACTIVE_SUBSCRIBERS	UINT32	Number of active subscribers using the reported service now irrespetive of the IP type. Dual-stack subscribers are counted only once.
TOTAL_ACTIVE_ SUBSCRIBERS	UINT32	Total subscribers having active flows in the corresponding vlink direction irrespetive of the IP type. Dual-stack subscribers are counted only once.
IP_TYPE	UINT8	Defines the IP version of the flows for which the report is generated. Possible values are 0, 1, and 3 where 0 means IPv4, 1 means IPv6, and 3 means DS-Lite.

Table 2-21 Virtual Links Usage RDR Fields (continued)

RDR Field Name	Type	Description
IP_TYPE_ACTIVE_SUBSCRIBERS	UINT32	Number of subscribers using the reported service per IP type.
IP_TYPE_TOTAL_ACTIVE_SUBSCRIBERS	UINT32	All subscribers having active flows in the corresponding vlink direction per IP type.

Example Scenario

The following is an example scenario in which there are 3 active IPv4 subscribers, one active IPv6 subscriber, and one active dual stack subscriber in Cisco SCE and all these subscribers use the same service and fall under same service usage counter in up vlink 10 and down vlink 20.

The value of the ACTIVE_SUBSCRIBERS and TOTAL_ACTIVE_SUBSCRIBERS fields is 5 for both IPv4 and IPv6 in the respective up vlinks and down vlinks.

The values of IP_TYPE_ACTIVE_SUBSCRIBERS and IP_TYPE_TOTAL_ACTIVE_SUBSCRIBERS are 4 for IPv4 and 2 for IPv6.

Virtual Links Usage RDR Example

```
PPC: 255; SIP: x.0; DIP: x.0; SP: 0; DP: 0; FCID: 0;
 #4042321926:10 0 0 0 60 60 1359060010 0 0 0 0 0 0 5 0 0 4

PPC: 255; SIP: x.0; DIP: x.0; SP: 0; DP: 0; FCID: 0;
 #4042321926:10 0 0 91 60 60 1359060010 0 0 4 0 4 5 5 0 4 4

PPC: 255; SIP: x.0; DIP: x.0; SP: 0; DP: 0; FCID: 0;
 #4042321926:10 0 0 0 60 60 1359060010 0 0 0 0 0 0 5 1 0 2

PPC: 255; SIP: x.0; DIP: x.0; SP: 0; DP: 0; FCID: 0;
 #4042321926:10 0 0 91 60 60 1359060010 0 0 101 0 101 5 5 1 2 2

PPC: 255; SIP: x.0; DIP: x.0; SP: 0; DP: 0; FCID: 0;
 #4042321926:20 1 0 0 60 60 1359060010 0 0 0 0 0 0 5 0 0 4

PPC: 255; SIP: x.0; DIP: x.0; SP: 0; DP: 0; FCID: 0;
 #4042321926:20 1 0 91 60 60 1359060010 0 0 4 0 4 5 5 0 4 4

PPC: 255; SIP: x.0; DIP: x.0; SP: 0; DP: 0; FCID: 0;
 #4042321926:20 1 0 0 60 60 1359060010 0 0 0 0 0 0 5 1 0 2

PPC: 255; SIP: x.0; DIP: x.0; SP: 0; DP: 0; FCID: 0;
 #4042321926:20 1 0 91 60 60 1359060010 0 0 101 0 101 5 5 1 2 2
```

Related Topics

- Periodic RDR Zero Adjustment Mechanism, page 2-152

Blocking RDR

The SERVICE_BLOCK_RDR is generated each time a transaction is blocked, and the profile and the rate/quota limitations indicate that this RDR should be generated.

- A Blocking RDR is generated when a session is blocked. A session may be blocked for various reasons; for example, access is blocked or concurrent session limit is reached.
- Generation of Blocking RDRs is subject to two limitations:
  - Quota—Maximum number of Blocking RDRs that Cisco SCA BB can generate for a subscriber in a specific aggregation period (day, week, month, and so on). The quota is package dependent; its value is set according to the package assigned to the subscriber.
  - Rate—Global, maximum number of Blocking RDRs that an SCE platform can generate per second. The rate is a global value that sets an upper limit for the total number of RDRs that are generated for all subscribers.

The RDR tag of the SERVICE_BLOCK_RDR is 0xf0f0f040 / 4042321984.

Table 2-22 lists the Blocking RDR fields and their descriptions.

Table 2-22 Blocking RDR Fields

RDR Field Name	Type	Description
SUBSCRIBER_ID	STRING	Subscriber identification string, introduced through the subscriber management interfaces. It may contain up to 64 characters. For unknown subscribers, this field may contain an empty string.
PACKAGE_ID	UINT16	ID of the package assigned to the subscriber whose traffic is being reported. An assigned Package ID is an integer value between 0 and 4999. The value 4999 is reserved for unknown subscribers, and this is the maximum_number_of_packages possible.
SERVICE_ID	INT32	Service classification of the reported session. For example, in the Transaction RDR, this field indicates which service was accessed, and in the Breaching RDR, this field indicates which service was breached.
PROTOCOL_ID	INT16	Unique ID of the protocol associated with the reported session.
CLIENT_IP	UINT32	IP address of the client side of the reported session. The client side is defined as the initiator of the networking session. The IP address is in a 32-bit binary format, but the value is obtained in decimal format in RDR.
CLIENT_PORT	UINT16	Port number of the client side (initiator) of the TCP/UDP-based networking session. For non-TCP/UDP sessions, this field has the value zero.
SERVER_IP	UINT32	Destination IP address of the reported session. The destination is defined as the server or the listener of the networking session. The IP address is in a 32-bit binary format, but the value is obtained in decimal format in RDR.

Table 2-22 Blocking RDR Fields (continued)

RDR Field Name	Type	Description
SERVER_PORT	UINT16	Destination port number of the TCP/UDP-based networking session. For non-TCP/UDP sessions, this field contains the IP protocol number of the session flow.
INITIATING_SIDE	INT8	Side of the SCE platform on which the initiator of the transaction resides: • 0—Subscriber side • 1—Network side
ACCESS_STRING	STRING	Layer 7 property, extracted from the transaction.
INFO_STRING	STRING	Layer 7 property, extracted from the transaction.
BLOCK_REASON	UINT8	Indicates the reason why this session was blocked.
BLOCK_RDR_COUNT	INT32	Total number of blocked flows reported so far (from the beginning of the current aggregation period).
REDIRECTED	INT8	Indicates whether the flow has been redirected after being blocked: • 0—Not redirected • 1—Redirected
REPORT_TIME	UINT32	Ending time stamp of this RDR. The field is in UNIX time_t format, which is the number of seconds since midnight of 1 January 1970.
IP_TYPE	UINT8	Defines the IP flow type of the respective RDR. For example, when the flow type is IPv6, the IPv4 address of the RDR will contain the value zero. However, the IPv6 address of the RDR will contain a white space for IPv4 flow type.
CLIENTIPv6ADDRESS	STRING	Destination IPv6 address of the reported session. The destination is defined as the server or the listener of the networking session.
SERVERIPv6ADDRESS	STRING	IPv6 address of the client side of the reported session. The client side is defined as the initiator of the networking session.

Related Topics

- Block Reason (uint8), page 2-145
- Anonymized Blocking RDR, page 2-86

Anonymized Blocking RDR

The ANONYMIZED_SERVICE_BLOCK_RDR is generated each time a transaction is blocked, and the profile and the rate/quota limitations indicate that this RDR should be generated. This RDR does not contain personal subscriber data.

- A Blocking RDR is generated when a session is blocked. A session may be blocked for various reasons; for example, access is blocked or concurrent session limit is reached.
- Generation of Blocking RDRs is subject to two limitations:
  - Quota—Maximum number of Blocking RDRs that Cisco SCA BB can generate for a subscriber in a specific aggregation period (day, week, month, and so on). The quota is package-dependent; its value is set according to the package assigned to the subscriber.
  - Rate—Global, maximum number of Blocking RDRs that an SCE platform can generate per second. The rate is a global value that sets an upper limit for the total number of RDRs that are generated for all subscribers.

The RDR tag of the ANONYMIZED_SERVICE_BLOCK_RDR is 0xf0f0f543 / 4042323267.

Table 2-23 lists the Anonymized Blocking RDR fields and their descriptions.

Table 2-23 Anonymized Blocking RDR Fields

RDR Field Name	Type	Description
HASHED_SUBSCRIBER_ID	STRING	Subscriber identification string, introduced through the subscriber management interfaces, may be passed through hashing algorithm. It may contain up to 64 characters. For unknown subscribers, this field may contain an empty string.
PACKAGE_ID	UINT16	ID of the package assigned to the subscriber whose traffic is being reported. An assigned Package ID is an integer value between 0 and 4999. The value 4999 is reserved for unknown subscribers, and this is the maximum_number_of_packages possible.
SERVICE_ID	INT32	Service classification of the reported session. For example, in the Transaction RDR, this field indicates which service was accessed, and in the Breaching RDR, this field indicates which service was breached.
PROTOCOL_ID	INT16	Unique ID of the protocol associated with the reported session.
CLIENT_IP	UINT32	IP address of the client side of the reported session. The client side is defined as the initiator of the networking session. The IP address is in a 32-bit binary format, but the value is obtained in decimal format in RDR. If this is the subscriber IP, this field may contain the short-hash of the IP if configured.
CLIENT_PORT	UINT16	Port number of the client side (initiator) of the TCP/UDP-based networking session. For non-TCP/UDP sessions, this field has the value zero.

Table 2-23 Anonymized Blocking RDR Fields (continued)

RDR Field Name	Type	Description
SERVER_IP	UINT32	Destination IP address of the reported session. The destination is defined as the server or the listener of the networking session. The IP address is in a 32-bit binary format, but the value is obtained in decimal format in RDR. If this is the subscriber IP, this field may contain the short-hash of the IP if configured.
SERVER_PORT	UINT16	Destination port number of the TCP/UDP-based networking session. For non-TCP/UDP sessions, this field contains the IP protocol number of the session flow.
INITIATING_SIDE	INT8	Side of the SCE platform on which the initiator of the transaction resides: • 0—Subscriber side • 1—Network side
ACCESS_STRING	STRING	Layer 7 property, extracted from the transaction.
INFO_STRING	STRING	Layer 7 property, extracted from the transaction.
BLOCK_REASON	UINT8	Indicates the reason why this session was blocked.
BLOCK_RDR_COUNT	INT32	Total number of blocked flows reported so far (from the beginning of the current aggregation period).
REDIRECTED	INT8	Indicates whether the flow has been redirected after being blocked: • 0—Not redirected • 1—Redirected
REPORT_TIME	UINT32	Ending time stamp of this RDR. The field is in UNIX time_t format, which is the number of seconds since midnight of 1 January 1970.
IP_TYPE	UINT8	Defines the IP flow type of the respective RDR. For example, when the flow type is IPv6, the IPv4 address of the RDR will contain the value zero. However, the IPv6 address of the RDR will contain a white space for IPv4 flow type.
CLIENTIPv6ADDRESS	STRING	IPv6 address of the client side of the reported session. The client side is defined as the initiator of the networking session. If this is the subscriber IP, this field may contain a 32-byte string hash, if configured.
SERVERIPv6ADDRESS	STRING	Destination IPv6 address of the reported session. The destination is defined as the server or the listener of the networking session. If this is the subscriber IP, this field may contain a 32-byte string hash, if configured.

Related Topics

- Block Reason (uint8), page 2-145
- Blocking RDR, page 2-84

Quota Breach RDR

The QUOTA_BREACH_RDR is generated each time a bucket is breached.

This RDR does not have a rate limit; it is generated whenever a quota breach occurs, if the RDR is enabled.

The RDR tag of the QUOTA_BREACH_RDR is 0xf0f0f072 / 4,042,322,034.

Table 2-24 lists the Quota Breach RDR fields and their descriptions.

Table 2-24 Quota Breach RDR Fields

RDR Field Name	Type	Description
QUOTA_MODEL_TYPE	UINT8	Quota model type: • 1—Gy Quota Model • 2—QM Quota Model • 3—Internal Quota Model
RDR_REASON	UINT8	Reason the RDR was sent. Not in use, RESERVED - 0xfe
SUBSCRIBER_ID	STRING	Subscriber identification string, introduced through the subscriber management interfaces. It may contain up to 40 characters. For unknown subscribers, this field may contain an empty string.
PACKAGE_ID	UINT16	ID of the package assigned to the subscriber whose traffic is being reported. An assigned Package ID is an integer value between 0 and 4999. The value 4999 is reserved for unknown subscribers, and this is the maximum_number_of_packages possible.
ADDITIONAL_INFO	UINT32	See "ADDITIONAL_INFO Field" section on page 2-6 for details.
END_TIME	UINT32	Ending time stamp of this RDR. The field is in UNIX time_t format, which is the number of seconds since midnight of 1 January 1970.
BUCKET_ID	UINT16	Bucket ID to report.

Table 2-24 Quota Breach RDR Fields (continued)

RDR Field Name	Type	Description
BUCKET_TYPE	UINT16	Bucket type: • 1—Volume_UP Only the upstream volume is reported in the RDR. UNIT_AMOUNT_IN is 0 and UNIT_AMOUNT_OUT indicates the upstream volume. • 2—Volume_DOWN Only the downstream volume is reported in the RDR. UNIT_AMOUNT_IN indicates the downstream volume and UNIT_AMOUNT_OUT is 0. • 3—Total Volume The sum of downstream and upstream volumes, that is, the total volume consumed, and the remaining volume, that is, bucket size – total volume is reported in the RDR. UNIT_AMOUNT_IN indicates the total volume consumed and UNIT_AMOUNT_OUT indicates the remaining volume. • 4—VolumeUpDown Both upstream and downstream volumes are reported in the RDR. UNIT_AMOUNT_IN indicates the downstream volume and UNIT_AMOUNT_OUT indicates the upstream volume. • 5—Events (sessions) UNIT_AMOUNT_IN indicates the number of sessions that has used the bucket. UNIT_AMOUNT_OUT indicates the remaining number of sessions for the bucket. • 6—Time UNIT_AMOUNT_IN indicates how long a bucket has been used. This unit is represented in seconds. The UNIT_AMOUNT_OUT field is 0. **Note** For the following bucket types, only the UNIT_AMOUNT_IN field is valid: – Time – Events (sessions) – Total Volume
UNIT_AMOUNT_IN	UINT32	Consumed downstream volume in volume units/ Seconds/ Sessions.

Table 2-24 Quota Breach RDR Fields (continued)

RDR Field Name	Type	Description
UNIT_AMOUNT_OUT	UINT32	Consumed upstream volume in volume units. For Internal/QM quota models – remaining quota as 32-bit integer value (may be negative).
BUCKET_SIZE_IN	UINT32	Original bucket size in volume units/Seconds/ Sessions. For GY quota model – downstream bucket size in volume units.
BUCKET_SIZE_OUT	UINT32	(Only valid for Gy quota model) Upstream bucket size in volume units.
FINAL_UNIT_SPECIFIED	UNIT8	(Only valid for Gy quota model) Used to specify if final unit indication (FUI) is set for this bucket. Possible values are 0 and 1. 0—FUI is not sent to Cisco SCE. 1—FUI is sent to Cisco SCE.

Quota Status RDR

The QUOTA_STATUS_RDR reports consumed quota of the subscriber for all associated buckets. If one RDR cannot contain all associated buckets, then two or more consecutive RDRs are sent.

The user can set a limit on the total number of these RDRs that are generated per second.

If a bucket is not in use, 0xFFFF appears in the BUCKET_ID, BUCKET_TYPE, UNIT_AMOUNT_IN, and UNIT_AMOUNT_OUT fields.

Note The QUOTA_STATUS_RDR is generated only for those subscribers whose policy requires the generation of such RDRs.

This RDR is sent:

- Periodically, at user-configured intervals. The intervals are defined globally.

  Applies to all quota models, including internal and QM external quota models.
- Triggered by these events:
  - Package switch event: Indicates consumed quota before the package switch.

    Applies to all quota models.
  - Subscriber logout event.

    Applies to all quota models.
  - Quota Validity Time/Quota Holding Time expiration.

    Applies only to Gy quota model.

The RDR tag of the QUOTA_STATUS_RDR is 0xf0f0f071 / 4042322033.

Table 2-25 lists the Quota Status RDR fields and descriptions.

Table 2-25 Quota Status RDR Fields

RDR Field Name	Type	Description
QUOTA_MODEL_TYPE	UINT8	Quota model type: • 1 - Gy Quota Model • 2 - QM Quota Model • 3 - Internal Quota Model
RDR_REASON	UINT8	Reason the RDR was sent: • 0 - Period time passed • 1 - Logout • 2 - Package Switch • 5 - Request (RAR)
SUBSCRIBER_ID	STRING	Subscriber identification string, introduced through the subscriber management interfaces. It may contain up to 40 characters. For unknown subscribers, this field may contain an empty string.

Table 2-25 Quota Status RDR Fields (continued)

RDR Field Name	Type	Description
PACKAGE_ID	UINT16	ID of the package assigned to the subscriber whose traffic is being reported. An assigned Package ID is an integer value between 0 and 4999. The value 4999 is reserved for unknown subscribers, and this is the maximum_number_of_packages possible.
ADDITIONAL_INFO	UINT32	See "ADDITIONAL_INFO Field" section on page 2-6 for details.
END_TIME	UINT32	Ending time stamp of this RDR. The field is in UNIX time_t format, which is the number of seconds since midnight of 1 January 1970.
BUCKET_ID	UINT16	Bucket ID to report.

Table 2-25 Quota Status RDR Fields (continued)

RDR Field Name	Type	Description
BUCKET_TYPE	UINT16	Bucket type: • 1—Volume_UP Only the upstream volume is reported in the RDR. UNIT_AMOUNT_IN is 0 and UNIT_AMOUNT_OUT indicates the upstream volume. • 2—Volume_DOWN Only the downstream volume is reported in the RDR. UNIT_AMOUNT_IN indicates the downstream volume and UNIT_AMOUNT_OUT is 0. • 3—Total Volume The sum of downstream and upstream volumes, that is, the total volume consumed, and the remaining volume, that is, bucket size – total volume is reported in the RDR. UNIT_AMOUNT_IN indicates the total volume consumed and UNIT_AMOUNT_OUT indicates the remaining volume. • 4—VolumeUpDown Both upstream and downstream volumes are reported in the RDR. UNIT_AMOUNT_IN indicates the downstream volume and UNIT_AMOUNT_OUT indicates the upstream volume. • 5—Events (sessions) UNIT_AMOUNT_IN indicates the number of sessions that has used the bucket. UNIT_AMOUNT_OUT indicates the remaining number of sessions for the bucket. • 6—Time UNIT_AMOUNT_IN indicates how long a bucket has been used. This unit is represented in seconds. The UNIT_AMOUNT_OUT field is 0. **Note** For the following bucket types, only the UNIT_AMOUNT_IN field is valid: – Time – Events (sessions) – Total Volume

Table 2-25 Quota Status RDR Fields (continued)

RDR Field Name	Type	Description
UNIT_AMOUNT_IN	UINT32	Consumed volume in volume units/ Seconds/ Sessions. For Gy quota model—downstream volume.
UNIT_AMOUNT_OUT	UINT32	For Gy quota model—consumed upstream volume in volume units. For QM/Internal quota models—remaining quota in 32-bit integer format (may be negative).

Note The following fields report information per bucket:

- BUCKET_ID
- BUCKET_TYPE
- UNIT_AMOUNT_IN
- UNIT_AMOUNT_OUT

This section of four fields is repeated 16 times, one time for each of the 16 buckets, for a total of 64 fields (added to the six header fields results in a total of 70 fields in the RDR).

Quota Threshold Breach RDR

The QUOTA_THRESHOLD_BREACH_RDR is generated each time a bucket exceeds the bucket threshold as defined for each package.

This RDR does not have a rate limit; it is generated whenever a threshold is exceeded, if the RDR is enabled.

The RDR tag of the QUOTA_THRESHOLD_BREACH_RDR is 0xf0f0f073 / 4042322035.

Table 2-26 lists the Quota Threshold Breach RDR fields and their descriptions.

Table 2-26 Quota Threshold Breach RDR Fields

RDR Field Name	Type	Description
QUOTA_MODEL_TYPE	UINT8	Quota model type: • 1 - Gy Quota Model • 2 - QM Quota Model • 3 - Internal Quota Model
RDR_REASON	UINT8	Reason the RDR was sent. Not in use, RESERVED - 0xfe
SUBSCRIBER_ID	STRING	Subscriber identification string, introduced through the subscriber management interfaces. It may contain up to 40 characters. For unknown subscribers, this field may contain an empty string.

Table 2-26 Quota Threshold Breach RDR Fields (continued)

RDR Field Name	Type	Description
PACKAGE_ID	UINT16	ID of the package assigned to the subscriber whose traffic is being reported. An assigned Package ID is an integer value between 0 and 4999. The value 4999 is reserved for unknown subscribers, and this is the maximum_number_of_packages possible.
ADDITIONAL_INFO	UINT32	See "ADDITIONAL_INFO Field" section on page 2-6 for details.
END_TIME	UINT32	Ending time stamp of this RDR. The field is in UNIX time_t format, which is the number of seconds since midnight of 1 January 1970.
BUCKET_ID	UINT16	Bucket ID to report.

Table 2-26 Quota Threshold Breach RDR Fields (continued)

RDR Field Name	Type	Description
BUCKET_TYPE	UINT16	Bucket type: • 1—Volume_UP Only the upstream volume is reported in the RDR. UNIT_AMOUNT_IN is 0 and UNIT_AMOUNT_OUT indicates the upstream volume. • 2—Volume_DOWN Only the downstream volume is reported in the RDR. UNIT_AMOUNT_IN indicates the downstream volume and UNIT_AMOUNT_OUT is 0. • 3—Total Volume The sum of downstream and upstream volumes, that is, the total volume consumed, and the remaining volume, that is, bucket size – total volume is reported in the RDR. UNIT_AMOUNT_IN indicates the total volume consumed and UNIT_AMOUNT_OUT indicates the remaining volume. • 4—VolumeUpDown Both upstream and downstream volumes are reported in the RDR. UNIT_AMOUNT_IN indicates the downstream volume and UNIT_AMOUNT_OUT indicates the upstream volume. • 5—Events (sessions) UNIT_AMOUNT_IN indicates the number of sessions that has used the bucket. UNIT_AMOUNT_OUT indicates the remaining number of sessions for the bucket. • 6—Time UNIT_AMOUNT_IN indicates how long a bucket has been used. This unit is represented in seconds. The UNIT_AMOUNT_OUT field is 0. **Note** For the following bucket types, only the UNIT_AMOUNT_IN field is valid: – Time – Events (sessions) – Total Volume
UNIT_AMOUNT_IN	UINT32	Consumed downstream volume in volume units/ Seconds/ Sessions.

Table 2-26 Quota Threshold Breach RDR Fields (continued)

RDR Field Name	Type	Description
UNIT_AMOUNT_OUT	UINT32	Consumed upstream volume in volume units. For QM/Internal quota models—remaining quota in 32-bit integer format (may be negative).
BUCKET_SIZE_IN	UINT32	Original bucket size in volume units/ Seconds/ Sessions. For GY quota model—downstream volume/total volume/sessions/seconds.
BUCKET_SIZE_OUT	UINT32	For GY quota model—original upstream volume.
THRESHOLD_SIZE_IN	UINT32	Threshold of the bucket in volume units/ Seconds/ Sessions.
THRESHOLD_SIZE_OUT	UINT32	Threshold of the bucket in volume units/ Seconds/ Sessions. Valid only for Gy quota models—upstream bucket threshold.

Session Creation RDR

Typically, the SESSION_CREATION_RDR is sent on subscriber login event. This RDR replaces the legacy QUOTA_STATE_RESTORE_RDR.

If a bucket is not in use, 0xFFFF appears in BUCKET_ID, and “0” appears in the BUCKET_TYPE, UNIT_AMOUNT_IN, and UNIT_AMOUNT_OUT fields.

The following events trigger the sending of this RDR:

- Subscriber association with package with external quota management (Gy or Qm)
- Package switch event transition from internal package to external one or in Gy.

The RDR tag of the SESSION_CREATION_RDR is 0xf0f0f070 / 4042322032.

Table 2-27 lists the Session Creation RDR fields and their descriptions.

Table 2-27 Session Creation RDR Fields

RDR Field Name	Type	Description
QUOTA_MODEL_TYPE	UINT8	Quota model type: • 1 - Gy Quota Model • 2 - QM Quota Model • 3 - Internal Quota Model
RDR_REASON	UINT8	Reason the RDR was sent: • 2 - Package Switch • 3 - Login
SUBSCRIBER_ID	STRING	Subscriber identification string, introduced through the subscriber management interfaces. It may contain up to 40 characters. For unknown subscribers, this field may contain an empty string.
PACKAGE_ID	UINT16	ID of the package assigned to the subscriber whose traffic is being reported. An assigned Package ID is an integer value between 0 and 4999. The value 4999 is reserved for unknown subscribers, and this is the maximum_number_of_packages possible.
ADDITIONAL_INFO	UINT32	See ADDITIONAL_INFO Field, page 2-6 for details.
END_TIME	UINT32	Ending time stamp of this RDR. The field is in UNIX time_t format, which is the number of seconds since midnight of 1 January 1970.
BUCKET_ID	UINT16	Use only for Gy quota model. If **request quota upon login** is specified for the bucket, this field contains the bucket ID. This field indicates to the server that quota should be provided to the specified bucket ID. '0xFFFF' – reserved.
BUCKET_TYPE	UINT16	Not used.

Table 2-27 Session Creation RDR Fields (continued)

RDR Field Name	Type	Description
UNIT_AMOUNT_IN	UINT32	Not used.
UNIT_AMOUNT_OUT	UINT32	Not used.

Note The following fields report information per bucket:

- BUCKET_ID
- BUCKET_TYPE
- UNIT_AMOUNT_IN
- UNIT_AMOUNT_OUT

This section of four fields is repeated 16 times, one time for each of the 16 buckets, for a total of 64 fields (added to the six header fields results in a total of 70 fields in the RDR).

DHCP RDR

The DHCP_RDR is generated each time a DHCP message of a specified type is intercepted.

Note DHCP RDRs are generated only if activated by a subscriber integration system, such as the SCMS Subscriber Manager DHCP Login Event Generator (LEG).

For each message read, the Cisco SCA BB extracts several option fields. You can configure which fields to extract. An RDR is generated even if none of the fields were found.

The RDR tag of the DHCP_RDR is 0xf0f0f042 / 4042321986.

Table 2-28 lists the DHCP RDR fields and descriptions.

Table 2-28 DHCP RDR Fields

RDR Field Name	Type	Description
CPE_MAC	STRING	DHCP protocol field.
CMTS_IP	UINT32	DHCP protocol field.
ASSIGNED_IP	UINT32	DHCP protocol field.
RELEASED_IP	UINT32	DHCP protocol field.
TRANSACTION_ID	UINT32	DHCP protocol field.
MESSAGE_TYPE	UINT8	DHCP message type.
OPTION_TYPE_0 through OPTION_TYPE_7	UINT8	List of DHCP options extracted from the message.
OPTION_TYPE_0 through OPTION_TYPE_7	STRING	Values associated with the above DHCP options.
END_TIME	INT32	Ending time stamp of this RDR. The field is in UNIX time_t format, which is the number of seconds since midnight of 1 January 1970.

DHCPv6 RDR

The DHCPv6_RDR is generated each time a DHCPv6 message of a specific type is intercepted.

Note DHCPv6 RDRs are generated only if they are activated by a subscriber integration system, such as the Cisco Service Control Subscriber Manager DHCPv6 Login Event Generator (LEG).

From each message that is read, the Cisco SCA BB extracts several option fields. You can configure which fields to extract. An RDR is generated even if none of the fields are found.

The RDR tag of the DHCPv6_RDR is 0xf0f0f044 / 4042321988.

Table 2-29 lists the DHCPv6 RDR fields and descriptions.

Table 2-29 DHCPv6 RDR Fields

RDR Field Name	Type	Description	Example
DUID	STRING	DHCP Unique Identifier field of the DHCPv6 message. If the DUID type is link layer, the value is displayed in ASCII format.	À%D+V This value indicates a DUID with type link layer.
CMTS_IPv6	STRING	IPv6 address of the CMTS.	fe80::1f:6cff:feef:ff65
TRANSACTION_ID	UINT32	Transaction ID of the DHCPv6 message.	16028092
MSG_TYPE	UINT8	Type of DHCPv6 message.	7
IPV6_PREFIX	STRING	IPv6 prefix, length, and valid life time or lease time, in seconds, captured in the format: IPv6Prefix Length LeaseTime. If the DHCPv6 message contains more than one prefix, the values are captured in the format: IPv6Prefix Length LeaseTime IPv6Prefix Length LeaseTime IPv6Prefix Length LeaseTime.	Example for an instance with one prefix in message: 2002:30FF:0903:672A :: 64 5930393 Example for an instance with multiple prefixes in message: 2002:30FF:0903:672A :: 64 5930393 2002:30FF:0903:672B :: 64 5930393

Table 2-29 DHCPv6 RDR Fields (continued)

RDR Field Name	Type	Description	Example
IA_NA_ADDRESS	STRING	The Identity Association for Non-temporary Addresses (IA_NA) identifier in the transaction. The value is captured in the format: IPv6Address LeaseTime If the message contains more than one IA_NA address, the values are captured in the format: IPv6Address LeaseTime IPv6Address LeaseTime IPv6Address LeaseTime.	Example for an instance with one IA_NA identifier: 2002:30FF:0903:672A :333:333:333:3333 5930393 Example for an instance with multiple IA_NA identifiers: 2002:30FF:0903:672A :333:333:333:3333 5930393 2002:30FF:0903:672A :333:333:333:3334 5930393
OPTION_TYPE_0 through OPTION_TYPE_7	UINT16	List of DHCPV6 options extracted from the message.	37
OPTION_VALUE_ 0 through OPTION_VALUE_ 7	STRING	Values associated with the above DHCPV6 options, displayed in ASCII format.	050103040506

RADIUS RDR

The RADIUS_RDR is generated each time a RADIUS message of a specified type is intercepted.

Note RADIUS RDRs are generated only if activated by a subscriber integration system, such as the SCMS-SM RADIUS LEG.

For each message read, Cisco SCA BB extracts several option fields. You can configure which fields to extract. An RDR is generated even if none of the fields were found.

The RDR tag of the RADIUS_RDR is 0xf0f0f043 / 4042321987.

Table 2-30 lists the RADIUS RDR fields and descriptions.

Table 2-30 RADIUS RDR Fields

RDR Field Name	Type	Description
SERVER_IP	UINT32	Destination IP address of the reported session. (The destination is defined as the server or the listener of the networking session.) The IP address is in a 32-bit binary format, but the value is obtained in decimal format in RDR.
SERVER_PORT	UINT16	Destination port number of the TCP/UDP-based networking session. For non-TCP/UDP sessions, this field contains the IP protocol number of the session flow.
CLIENT_IP	UINT32	IP address of the client side of the reported session. (The client side is defined as the initiator of the networking session.) The IP address is in a 32-bit binary format, but the value is obtained in decimal format in RDR.
CLIENT_PORT	UINT16	Port number of the client side (initiator) of the TCP/UDP-based networking session. For non-TCP/UDP sessions, this field has the value zero.
INITIATING_SIDE	INT8	Side of the SCE platform on which the initiator of the transaction resides: • 0—Subscriber side • 1—Network side
RADIUS_PACKET_CODE	UINT8	Type of the RADIUS message intercepted.
RADIUS_ID	UINT8	RADIUS transaction ID.
ATTRIBUTE_VALUE_1 through ATTRIBUTE_VALUE_20	STRING	Attributes extracted from the message. Sent as string format type, length, value (TLV). The last attribute field filled takes the value 0.

Flow Start RDR

The FLOW_START_RDR is generated when a flow starts, as follows:

- Any flow on packages and services that are configured to generate such an RDR.
- When an SIP INVITE request for voice and video traffic is received.

This RDR is designed for services and packages where specific, per-transaction RDRs are required (for example, transaction-level billing). It is easy to configure this RDR, in error, so that it is generated for every transaction, which may result in an excessive RDR rate.

Note Configure the generation scheme for this RDR with extra care.

The RDR tag of the FLOW_START_RDR is 0xf0f0f016 / 4042321942.

Table 2-31 lists the Flow Start RDR fields and their descriptions.

Table 2-31 Flow Start RDR Fields

RDR Field Name	Type	Description
SUBSCRIBER_ID	STRING	Subscriber identification string, introduced through the subscriber management interfaces. It may contain up to 64 characters. For unknown subscribers, this field may contain an empty string.
PACKAGE_ID	INT16	ID of the package assigned to the subscriber whose traffic is being reported. An assigned Package ID is an integer value between 0 and 4999. The value 4999 is reserved for unknown subscribers, and this is the maximum_number_of_packages possible.
SERVICE_ID	INT32	Service classification of the reported session. For example, in the Transaction RDR, this field indicates which service was accessed, and in the Breaching RDR, this field indicates which service was breached.
IP_PROTOCOL	UINT8	IP protocol type.
SERVER_IP	UINT32	Contains the destination IP address of the reported session. (The destination is defined as the server or the listener of the networking session.) The IP address is in a 32-bit binary format, but the value is obtained in decimal format in RDR.
SERVER_PORT	UINT16	Destination port number of the TCP/UDP-based networking session. For non-TCP/UDP sessions, this field contains the IP protocol number of the session flow.
CLIENT_IP	UINT32	IP address of the client side of the reported session. The client side is defined as the initiator of the networking session. The IP address is in a 32-bit binary format, but the value is obtained in decimal format in RDR.

Table 2-31 Flow Start RDR Fields

RDR Field Name	Type	Description
CLIENT_PORT	UINT16	Port number of the client side (initiator) of the TCP/UDP-based networking session. For non-TCP/UDP sessions, this field has the value zero.
INITIATING_SIDE	INT8	Side of the SCE platform on which the initiator of the transaction resides: • 0—Subscriber side • 1—Network side
START_TIME	UINT32	Flow start time.
REPORT_TIME	UINT32	Ending time stamp of this RDR. The field is in UNIX time_t format, which is the number of seconds since midnight of 1 January 1970.
BREACH_STATE	INT8	Indicates whether the quota allocated to the subscriber was breached.: • 0—Not breached • 1—Breached
FLOW ID	UINT32	Internal flow ID.
GENERATOR_ID	INT8	Numeric value identifying the processor generating the RDR.
IP_TYPE	UINT8	Defines the IP flow type of the respective RDR. For example, when the flow type is IPv6, the IPv4 address of the RDR will contain the value zero. However, the IPv6 address of the RDR will contain a white space for IPv4 flow type.
SERVERIPv6ADDRESS	STRING	Destination IPv6 address of the reported session. The destination is defined as the server or the listener of the networking session.
CLIENTIPv6ADDRESS	STRING	IPv6 address of the client side of the reported session. The client side is defined as the initiator of the networking session.

Anonymized Flow Start RDR

The ANONYMIZED_FLOW_START_RDR is generated when a flow starts, as follows:

- Any flow on packages and services that are configured to generate such an RDR.
- When an SIP INVITE request for voice and video traffic is received.

This RDR does not contain personal subscriber data.

This RDR is designed for services and packages where specific, per-transaction RDRs are required (for example, transaction-level billing). It is easy to configure this RDR, in error, so that it is generated for every transaction, which may result in an excessive RDR rate.

Note Configure the generation scheme for this RDR with extra care.

The RDR tag of the ANONYMIZED_FLOW_START_RDR is 0xf0f0f549 / 4042323273.

Table 2-32 lists the Anonymized Flow Start RDR fields and their descriptions.

Table 2-32 Anonymized Flow Start RDR Fields

RDR Field Name	Type	Description
HASHED_SUBSCRIBER_ID	STRING	Subscriber identification string, introduced through the subscriber management interfaces, may be passed through hashing algorithm. It may contain up to 64 characters. For unknown subscribers, this field may contain an empty string.
PACKAGE_ID	INT16	ID of the package assigned to the subscriber whose traffic is being reported. An assigned Package ID is an integer value between 0 and 4999. The value 4999 is reserved for unknown subscribers, and this is the maximum_number_of_packages possible.
SERVICE_ID	INT32	Service classification of the reported session. For example, in the Transaction RDR, this field indicates which service was accessed, and in the Breaching RDR, this field indicates which service was breached.
IP_PROTOCOL	UINT8	IP protocol type.
SERVER_IP	UINT32	Contains the destination IP address of the reported session. The destination is defined as the server or the listener of the networking session. The IP address is in a 32-bit binary format, but the value is obtained in decimal format in RDR. If this is the subscriber IP, this field may contain the short-hash of the IP if configured.
SERVER_PORT	UINT16	Destination port number of the TCP/UDP-based networking session. For non-TCP/UDP sessions, this field contains the IP protocol number of the session flow.

Table 2-32 Anonymized Flow Start RDR Fields

RDR Field Name	Type	Description
CLIENT_IP	UINT32	IP address of the client side of the reported session. (The client side is defined as the initiator of the networking session.) The IP address is in a 32-bit binary format, but the value is obtained in decimal format in RDR. If this is the subscriber IP, this field may contain the short-hash of the IP if configured.
CLIENT_PORT	UINT16	Port number of the client side (initiator) of the TCP/UDP-based networking session. For non-TCP/UDP sessions, this field has the value zero.
INITIATING_SIDE	INT8	Side of the SCE platform on which the initiator of the transaction resides: • 0—Subscriber side • 1—Network side
START_TIME	UINT32	Flow start time.
REPORT_TIME	UINT32	Ending time stamp of this RDR. The field is in UNIX time_t format, which is the number of seconds since midnight of 1 January 1970.
BREACH_STATE	INT8	Indicates whether the quota allocated to the subscriber was breached: • 0—Not breached • 1—Breached
FLOW ID	UINT32	Internal flow ID.
GENERATOR_ID	INT8	Numeric value identifying the processor generating the RDR.
IP_TYPE	UINT8	Defines the IP flow type of the respective RDR. For example, when the flow type is IPv6, the IPv4 address of the RDR will contain the value zero. However, the IPv6 address of the RDR will contain a white space for IPv4 flow type.
SERVERIPv6ADDRESS	STRING	Destination IPv6 address of the reported session. The destination is defined as the server or the listener of the networking session. If this is the subscriber IP, this field may contain a 32-byte string hash, if configured.
CLIENTIPv6ADDRESS	STRING	IPv6 address of the client side of the reported session. The client side is defined as the initiator of the networking session. If this is the subscriber IP, this field may contain a 32-byte string hash, if configured.

Flow End RDR

The FLOW_END_RDR is generated when a flow stops, for any flow that generated a FLOW_START_RDR.

This RDR is designed for services and packages where specific, per-transaction RDRs are required (for example, transaction-level billing). It is easy to configure this RDR, in error, so that it is generated for every transaction, which may result in an excessive RDR rate.

Note Configure the generation scheme for this RDR with extra care.

The RDR tag of the FLOW_END_RDR is 0xf0f0f018 / 4042321944.

Table 2-33 lists the Flow End RDR fields and their descriptions.

Table 2-33 Flow End RDR Fields

RDR Field Name	Type	Description
SUBSCRIBER_ID	STRING	Subscriber identification string, introduced through the subscriber management interfaces. It may contain up to 64 characters. For unknown subscribers, this field may contain an empty string.
PACKAGE_ID	INT16	ID of the package assigned to the subscriber whose traffic is being reported. An assigned Package ID is an integer value between 0 and 4999. The value 4999 is reserved for unknown subscribers, and this is the maximum_number_of_packages possible.
SERVICE_ID	INT32	Service classification of the reported session. For example, in the Transaction RDR, this field indicates which service was accessed, and in the Breaching RDR, this field indicates which service was breached.
IP_PROTOCOL	UINT8	IP protocol type.
SERVER_IP	UINT32	Destination IP address of the reported session. (The destination is defined as the server or the listener of the networking session.) The IP address is in a 32-bit binary format, but the value is obtained in decimal format in RDR.
SERVER_PORT	UINT16	Destination port number of the TCP/UDP-based networking session. For non-TCP/UDP sessions, this field contains the IP protocol number of the session flow.
CLIENT_IP	UINT32	IP address of the client side of the reported session. (The client side is defined as the initiator of the networking session.) The IP address is in a 32-bit binary format, but the value is obtained in decimal format in RDR.
CLIENT_PORT	UINT16	Port number of the client side (initiator) of the TCP/UDP-based networking session. For non-TCP/UDP sessions, this field has the value zero.

Table 2-33 Flow End RDR Fields (continued)

RDR Field Name	Type	Description
INITIATING_SIDE	INT8	Side of the SCE platform on which the initiator of the transaction resides: • 0—Subscriber side • 1—Network side
START_TIME	UINT32	Flow start time.
REPORT_TIME	UINT32	Ending time stamp of this RDR. The field is in UNIX time_t format, which is the number of seconds since midnight of 1 January 1970.
BREACH_STATE	INT8	Indicates whether the quota allocated to the subscriber was breached: • 0—Not breached • 1—Breached
FLOW ID	UINT32	Internal flow ID.
GENERATOR_ID	INT8	Numeric value identifying the processor generating the RDR.
IP_TYPE	UINT8	Defines the IP flow type of the respective RDR. For example, when the flow type is IPv6, the IPv4 address of the RDR will contain the value zero. However, the IPv6 address of the RDR will contain a white space for IPv4 flow type.
SERVERIPv6ADDRESS	STRING	Destination IPv6 address of the reported session. The destination is defined as the server or the listener of the networking session.
CLIENTIPv6ADDRESS	STRING	IPv6 address of the client side of the reported session. The client side is defined as the initiator of the networking session.

Anonymized Flow End RDR

The ANONYMIZED_FLOW_END_RDR is generated when a flow stops, for any flow that generated a FLOW_START_RDR.

This RDR does not contain personal subscriber data.

This RDR is designed for services and packages where specific, per-transaction RDRs are required (for example, transaction-level billing). It is easy to configure this RDR, in error, so that it is generated for every transaction, which may result in an excessive RDR rate.

Note Configure the generation scheme for this RDR with extra care.

The RDR tag of the ANONYMIZED_FLOW_END_RDR is 0xf0f0f54A / 4042323274.

Table 2-34 lists the Anonymized Flow End RDR fields and their descriptions.

Table 2-34 Anonymized Flow End RDR Fields

RDR Field Name	Type	Description
HASHED_SUBSCRIBER_ID	STRING	Subscriber identification string, introduced through the subscriber management interfaces, may be passed through hashing algorithm. It may contain up to 64 characters. For unknown subscribers, this field may contain an empty string.
PACKAGE_ID	INT16	ID of the package assigned to the subscriber whose traffic is being reported. An assigned Package ID is an integer value between 0 and 4999. The value 4999 is reserved for unknown subscribers, and this is the maximum_number_of_packages possible.
SERVICE_ID	INT32	Service classification of the reported session. For example, in the Transaction RDR, this field indicates which service was accessed, and in the Breaching RDR, this field indicates which service was breached.
IP_PROTOCOL	UINT8	IP protocol type.
SERVER_IP	UINT32	Destination IP address of the reported session. The destination is defined as the server or the listener of the networking session. The IP address is in a 32-bit binary format, but the value is obtained in decimal format in RDR. If this is the subscriber IP, this field may contain the short-hash of the IP if configured.
SERVER_PORT	UINT16	Destination port number of the TCP/UDP-based networking session. For non-TCP/UDP sessions, this field contains the IP protocol number of the session flow.

Table 2-34 Anonymized Flow End RDR Fields (continued)

RDR Field Name	Type	Description
CLIENT_IP	UINT32	IP address of the client side of the reported session. The client side is defined as the initiator of the networking session. The IP address is in a 32-bit binary format, but the value is obtained in decimal format in RDR. If this is the subscriber IP, this field may contain the short-hash of the IP if configured.
CLIENT_PORT	UINT16	Port number of the client side (initiator) of the TCP/UDP-based networking session. For non-TCP/UDP sessions, this field has the value zero.
INITIATING_SIDE	INT8	Side of the SCE platform on which the initiator of the transaction resides: • 0—Subscriber side • 1—Network side
START_TIME	UINT32	Flow start time.
REPORT_TIME	UINT32	Ending time stamp of this RDR. The field is in UNIX time_t format, which is the number of seconds since midnight of 1 January 1970.
BREACH_STATE	INT8	Indicates whether the quota allocated to the subscriber was breached: • 0—Not breached • 1—Breached
FLOW ID	UINT32	Internal flow ID.
GENERATOR_ID	INT8	Numeric value identifying the processor generating the RDR.
IP_TYPE	UINT8	Defines the IP flow type of the respective RDR. For example, when the flow type is IPv6, the IPv4 address of the RDR will contain the value zero. However, the IPv6 address of the RDR will contain a white space for IPv4 flow type.
SERVERIPv6ADDRESS	STRING	Destination IPv6 address of the reported session. The destination is defined as the server or the listener of the networking session. If this is the subscriber IP, this field may contain a 32-byte string hash, if configured.
CLIENTIPv6ADDRESS	STRING	IPv6 address of the client side of the reported session. The client side is defined as the initiator of the networking session. If this is the subscriber IP, this field may contain a 32-byte string hash, if configured.

Flow Ongoing RDR

The FLOW_ONGOING_RDR is generated at set time intervals during the life of a flow, for any flow that generated a FLOW_START_RDR, if the system is configured to issue such RDR.

This RDR is designed for services and packages where specific, per-transaction RDRs are required (for example, transaction-level billing). It is easy to configure this RDR, in error, so that it is generated for every transaction, which may result in an excessive RDR rate.

Note Configure the generation scheme for this RDR with extra care.

The RDR tag of the FLOW_ONGOING_RDR is 0xf0f0f017 / 4042321943.

Table 2-35 lists the Flow Ongoing RDR fields and their descriptions.

Table 2-35 Flow Ongoing RDR Fields

RDR Field Name	Type	Description
SUBSCRIBER_ID	STRING	Subscriber identification string, introduced through the subscriber management interfaces. It may contain up to 64 characters. For unknown subscribers, this field may contain an empty string.
PACKAGE_ID	INT16	ID of the package assigned to the subscriber whose traffic is being reported. An assigned Package ID is an integer between 0 and 4999. The value 4999 is reserved for unknown subscribers, and this is the maximum_number_of_packages possible.
SERVICE_ID	INT32	Service classification of the reported session. For example, in the Transaction RDR, this field indicates which service was accessed, and in the Breaching RDR, this field indicates which service was breached.
IP_PROTOCOL	UINT8	IP protocol type.
SERVER_IP	UINT32	Destination IP address of the reported session. The destination is defined as the server or the listener of the networking session. The IP address is in a 32-bit binary format, but the value is obtained in decimal format in RDR.
SERVER_PORT	UINT16	Destination port number of the TCP/UDP-based networking session. For non-TCP/UDP sessions, this field contains the IP protocol number of the session flow.
CLIENT_IP	UINT32	IP address of the client side of the reported session. The client side is defined as the initiator of the networking session. The IP address is in a 32-bit binary format, but the value is obtained in decimal format in RDR.
CLIENT_PORT	UINT16	Port number of the client side (initiator) of the TCP/UDP-based networking session. For non-TCP/UDP sessions, this field has the value zero.

Table 2-35 Flow Ongoing RDR Fields (continued)

RDR Field Name	Type	Description
INITIATING_SIDE	INT8	Side of the SCE platform on which the initiator of the transaction resides: • 0—Subscriber side • 1—Network side
START_TIME	UINT32	Flow start time.
REPORT_TIME	UINT32	Ending time stamp of this RDR. The field is in UNIX time_t format, which is the number of seconds since midnight of 1 January 1970.
BREACH_STATE	INT8	Indicates whether the quota allocated to the subscriber was breached.: • 0—Not breached • 1—Breached
FLOW ID	UINT32	Internal flow ID.
GENERATOR_ID	INT8	Numeric value identifying the processor generating the RDR.
IP_TYPE	UINT8	Defines the IP flow type of the respective RDR. For example, when the flow type is IPv6, the IPv4 address of the RDR will contain the value zero. However, the IPv6 address of the RDR will contain a white space for IPv4 flow type.
SERVERIPv6ADDRESS	STRING	Destination IPv6 address of the reported session. The destination is defined as the server or the listener of the networking session.
CLIENTIPv6ADDRESS	STRING	IPv6 address of the client side of the reported session. The client side is defined as the initiator of the networking session.

Anonymized Flow Ongoing RDR

The ANONYMIZED_FLOW_ONGOING_RDR is generated at set time intervals during the life of a flow, for any flow that generated a FLOW_START_RDR, if the system is configured to issue such RDR.

This RDR does not contain personal subscriber data.

This RDR is designed for services and packages where specific, per-transaction RDRs are required (for example, transaction-level billing). It is easy to configure this RDR, in error, so that it is generated for every transaction, which may result in an excessive RDR rate.

Note Configure the generation scheme for this RDR with extra care.

The RDR tag of the ANONYMIZED_FLOW_ONGOING_RDR is 0xf0f0f54B / 4042323275.

Table 2-36 lists the Anonymized Flow Ongoing RDR fields and their descriptions.

Table 2-36 Anonymized Flow Ongoing RDR Fields

RDR Field Name	Type	Description
HASHED_SUBSCRIBER_ID	STRING	Subscriber identification string, introduced through the subscriber management interfaces, may be passed through hashing algorithm. It may contain up to 64 characters. For unknown subscribers, this field may contain an empty string.
PACKAGE_ID	INT16	ID of the package assigned to the subscriber whose traffic is being reported. An assigned Package ID is an integer between 0 and 4999. The value 4999 is reserved for unknown subscribers, and this is the maximum_number_of_packages possible.
SERVICE_ID	INT32	Service classification of the reported session. For example, in the Transaction RDR, this field indicates which service was accessed, and in the Breaching RDR, this field indicates which service was breached.
IP_PROTOCOL	UINT8	IP protocol type.
SERVER_IP	UINT32	Destination IP address of the reported session. The destination is defined as the server or the listener of the networking session. The IP address is in a 32-bit binary format, but the value is obtained in decimal format in RDR. If this is the subscriber IP, this field may contain the short-hash of the IP if configured.
SERVER_PORT	UINT16	Destination port number of the TCP/UDP-based networking session. For non-TCP/UDP sessions, this field contains the IP protocol number of the session flow.

Table 2-36 Anonymized Flow Ongoing RDR Fields (continued)

RDR Field Name	Type	Description
CLIENT_IP	UINT32	IP address of the client side of the reported session. The client side is defined as the initiator of the networking session. The IP address is in a 32-bit binary format, but the value is obtained in decimal format in RDR. If this is the subscriber IP, this field may contain the short-hash of the IP if configured.
CLIENT_PORT	UINT16	Port number of the client side (initiator) of the TCP/UDP-based networking session. For non-TCP/UDP sessions, this field has the value zero.
INITIATING_SIDE	INT8	Side of the SCE platform on which the initiator of the transaction resides: • 0—Subscriber side • 1—Network side
START_TIME	UINT32	Flow start time.
REPORT_TIME	UINT32	Ending time stamp of this RDR. The field is in UNIX time_t format, which is the number of seconds since midnight of 1 January 1970.
BREACH_STATE	INT8	Indicates whether the quota allocated to the subscriber was breached: • 0—Not breached • 1—Breached
FLOW ID	UINT32	Internal flow ID.
GENERATOR_ID	INT8	Numeric value identifying the processor generating the RDR.
IP_TYPE	UINT8	Defines the IP flow type of the respective RDR. For example, when the flow type is IPv6, the IPv4 address of the RDR will contain the value zero. However, the IPv6 address of the RDR will contain a white space for IPv4 flow type.
SERVERIPv6ADDRESS	STRING	Destination IPv6 address of the reported session. The destination is defined as the server or the listener of the networking session. If this is the subscriber IP, this field may contain a 32-byte string hash, if configured.
CLIENTIPv6ADDRESS	STRING	IPv6 address of the client side of the reported session. The client side is defined as the initiator of the networking session. If this is the subscriber IP, this field may contain a 32-byte string hash, if configured.

Media Flow RDR

The MEDIA_FLOW_RDR is generated at the end of every Session Initiation Protocol (SIP), Skype, H.323, Push-to-talk (PTT), Skinny Call Control Protocol (SCCP or Skinny), and Media Gateway Control Protocol (MGCP) media flow:

- For SIP, this RDR is generated when a media channel is closed.
- For Skype, H.323, PTT, and SCCP this RDR is generated when an end-of-call is detected.
- For MGCP, this RDR is generated when a media flow is closed.

Note SIP includes all SIP-based applications (such as Vonage and Yahoo Messenger VoIP).

The Media Flow RDR reports the QOS statistics retrieved from the Real Time Control Protocol (RTCP) flow. This RDR is independent of the control protocols.

Media Flow RDRs are not generated for the flows for which H.245 tunnelling is enabled. Cisco SCE supports a maximum of 4 RTP/RTCP flows.

The RDR tag of the MEDIA_FLOW_RDR is 0xF0F0F46C / 4042323052.

Table 2-37 lists the Media Flow RDR fields and their descriptions.

Table 2-37 Media Flow RDR Fields

RDR Field Name	Type	Description
SUBSCRIBER_ID	STRING	Subscriber identification string, introduced through the subscriber management interfaces. It may contain up to 64 characters. For unknown subscribers, this field contains a string N/A.
PACKAGE_ID	INT16	ID of the package assigned to the subscriber whose traffic is being reported. An assigned Package ID is an integer between 0 and 4999. The value 4999 is reserved for unknown subscribers, and this is the maximum_number_of_packages possible.
SERVICE_ID	INT32	Service classification of the reported session. For example, in the Transaction RDR, this field indicates which service was accessed, and in the Breaching RDR, this field indicates which service was breached.
PROTOCOL_ID	INT16	Unique ID of the protocol associated with the reported session.
DESTINATION_IP	UINT32	• SIP—Destination IP address of RTP flow. • Skype—Destination IP address of Skype flow. • H.323—Destination IP address of RTP flow. • PTT—Destination IP address of RTP flow. • SCCP—Destination IP address of RTP flow. • MGCP—Destination IP address of RTP flow.

Table 2-37 Media Flow RDR Fields (continued)

RDR Field Name	Type	Description
DESTINATION_PORT	UINT16	• SIP—Destination port of RTP flow. • Skype—Destination port of Skype flow. • H.323—Destination port of RTP flow. • PTT—Destination port of RTP flow. • SCCP—Destination port of RTP flow. • MGCP—Destination port of RTP flow.
SOURCE_IP	UINT32	• SIP—Source IP address of RTP flow. • Skype—Source IP address of Skype flow. • H.323—Source IP address of RTP flow. • PTT—Source IP address of RTP flow. • SCCP—Source IP address of RTP flow. • MGCP—Source IP address of RTP flow.
SOURCE_PORT	UINT16	• SIP—Source port of RTP flow. • Skype—Source port of Skype flow. • H.323—Source port of RTP flow. • PTT—Source port of RTP flow. • SCCP—Source port of RTP flow. • MGCP—Source port of RTP flow.
INITIATING_SIDE	INT8	Side of the SCE platform on which the initiator of the transaction resides: • 0—Subscriber side • 1—Network side For Skype, this field indicates the initiating side of the flow, and not necessarily the initiating side of the voice call.
ZONE_ID	INT32	ID of the zone associated with this session.
FLAVOR_ID	INT32	ID of the protocol signatures with flavor associated with this session.
DOMAIN	STRING	• SIP—Domain name extracted from the SIP header. • MGCP—Not applicable. • H.323—Not applicable. • PTT—Not applicable. • SCCP—Not applicable.

Table 2-37 Media Flow RDR Fields (continued)

RDR Field Name	Type	Description
USER_AGENT	STRING	• SIP—User-Agent field extracted from the SIP header. • MGCP—Not applicable. • H.323—Not applicable. • PTT—Not applicable. • SCCP—Not applicable.
START_TIME	UINT32	Flow start time.
REPORT_TIME	UINT32	Ending time stamp of this RDR. The field is in UNIX time_t format, which is the number of seconds since midnight of 1 January 1970.
DURATION_SECONDS	INT32	• SIP—The active duration from the SIP Invite request to the 200 OK BYE message, which includes the duration of the RTP flow pertaining to the end-of-call event. • Skype—Duration of the VoIP flow, excluding the aging time. • H.323—The active duration of the RTP flow, not including the aging time. • PTT—The active duration of the RTP flow, not including the aging time. • SCCP—The active duration of the RTP flow, not including the aging time. • MGCP—The active duration of the RTP flow, not including the aging time.
UPSTREAM_VOLUME	UINT32	• SIP—The upstream volume of the RTP flow, in bytes. • Skype—The upstream volume during VoIP flow. • H.323—The upstream volume of the RTP flow, in bytes. • PTT—The upstream volume of the RTP flow, in bytes. • SCCP—The upstream volume of the RTP flow, in bytes. • MGCP—The upstream volume of the RTP flow, in bytes.

Table 2-37 Media Flow RDR Fields (continued)

RDR Field Name	Type	Description
DOWNSTREAM_VOLUME	UINT32	• SIP—The downstream volume of the RTP flow, in bytes. • Skype—The downstream volume during VoIP flow. • H.323—The downstream volume of the RTP flow, in bytes. • PTT—The downstream volume of the RTP flow, in bytes. • SCCP—The downstream volume of the RTP flow, in bytes. • MGCP—The downstream volume of the RTP flow, in bytes.
IP_PROTOCOL	UINT8	IP protocol type: • 6—TCP • 17—UDP
FLOW_TYPE	INT8	• 0—All Skype, PTT, SKINNY, and H.323 flows • 1—Audio (SIP/MGCP/PTT/SKINNY/H.323) • 2—Video (SIP/MGCP/PTT/SKINNY/H.323)
SESSION_ID	UINT32	• SIP—The flow-context ID of the control flow. • Skype—The flow-context ID of the flow. • H.323—The flow-context ID of the control flow. • PTT—The flow-context ID of the control flow. • SCCP—The flow-context ID of the control flow. • MGCP—The flow-context ID of the control flow.

Table 2-37 Media Flow RDR Fields (continued)

RDR Field Name	Type	Description
UPSTREAM_JITTER	UINT32	• SIP—The average upstream jitter for the session, taken from the RTCP flow. The field will have the maximum value of data type, that is, (0xFFFFFFFF) if RTCP flow is missing. • Skype—N/A (0xFFFFFFFF). • H.323—The average upstream jitter for the session, taken from the RTCP flow. The field will have the maximum value of data type, that is, (0xFFFFFFFF) if RTCP flow is missing. • PTT—The average upstream jitter for the session, taken from the RTCP flow. The field will have the maximum value of data type, that is, (0xFFFFFFFF) if RTCP flow is missing. • SCCP—The average upstream jitter for the session, taken from the RTCP flow. The field will have the maximum value of data type, that is, (0xFFFFFFFF) if RTCP flow is missing. • MGCP—The average upstream jitter for the session, taken from the RTCP flow. The field will have the maximum value of data type, that is, (0xFFFFFFFF) if RTCP flow is missing.
DOWNSTREAM_JITTER	UINT32	• SIP—The average downstream jitter for the session, taken from the RTCP flow. The field will have the maximum value of data type, that is, (0xFFFFFFFF) if RTCP flow is missing. • Skype—N/A (0xFFFFFFFF). • H.323—The average downstream jitter for the session, taken from the RTCP flow. The field will have the maximum value of data type, that is, (0xFFFFFFFF) if RTCP flow is missing. • PTT—The average downstream jitter for the session, taken from the RTCP flow. The field will have the maximum value of data type, that is, (0xFFFFFFFF) if RTCP flow is missing. • SCCP—The average downstream jitter for the session, taken from the RTCP flow. The field will have the maximum value of data type, that is, (0xFFFFFFFF) if RTCP flow is missing. • MGCP—The average downstream jitter for the session, taken from the RTCP flow. The field will have the maximum value of data type, that is, (0xFFFFFFFF) if RTCP flow is missing.

Table 2-37 Media Flow RDR Fields (continued)

RDR Field Name	Type	Description
UPSTREAM_PACKET_LOSS	UINT16	• SIP—The average fractional upstream packet loss for the session, taken from the RTCP flow. The field will have the maximum value of data type, that is, (0xFFFFFFFF) if RTCP flow is missing. • Skype—N/A (0xFFFF). • H.323—The average fractional upstream packet loss for the session, taken from the RTCP flow. The field will have the maximum value of data type, that is, (0xFFFFFFFF) if RTCP flow is missing. • PTT—The average fractional upstream packet loss for the session, taken from the RTCP flow. The field will have the maximum value of data type, that is, (0xFFFFFFFF) if RTCP flow is missing. • SCCP—The average fractional upstream packet loss for the session, taken from the RTCP flow. The field will have the maximum value of data type, that is, (0xFFFFFFFF) if RTCP flow is missing. • MGCP—The average fractional upstream packet loss for the session, taken from the RTCP flow. The field will have the maximum value of data type, that is, (0xFFFFFFFF) if RTCP flow is missing.

Table 2-37 Media Flow RDR Fields (continued)

RDR Field Name	Type	Description
DOWNSTREAM_PACKET_LOSS	UINT16	• SIP—The average fractional downstream packet loss for the session, taken from the RTCP flow. The field will have the maximum value of data type, that is, (0xFFFFFFFF) if RTCP flow is missing. • Skype—N/A (0xFFFF). • H.323—The average fractional downstream packet loss for the session, taken from the RTCP flow. The field will have the maximum value of data type, that is, (0xFFFFFFFF) if RTCP flow is missing. • PTT—The average fractional downstream packet loss for the session, taken from the RTCP flow. The field will have the maximum value of data type, that is, (0xFFFFFFFF) if RTCP flow is missing. • SCCP—The average fractional downstream packet loss for the session, taken from the RTCP flow. The field will have the maximum value of data type, that is, (0xFFFFFFFF) if RTCP flow is missing. • MGCP—The average fractional downstream packet loss for the session, taken from the RTCP flow. The field will have the maximum value of data type, that is, (0xFFFFFFFF) if RTCP flow is missing.
UPSTREAM_PAYLOAD_TYPE	UINT8	• SIP—The upstream RTP payload type for the session. • Skype—N/A (0xFF). • H.323—The upstream RTP payload type for the session. • PTT—The upstream RTP payload type for the session. • SCCP—The upstream RTP payload type for the session. • MGCP—The upstream RTP payload type for the session.

Table 2-37 Media Flow RDR Fields (continued)

RDR Field Name	Type	Description
DOWNSTREAM_PAYLOAD_TYPE	UINT8	• SIP—The downstream RTP payload type for the session. • Skype—N/A (0xFF). • H.323—The downstream RTP payload type for the session. • PTT—The downstream RTP payload type for the session. • SCCP—The downstream RTP payload type for the session. • MGCP—The downstream RTP payload type for the session.
IP_TYPE	UINT8	Defines the IP flow type of the respective RDR. For example, when the flow type is IPv6, the IPv4 address of the RDR will contain the value zero. However, the IPv6 address of the RDR will contain a white space for IPv4 flow type.
SERVERIPv6ADDRESS	STRING	• SIP—Destination IPv6 address of RTP flow. • Skype—Destination IPv6 address of Skype flow. • H.323—Destination IPv6 address of RTP flow. • PTT—Destination IPv6 address of RTP flow. • SCCP—Destination IPv6 address of RTP flow. • MGCP—Destination IPv6 address of RTP flow.
CLIENTIPv6ADDRESS	STRING	• SIP—Source IPv6 address of RTP flow. • Skype—Source IPv6 address of Skype flow. • H.323—Source IPv6 address of RTP flow. • PTT—Source IPv6 address of RTP flow. • SCCP—Source IPv6 address of RTP flow. • MGCP—Source IPv6 address of RTP flow.

Note

Packet Loss

This field is taken from the RTCP field “fraction lost”. It is the average value of all RTCP packets seen during the flow life for the specified direction. The value is the numerator of a fraction whose denominator is 256. To get the packet loss value as percentage, divide this value by 2.56.

Average Jitter

This field is taken from the RTCP field “interval jitter”. The reported value is the average value of all RTCP packets seen during the flow life for the specified direction. This value is multiplied by the NTP time-stamp delta (middle 32 bits) and divided by the RTCP time-stamp delta to convert it to normal time

units. These two time stamps are also taken from the RTCP packet. The reported value is the average jitter in units of 1/65536 second. To convert to milliseconds, divide by 65.536.

For more information about the RCP/RTCP standard, see RFC 1889.

Anonymized Media Flow RDR

The ANONYMIZED_MEDIA_FLOW_RDR is generated at the end of every Session Initiation Protocol (SIP), Skype, H.323, Push-to-talk (PTT), Skinny Call Control Protocol (SCCP or Skinny), and Media Gateway Control Protocol (MGCP) media flow, without personal subscriber data:

- For SIP, this RDR is generated when a media channel is closed.
- For Skype, H.323, PTT, and SCCP this RDR is generated when an end-of-call is detected.
- For MGCP, this RDR is generated when a media flow is closed.

Note SIP includes all SIP-based applications (such as Vonage and Yahoo Messenger VoIP).

The Anonymized Media Flow RDR reports the QOS statistics retrieved from the Real Time Control Protocol (RTCP) flow. This RDR is independent of the control protocols.

Anonymized Media Flow RDRs are not generated for the flows for which H.245 tunnelling is enabled. Cisco SCE supports a maximum of 4 RTP/RTCP flows.

The RDR tag of the ANONYMIZED_MEDIA_FLOW_RDR is 0xf0f0f54C / 4042323276.

Table 2-38 lists the Anonymized Media Flow RDR fields and their descriptions.

Table 2-38 Anonymized Media Flow RDR Fields

RDR Field Name	Type	Description
HASHED_SUBSCRIBER_ID	STRING	Subscriber identification string, introduced through the subscriber management interfaces, may be passed through hashing algorithm. It may contain up to 64 characters. For unknown subscribers, this field contains a string N/A.
PACKAGE_ID	INT16	ID of the package assigned to the subscriber whose traffic is being reported. An assigned Package ID is an integer between 0 and 4999. The value 4999 is reserved for unknown subscribers, and this is the maximum_number_of_packages possible.
SERVICE_ID	INT32	Service classification of the reported session. For example, in the Transaction RDR, this field indicates which service was accessed, and in the Breaching RDR, this field indicates which service was breached.
PROTOCOL_ID	INT16	Unique ID of the protocol associated with the reported session.

Table 2-38 Anonymized Media Flow RDR Fields (continued)

RDR Field Name	Type	Description
DESTINATION_IP	UINT32	• SIP—Destination IP address of RTP flow. • Skype—Destination IP address of Skype flow. • H.323—Destination IP address of RTP flow. • PTT—Destination IP address of RTP flow. • SCCP—Destination IP address of RTP flow. • MGCP—Destination IP address of RTP flow. If this is the subscriber IP, this field may contain the short hash of the IP, if configured.
DESTINATION_PORT	UINT16	• SIP—Destination port of RTP flow. • Skype—Destination port of Skype flow. • H.323—Destination port of RTP flow. • PTT—Destination port of RTP flow. • SCCP—Destination port of RTP flow. • MGCP—Destination port of RTP flow.
SOURCE_IP	UINT32	• SIP—Source IP address of RTP flow. • Skype—Source IP address of Skype flow. • H.323—Source IP address of RTP flow. • PTT—Source IP address of RTP flow. • SCCP—Source IP address of RTP flow. • MGCP—Source IP address of RTP flow. If this is the subscriber IP, this field may contain the short hash of the IP, if configured.
SOURCE_PORT	UINT16	• SIP—Source port of RTP flow. • Skype—Source port of Skype flow. • H.323—Source port of RTP flow. • PTT—Source port of RTP flow. • SCCP—Source port of RTP flow. • MGCP—Source port of RTP flow.
INITIATING_SIDE	INT8	Side of the SCE platform on which the initiator of the transaction resides: • 0—Subscriber side • 1—Network side For Skype, this field indicates the initiating side of the flow, and not necessarily the initiating side of the voice call.
ZONE_ID	INT32	ID of the zone associated with this session.

Table 2-38 Anonymized Media Flow RDR Fields (continued)

RDR Field Name	Type	Description
FLAVOR_ID	INT32	ID of the protocol signatures with flavor associated with this session.
DOMAIN	STRING	• SIP—Domain name extracted from the SIP header. • MGCP—Not applicable. • H.323—Not applicable. • PTT—Not applicable. • SCCP—Not applicable.
USER_AGENT	STRING	• SIP—User-Agent field extracted from the SIP header. • MGCP—Not applicable. • H.323—Not applicable. • PTT—Not applicable. • SCCP—Not applicable.
START_TIME	UINT32	Flow start time.
REPORT_TIME	UINT32	Ending time stamp of this RDR. The field is in UNIX time_t format, which is the number of seconds since midnight of 1 January 1970.
DURATION_SECONDS	INT32	• SIP—The active duration of the RTP flow, not including aging timke. • Skype—Duration of the VoIP flow, excluding the aging time. • H.323—The active duration of the RTP flow, not including the aging time. • PTT—The active duration of the RTP flow, not including the aging time. • SCCP—The active duration of the RTP flow, not including the aging time. • MGCP—The active duration of the RTP flow, not including the aging time.

Table 2-38 Anonymized Media Flow RDR Fields (continued)

RDR Field Name	Type	Description
UPSTREAM_VOLUME	UINT32	• SIP—The upstream volume of the RTP flow, in bytes. • Skype—The upstream volume during VoIP flow. • H.323—The upstream volume of the RTP flow, in bytes. • PTT—The upstream volume of the RTP flow, in bytes. • SCCP—The upstream volume of the RTP flow, in bytes. • MGCP—The upstream volume of the RTP flow, in bytes.
DOWNSTREAM_VOLUME	UINT32	• SIP—The downstream volume of the RTP flow, in bytes. • Skype—The downstream volume during VoIP flow. • H.323—The downstream volume of the RTP flow, in bytes. • PTT—The downstream volume of the RTP flow, in bytes. • SCCP—The downstream volume of the RTP flow, in bytes. • MGCP—The downstream volume of the RTP flow, in bytes.
IP_PROTOCOL	UINT8	IP protocol type: • 6—TCP • 17—UDP
FLOW_TYPE	INT8	• 0—All Skype, PTT, SKINNY, and H.323 flows • 1—Audio (SIP/MGCP/PTT/SKINNY/H.323) • 2—Video (SIP/MGCP/PTT/SKINNY/H.323)
SESSION_ID	UINT32	• SIP—The flow-context ID of the control flow. • Skype—The flow-context ID of the flow. • H.323—The flow-context ID of the control flow. • PTT—The flow-context ID of the control flow. • SCCP—The flow-context ID of the control flow. • MGCP—The flow-context ID of the control flow.

Table 2-38 Anonymized Media Flow RDR Fields (continued)

RDR Field Name	Type	Description
UPSTREAM_JITTER	UINT32	• SIP—The average upstream jitter for the session, taken from the RTCP flow. The field will have the maximum value of data type, that is, (0xFFFFFFFF) if RTCP flow is missing. • Skype—N/A (0xFFFFFFFF). • H.323—The average upstream jitter for the session, taken from the RTCP flow. The field will have the maximum value of data type, that is, (0xFFFFFFFF) if RTCP flow is missing. • PTT—The average upstream jitter for the session, taken from the RTCP flow. The field will have the maximum value of data type, that is, (0xFFFFFFFF) if RTCP flow is missing. • SCCP—The average upstream jitter for the session, taken from the RTCP flow. The field will have the maximum value of data type, that is, (0xFFFFFFFF) if RTCP flow is missing. • MGCP—The average upstream jitter for the session, taken from the RTCP flow. The field will have the maximum value of data type, that is, (0xFFFFFFFF) if RTCP flow is missing.
DOWNSTREAM_JITTER	UINT32	• SIP—The average downstream jitter for the session, taken from the RTCP flow. The field will have the maximum value of data type, that is, (0xFFFFFFFF) if RTCP flow is missing. • Skype—N/A (0xFFFFFFFF). • H.323—The average downstream jitter for the session, taken from the RTCP flow. The field will have the maximum value of data type, that is, (0xFFFFFFFF) if RTCP flow is missing. • PTT—The average downstream jitter for the session, taken from the RTCP flow. The field will have the maximum value of data type, that is, (0xFFFFFFFF) if RTCP flow is missing. • SCCP—The average downstream jitter for the session, taken from the RTCP flow. The field will have the maximum value of data type, that is, (0xFFFFFFFF) if RTCP flow is missing. • MGCP—The average downstream jitter for the session, taken from the RTCP flow. The field will have the maximum value of data type, that is, (0xFFFFFFFF) if RTCP flow is missing.

Table 2-38 Anonymized Media Flow RDR Fields (continued)

RDR Field Name	Type	Description
UPSTREAM_PACKET_LOSS	UINT16	• SIP—The average fractional upstream packet loss for the session, taken from the RTCP flow. The field will have the maximum value of data type, that is, (0xFFFFFFFF) if RTCP flow is missing. • Skype—N/A (0xFFFF). • H.323—The average fractional upstream packet loss for the session, taken from the RTCP flow. The field will have the maximum value of data type, that is, (0xFFFFFFFF) if RTCP flow is missing. • PTT—The average fractional upstream packet loss for the session, taken from the RTCP flow. The field will have the maximum value of data type, that is, (0xFFFFFFFF) if RTCP flow is missing. • SCCP—The average fractional upstream packet loss for the session, taken from the RTCP flow. The field will have the maximum value of data type, that is, (0xFFFFFFFF) if RTCP flow is missing. • MGCP—The average fractional upstream packet loss for the session, taken from the RTCP flow. The field will have the maximum value of data type, that is, (0xFFFFFFFF) if RTCP flow is missing.

Table 2-38 Anonymized Media Flow RDR Fields (continued)

RDR Field Name	Type	Description
DOWNSTREAM_PACKET_LOSS	UINT16	• SIP—The average fractional downstream packet loss for the session, taken from the RTCP flow. The field will have the maximum value of data type, that is, (0xFFFFFFFF) if RTCP flow is missing. • Skype—N/A (0xFFFF). • H.323—The average fractional downstream packet loss for the session, taken from the RTCP flow. The field will have the maximum value of data type, that is, (0xFFFFFFFF) if RTCP flow is missing. • PTT—The average fractional downstream packet loss for the session, taken from the RTCP flow. The field will have the maximum value of data type, that is, (0xFFFFFFFF) if RTCP flow is missing. • SCCP—The average fractional downstream packet loss for the session, taken from the RTCP flow. The field will have the maximum value of data type, that is, (0xFFFFFFFF) if RTCP flow is missing. • MGCP—The average fractional downstream packet loss for the session, taken from the RTCP flow. The field will have the maximum value of data type, that is, (0xFFFFFFFF) if RTCP flow is missing.
UPSTREAM_PAYLOAD_TYPE	UINT8	• SIP—The upstream RTP payload type for the session. • Skype—N/A (0xFF). • H.323—The upstream RTP payload type for the session. • PTT—The upstream RTP payload type for the session. • SCCP—The upstream RTP payload type for the session. • MGCP—The upstream RTP payload type for the session.

Table 2-38 Anonymized Media Flow RDR Fields (continued)

RDR Field Name	Type	Description
DOWNSTREAM_PAYLOAD_TYPE	UINT8	• SIP—The downstream RTP payload type for the session. • Skype—N/A (0xFF). • H.323—The downstream RTP payload type for the session. • PTT—The downstream RTP payload type for the session. • SCCP—The downstream RTP payload type for the session. • MGCP—The downstream RTP payload type for the session.
IP_TYPE	UINT8	Defines the IP flow type of the respective RDR. For example, when the flow type is IPv6, the IPv4 address of the RDR will contain the value zero. However, the IPv6 address of the RDR will contain a white space for IPv4 flow type.
SERVERIPv6ADDRESS	STRING	• SIP—Destination IPv6 address of RTP flow. • Skype—Destination IPv6 address of Skype flow. • H.323—Destination IPv6 address of RTP flow. • PTT—Destination IPv6 address of RTP flow. • SCCP—Destination IPv6 address of RTP flow. • MGCP—Destination IPv6 address of RTP flow. If this is the subscriber IP address, this field may contain a 32-byte string hash, if configured.
CLIENTIPv6ADDRESS	STRING	• SIP—Source IP address of RTP flow. • Skype—Source IP address of Skype flow. • H.323—Source IP address of RTP flow. • PTT—Source IP address of RTP flow. • SCCP—Source IP address of RTP flow. • MGCP—Source IP address of RTP flow. If this is the subscriber IP address, this field may contain a 32-byte string hash, if configured.

Note **Packet Loss**

This field is taken from the RTCP field “fraction lost”. It is the average value of all RTCP packets seen during the flow life for the specified direction. The value is the numerator of a fraction whose denominator is 256. To get the packet loss value as percentage, divide this value by 2.56.

Average Jitter

This field is taken from the RTCP field “interval jitter”. The reported value is the average value of all RTCP packets seen during the flow life for the specified direction. This value is multiplied by the NTP time-stamp delta (middle 32 bits) and divided by the RTCP time-stamp delta to convert it to normal time units. These two time stamps are also taken from the RTCP packet. The reported value is the average jitter in units of 1/65536 second. To convert to milliseconds, divide by 65.536.

For more information about the RCP/RTCP standard, see RFC 1889.

Attack Start RDR

The ATTACK_START_RDR is generated at the beginning of an attack for all attack types that are configured to generate such an RDR. (To enable and configure the generation of these RDRs, see "The Service Security Dashboard" section in the "Using the Service Configuration Editor: Additional Options" chapter of *Cisco Service Control Application for Broadband User Guide*.)

The RDR tag of the ATTACK_START_RDR is 0xf0f0f019 / 4042321945.

Table 2-39 lists the Attack Start RDR fields and their descriptions.

Table 2-39 Attack Start RDR Fields

RDR Field Name	Type	Description
SUBSCRIBER_ID	STRING	Subscriber identification string, introduced through the subscriber management interfaces. It may contain up to 64 characters. For unknown subscribers, this field may contain an empty string.
ATTACK_ID	UINT32	Unique attack ID.
ATTACKING_IP	UINT32	IP address related to the attack (for example, in a DDoS, this is the IP address under attack; in a scan, this is the IP address of the source of the scan).
ATTACKED_IP	UINT32	Other IP address related to the attack, if one exists; otherwise, 0xFFFFFFFF.
ATTACKED_PORT	UINT16	Attacked port; 0xFFFF if not present.
ATTACKING_SIDE	INT8	Side of the SCE ATTACKING_IP on which it resides: • 0—Subscriber • 1—Network
IP_PROTOCOL	UINT8	IP protocol type.
ATTACK_TYPE	UINT32	ATTACKING_IP to whom it belongs: • 0—Attacked • 1—Attacker
GENERATOR_ID	INT8	Numeric value identifying the processor generating the RDR.
ATTACK_TIME	UINT32	Time since attack started in seconds.
REPORT_TIME	UINT32	Ending time stamp of this RDR. The field is in UNIX time_t format, which is the number of seconds since midnight of 1 January 1970.

Attack End RDR

The ATTACK_END_RDR is generated at the end of an attack for any attack that caused the generation of an ATTACK_START_RDR.

The RDR tag of the ATTACK_END_RDR is 0xf0f0f01a / 4042321946.

Table 2-40 lists the Attack End RDR fields and their descriptions.

Table 2-40 Attack End RDR Fields

RDR Field Name	Type	Description
SUBSCRIBER_ID	STRING	Subscriber identification string, introduced through the subscriber management interfaces. It may contain up to 64 characters. For unknown subscribers, this field may contain an empty string.
ATTACK_ID	UINT32	Unique attack ID.
ATTACKING_IP	UINT32	IP address related to the attack (for example, in a DDoS, this will be the IP address under attack; in a scan, this is the IP address of the source of the scan).
ATTACKED_IP	UINT32	Other IP address related to the attack, if one exists; otherwise, 0xFFFFFFFF.
ATTACKED_PORT	UINT16	Attacked port; 0xFFFF if not present.
ATTACKING_SIDE	INT8	Side of the SCE ATTACKING_IP on which it resides: • 0—Subscriber • 1—Network
IP_PROTOCOL	UINT8	IP protocol type.
ATTACK_TYPE	UINT32	To whom ATTACKING_IP belongs: • 0—Attacked • 1—Attacker
GENERATOR_ID	INT8	A numeric value identifying the processor generating the RDR.
ATTACK_TIME	UINT32	Time since attack started in seconds.
REPORT_TIME	UINT32	Ending time stamp of this RDR. The field is in UNIX time_t format, which is the number of seconds since midnight of 1 January 1970.

Malicious Traffic Periodic RDR

The MALICIOUS_TRAFFIC_PERIODIC_RDR is generated when an attack is detected, periodically, at user-configured intervals, for the duration of the attack, and at the end of the attack. The MALICIOUS_TRAFFIC_PERIODIC_RDR reports the details of the attack or malicious traffic.

The RDR tag of the MALICIOUS_TRAFFIC_PERIODIC_RDR is 0xf0f0f050 / 4042322000.

Table 2-41 lists the Malicious Traffic Periodic RDR fields and their descriptions.

Table 2-41 Malicious Traffic Periodic RDR Fields

RDR Field Name	Type	Description
ATTACK_ID	INT32	Unique attack ID.
SUBSCRIBER_ID	STRING	Subscriber identification string, introduced through the subscriber management interfaces. It may contain up to 64 characters. For unknown subscribers, this field may contain an empty string.
ATTACK_IP	UINT32	IP address related to this attack.
OTHER_IP	UINT32	IP address other than the one displayed in ATTACK_IP. For example, in a DDoS, this is the IP address under attack; in a scan, this is the IP address of the source of the scan. If there is no attack, 0xFFFFFFFF is displayed.
PORT_NUMBER	UINT16	Displays the attacked port. If there is no attack, 0xFFFF is displayed.
ATTACK_TYPE	UINT32	ATTACK_IP to whom it belongs: • 0—Attacked • 1—Attacker
SIDE	INT8	The IP address side: • 0—Subscriber • 1—Network
IP_PROTOCOL	UINT8	IP protocol type: • 0—Other • 1—ICMP • 6—TCP • 17—UDP
CONFIGURED_DURATION	INT32	Configured period for periodic RDRs, in seconds, between successive RDRs.
DURATION	INT32	Indicates the number of seconds that have passed since the previous MALICIOUS_TRAFFIC_RDR.
END_TIME	INT32	Ending time stamp of this RDR. The field is in UNIX time_t format, which is the number of seconds since midnight of 1 January 1970.

Table 2-41 Malicious Traffic Periodic RDR Fields (continued)

RDR Field Name	Type	Description
ATTACKS	INT8	Number of attacks in the current reporting period. Because this report is generated per attack, the value is 0 or 1.
MALICIOUS_SESSIONS	UINT32	Aggregated number of sessions for the reported attack, for the current reporting period. If the SCE platform blocks the attack, this field takes the value -1.

Note You can identify the type of attack (scan, DDoS, or DoS) from Malicious Traffic Periodic RDR data:

Scan—OTHER_IP=-1 and ATTACK_TYPE=1 (the RDR contains the source [attacker] IP address).

DDoS attack—OTHER_IP=-1 and ATTACK_TYPE=0 (the RDR contains the destination [attacked] IP address).

DoS attack—OTHER_IP contains an IP address (the RDR contains two IP addresses).

Spam RDR

The SPAM_RDR is generated when mass-mailing activity is detected.

The RDR tag of the SPAM_RDR is 4042322048.

Table 2-42 lists the Spam RDR fields and their descriptions.

Table 2-42 Spam RDR Fields

RDR Field Name	Type	Description
SUBSCRIBER_ID	STRING	Subscriber identification string, introduced through the subscriber management interfaces. It may contain up to 64 characters. For unknown subscribers, this field may contain an empty string.
PACKAGE_ID	UINT16	ID of the package assigned to the subscriber whose traffic is being reported. An assigned Package ID is an integer value between 0 and 4999. The value 4999 is reserved for unknown subscribers, and this is the maximum_number_of_packages possible.
SERVICE_ID	INT32	Service classification of the reported session. For example, in the Transaction RDR, this field indicates which service was accessed, and in the Breaching RDR, this field indicates which service was breached.
PROTOCOL_ID	INT16	Unique ID of the protocol associated with the reported session.
CLIENT_IP	UINT32	IP address of the client side of the reported session. The client side is defined as the initiator of the networking session. The IP address is in a 32-bit binary format, but the value is obtained in decimal format in RDR.
CLIENT_PORT	UINT16	Port number of the client side (initiator) of the TCP/UDP-based networking session. For non-TCP/UDP sessions, this field has the value zero.
SERVER_IP	UINT32	Destination IP address of the reported session. The destination is defined as the server or the listener of the networking session. The IP address is in a 32-bit binary format, but the value is obtained in decimal format in RDR.
SERVER_PORT	UINT16	Destination port number of the TCP/UDP-based networking session. For non-TCP/UDP sessions, this field contains the IP protocol number of the session flow.
INITIATING_SIDE	INT8	Side of the SCE platform on which the initiator of the transaction resides: • 0—Subscriber side • 1—Network side
ACCESS_STRING	STRING	Layer 7 property, extracted from the transaction.

Table 2-42 Spam RDR Fields (continued)

RDR Field Name	Type	Description
INFO_STRING	STRING	Layer 7 property, extracted from the transaction.
SPAM_FOUND	UINT8	Indicates whether spam was found (1) or stopped (0).
THRESHOLD_LEVEL	UINT16	Threshold level. Reserved for future use. Currently 0.
SESSION_COUNTER	UINT32	Number of sessions found.
TIME_INTERVAL	UINT32	Time that elapsed since the beginning of the period.
DEFINED_SESSION_ COUNTER	UINT32	Indicates the defined number of sessions.
DEFINED_TIME_INTERVAL	UINT32	Indicates the defined time interval.
REPORT_TIME	INT32	Ending time stamp of this RDR. The field is in UNIX time_t format, which is the number of seconds since midnight of 1 January 1970.
NO_OF_MSG_SMTP_ SESSION	UINT32	The number of messages found in an SMTP session. Here message represents the 'RCPT TO' commands.
TIME_INTERVAL_MSG_ COUNTER	UINT32	The time interval in which the aggregated messages (of cumulative SMTP sessions) are counted.
AGGR_MESSAGES_ COUNTER	UINT32	The number of aggregated messages found and counted cumulatively over the SMTP sessions. Here, message represents the 'RCPT TO'command.
NO_OF_FAILED_MSG_ SMTP_SESSION	UINT32	The number of failed messages found in an SMTP session. Here message represents the'RCPT TO' commands.
FAILED_MSG_SMTP_ SESSION	UINT8	The percentage of failed messages in an SMTP session.
PROTOCOL_NON_ COMPLIANCE	UINT8	Indicates whether the session is SMTP protocol compliance (0) or protocol non-compliance (1).
DEFINED_MSG_COUNTER	UINT32	Defines threshold for number of messages (cumulative count) over SMTP sessions.
DEFINED_MSG_TIME_ INTERVAL	UINT32	Defines time interval for cumulative message count over SMTP sessions.
DEFINED_NO_OF_MSG_ SMTP_SESSION	UINT32	Defines threshold for number of messages per SMTP session.
EMAIL_HARVEST_ MSGSMTP_SESSION	UINT32	The total number of messages in a session, to notify the sessions which are eligible for Anti-Harvest checking.
DEFINED_FAILED_ MSGSMTP_SESSION	UINT8	Defines the percentage of failed messages per SMTP session, to check for anti-harvest spam activity.
PROTOCOL_COMPLIANCE	UINT8	Indicates whether protocol compliance check is to be done: 0 — No protocol compliance check 1 — Perform protocol compliance check

Table 2-42 Spam RDR Fields (continued)

RDR Field Name	Type	Description
IP_TYPE	UINT8	IP flow type of the respective RDR. For example, when the flow type is IPv6, the IPv4 address of the RDR will contain the value zero. However, the IPv6 address of the RDR will contain a white space for IPv4 flow type.
CLIENTIPv6ADDRESS	STRING	IPv6 address of the client side of the reported session. The client side is defined as the initiator of the networking session.
SERVERIPv6ADDRESS	STRING	Destination IPv6 address of the reported session. The destination is defined as the server or the listener of the networking session.

Related Topics

- Universal RDR Fields, page 2-4
- Anonymized Spam RDR, page 2-142

Anonymized Spam RDR

The ANONYMIZED_SPAM_RDR is generated when mass-mailing activity is detected, without personal subscriber data.

The RDR tag of the ANONYMIZED_SPAM_RDR is 0xf0f0f54F / 4042323279.

Table 2-43 lists the Anonymized Spam RDR fields and their descriptions.

Table 2-43 Anonymized Spam RDR Fields

RDR Field Name	Type	Description
HASHED_SUBSCRIBER_ID	STRING	Subscriber identification string, introduced through the subscriber management interfaces, may be passed through hashing algorithm. It may contain up to 64 characters. For unknown subscribers, this field may contain an empty string.
PACKAGE_ID	UINT16	ID of the package assigned to the subscriber whose traffic is being reported. An assigned Package ID is an integer value between 0 and 4999. The value 4999 is reserved for unknown subscribers, and this is the maximum_number_of_packages possible.
SERVICE_ID	INT32	Service classification of the reported session. For example, in the Transaction RDR, this field indicates which service was accessed, and in the Breaching RDR, this field indicates which service was breached.
PROTOCOL_ID	INT16	Unique ID of the protocol associated with the reported session.
CLIENT_IP	UINT32	IP address of the client side of the reported session. The client side is defined as the initiator of the networking session. The IP address is in a 32-bit binary format, but the value is obtained in decimal format in RDR. If this is the subscriber IP, this field may contain the short-hash of the IP if configured.
CLIENT_PORT	UINT16	Port number of the client side (initiator) of the TCP/UDP-based networking session. For non-TCP/UDP sessions, this field has the value zero.
SERVER_IP	UINT32	Destination IP address of the reported session. The destination is defined as the server or the listener of the networking session. The IP address is in a 32-bit binary format, but the value is obtained in decimal format in RDR. If this is the subscriber IP, this field may contain the short-hash of the IP if configured.
SERVER_PORT	UINT16	Destination port number of the TCP/UDP-based networking session. For non-TCP/UDP sessions, this field contains the IP protocol number of the session flow.

Table 2-43 Anonymized Spam RDR Fields (continued)

RDR Field Name	Type	Description
INITIATING_SIDE	INT8	Side of the SCE platform on which the initiator of the transaction resides: • 0—Subscriber side • 1—Network side
ACCESS_STRING	STRING	Layer 7 property, extracted from the transaction.
INFO_STRING	STRING	Layer 7 property, extracted from the transaction.
SPAM_FOUND	UINT8	Indicates whether spam was found (1) or stopped (0).
THRESHOLD_LEVEL	UINT16	Threshold level. Reserved for future use. Currently 0.
SESSION_COUNTER	UINT32	Number of sessions found.
TIME_INTERVAL	UINT32	Time that elapsed since the beginning of the period.
DEFINED_SESSION_ COUNTER	UINT32	Indicates the defined number of sessions.
DEFINED_TIME_INTERVAL	UINT32	Indicates the defined time interval.
REPORT_TIME	INT32	Ending time stamp of this RDR. The field is in UNIX time_t format, which is the number of seconds since midnight of 1 January 1970.
NO_OF_MSG_SMTP_ SESSION	UINT32	The number of messages found in an SMTP session. Here message represents 'RCPT TO' commands.
TIME_INTERVAL_MSG_ COUNTER	UINT32	The time interval in which the aggregated messages (of cumulative SMTP sessions) are counted.
AGGR_MESSAGES_ COUNTER	UINT32	The number of aggregated messages found, counted cumulatively over SMTP sessions. Here message represents 'RCPT TO' command.
NO_OF_FAILED_MSG_ SMTP_SESSION	UINT32	The number of failed messages found in an SMTP session. Here message represents 'RCPT TO' commands.
FAILED_MSG_SMTP_ SESSION	UINT8	The percentage of failed messages in an SMTP session
PROTOCOL_NON_ COMPLIANCE	UINT8	Indicates whether the session is SMTP protocol compliance (0) or protocol non-compliance (1)
DEFINED_MSG_COUNTER	UINT32	Defines threshold for number of messages (cumulative count) over SMTP sessions
DEFINED_MSG_TIME_ INTERVAL	UINT32	Defines time interval for cumulative message count over SMTP sessions
DEFINED_NO_OF_MSG_ SMTP_SESSION	UINT32	Defines threshold for number of messages per SMTP session
EMAIL_HARVEST_ MSGSMTP_SESSION	UINT32	The total number of messages in a session, to notify the sessions which are eligible for Anti-Harvest checking
DEFINED_FAILED_ MSGSMTP_SESSION	UINT8	Defines the percentage of failed messages per SMTP session, to check for anti-harvest spam activity.

Table 2-43 Anonymized Spam RDR Fields (continued)

RDR Field Name	Type	Description
PROTOCOL_COMPLIANCE	UINT8	Indicates whether protocol compliance check is to be done: 0 – No Protocol compliance check 1 – Do Protocol compliance check
IP_TYPE	UINT8	IP flow type of the respective RDR. For example, when the flow type is IPv6, the IPv4 address of the RDR will contain the value zero. However, the IPv6 address of the RDR will contain a white space for IPv4 flow type.
CLIENTIPv6ADDRESS	STRING	IPv6 address of the client side of the reported session. The client side is defined as the initiator of the networking session. If this is the subscriber IP, this field may contain a 32-byte string hash, if configured.
SERVERIPv6ADDRESS	STRING	Destination IPv6 address of the reported session. The destination is defined as the server or the listener of the networking session. If this is the subscriber IP, this field may contain a 32-byte string hash, if configured.

Related Topics

- Universal RDR Fields, page 2-4
- Spam RDR, page 2-139

Information About RDR Enumeration Fields

The following sections list possible values for the RDR enumeration fields.:

- Block Reason (uint8), page 2-145
- String Fields, page 2-145
- Aggregation Period (uint8), page 2-147
- Flow Close Mode (uint8), page 2-147
- Time Frames (unint16), page 2-148

Block Reason (uint8)

The BLOCK_REASON field is a bit field. Table 2-44 lists the meanings of the bits of this field.

Table 2-44 Block Reason Field Bit Values

Bits Number	Value and Description
7 (msb)	Always on.
6	• 0—Action of the effective rule is block. • 1—Concurrent session limit of the effective rule was reached.
5	• 0—Effective rule was in prebreach state. • 1—Effective rule was in postbreach state.
4 to 0 (lsb)	Number of the breached bucket (1 - 16).

String Fields

Table 2-45 lists the ACCESS_STRING and INFO_STRING field values.

Table 2-45 String Field Values

Name	TR ACCESS_STRING	TR INFO_STRING	Description
PROTOCOL_TCP_ GENERIC_	Null	Null	—
PROTOCOL_UDP_ GENERIC	Null	Null	—
PROTOCOL_HTTP_ BROWSING	Host name	URL	—
PROTOCOL_FTP	Null	Null	—
PROTOCOL_RTSP	Host name	Null	—
PROTOCOL_MMS	Null	Null	—
PROTOCOL_SMTP	Server IP	Sender	—
PROTOCOL_POP3	Server name	Login name	—

Table 2-45 String Field Values (continued)

Name	TR ACCESS_STRING	TR INFO_STRING	Description
PROTOCOL_IP_ GENERIC	Null	Null	Non–TCP/UDP transaction
PROTOCOL_ GNUTELLA_ NETWORKING	Null	Null	Peer-to-peer
PROTOCOL_ GNUTELLA_FILE_ TRANSFER	Null	Null	Peer-to-peer
PROTOCOL_ FASTTRACK_ NETWORKING	Null	Null	Peer-to-peer
PROTOCOL_NNTP	Null	Group name	—
PROTOCOL_NAP_ WINMX_TRANSFER	Null	Null	Peer-to-peer
PROTOCOL_WINNY	Null	Null	Peer-to-peer
PROTOCOL_ EDONKEY	Null	Null	Peer-to-peer
PROTOCOL_ DIRECT_CONNECT	Null	Null	Peer-to-peer
PROTOCOL_ HOTLINE	Null	Null	Peer-to-peer
PROTOCOL_ DYNAMIC_ SIGNATURE	Null	Null	—
PROTOCOL_ MANOLITO	Null	Null	Peer-to-peer
PROTOCOL_SIP	SIP Method	SIP Domain	—
PROTOCOL_ BITTORRENT	Null	Null	Peer-to-peer
PROTOCOL_SKYPE	Null	Null	Peer-to-peer
PROTOCOL_VONAGE	SIP Method	SIP Subscriber ID	
PROTOCOL_SHARE	Null	Null	Peer-to-peer
PROTOCOL_H323	Null	Is Fast Start	
PROTOCOL_ SOULSEEK	Null	Null	Peer-to-peer
PROTOCOL_ITUNES	Null	Null	Peer-to-peer
PROTOCOL_ FILETOPIA	Null	Null	Peer-to-peer
PROTOCOL_ NAPSTER	Null	Null	Peer-to-peer
PROTOCOL_DHCP	Null	Null	—

Table 2-45 String Field Values (continued)

Name	TR ACCESS_STRING	TR INFO_STRING	Description
PROTOCOL_MUTE	Null	Null	Peer-to-peer
PROTOCOL_ NODEZILLA	Null	Null	Peer-to-peer
PROTOCOL_WASTE	Null	Null	Peer-to-peer
PROTOCOL_NEONET	Null	Null	Peer-to-peer
PROTOCOL_MGCP	Null	Null	—
PROTOCOL_WAREZ	Null	Null	Peer-to-peer

Aggregation Period (uint8)

Table 2-46 lists the AGG_PERIOD field values.

Table 2-46 AGG_PERIOD Field Values

Name	Value	Description
AGGREGATE_HOURLY	0	Hourly aggregate—Every hour, on the hour.
AGGREGATE_DAILY	1	Daily aggregate—Every day at midnight.
AGGREGATE_WEEKLY	2	Deprecated in 3.0.
AGGREGATE_MONTHLY	3	Deprecated in 3.0.
EXTERNAL_QUOTA_ PROVISION	4	Third-party source that provisions and manages the quota externally.

Flow Close Mode (uint8)

Table 2-47 lists the FLOW_CLOSE_MODE field values.

Table 2-47 Flow Close Mode Field Values

Name	Value	Description
TCP_NORMAL_CLOSE	0	SCE observed a normal termination of the TCP connection.
FLOW_CLOSED_BY_ SYSTEM	2	SCE concluded that the connection has terminated after a period of inactivity.

Time Frames (unint16)

Table 2-48 lists the TIME_FRAME field values.

Table 2-48 Time Frame Field Values

Name	Value	Description
TIME_FRAME_0 through TIME_FRAME_3	0–3	ID of active time frame. A number from 0 to 3 that indicates the time frame internal index.

RDR Tag Assignment Summary

Table 2-49 summarizes RDR tag assignments.

Table 2-49 RDR Tag Assignments

RDR Name	Default Category (see Table 2-50)	Tag Value (decimal)	Tag Value (hex)
SUBSCRIBER USAGE RDR (NUR)	CM-DB (1)	4,042,321,920	F0 F0 F0 00
REALTIME SUBSCRIBER USAGE RDR (SUR)	CM-DB (1)	4,042,321,922	F0 F0 F0 02
PACKAGE USAGE RDR	CM-DB (1)	4,042,321,924	F0 F0 F0 04
LINK USAGE RDR	CM-DB (1)	4,042,321,925	F0 F0 F0 05
ZONE USAGE RDR	CM-DB (1)	4,042,321,928	F0 F0 F0 08
VIRTUAL LINK RDR	CM-DB (1)	4,042,321,926	F0 F0 F0 06
TRANSACTION RDR	CM-DB (1)	4,042,321,936	F0 F0 F0 10
TRANSACTION USAGE RDR	CM-CSV (1)	4,042,323,000	F0 F0 F4 38
HTTP TRANSACTION USAGE RDR	CM-CSV (1)	4,042,323,004	F0 F0 F4 3C
RTSP TRANSACTION USAGE RDR	CM-CSV (1)	4,042,323,008	F0 F0 F4 40
VOIP TRANSACTION USAGE RDR	CM-CSV (1)	4,042,323,050	F0 F0 F4 6A
VIDEO TRANSACTION USAGE RDR	CM-CSV (1)	4,042,323,072	F0 F0 F4 80
BLOCKING RDR	CM-CSV (1)	4,042,321,984	F0 F0 F0 40
QUOTA BREACH RDR	QP (4)	4,042,322,034	F0 F0 F0 72
QUOTA STATUS RDR	QP (4)	4,042,322,033	F0 F0 F0 71
QUOTA THRESHOLD RDR	QP (4)	4,042,322,035	F0 F0 F0 73
SESSION CREATION RDR	QP (4)	4,042,322,032	F0 F0 F0 70
RADIUS RDR	SM (3)	4,042,321,987	F0 F0 F0 43
DHCP RDR	SM (3)	4,042,321,986	F0 F0 F0 42
DHCPv6 RDR	SM (3)	4,042,321,988	F0 F0 F0 44
FLOW START RDR	RT (2)	4,042,321,942	F0 F0 F0 16
FLOW END RDR	RT (2)	4,042,321,944	F0 F0 F0 18
MEDIA FLOW RDR	CM-DB (1)	4,042,323,052	F0 F0 F4 6C

Table 2-49 RDR Tag Assignments (continued)

RDR Name	Default Category (see Table 2-50)	Tag Value (decimal)	Tag Value (hex)
FLOW ONGOING RDR	RT (2)	4,042,321,943	F0 F0 F0 17
ATTACK START RDR	RT (2)	4,042,321,945	F0 F0 F0 19
ATTACK END RDR	RT (2)	4,042,321,946	F0 F0 F0 1A
MALICIOUS TRAFFIC RDR	DC-DB (1)	4,042,322,000	F0 F0 F0 50
GENERIC USAGE RDR	CM-DB (1)	4,042,322,064	F0 F0 F0 90
SPAM RDR	CM-DB (1)	4,042,322,048	F0 F0 F0 80
ANONYMIZED HTTP TRANSACTION USAGE RDR	CM-CSV (1)	4,042,323,260	F0 F0 F5 3C
ANONYMIZED TRANSACTION RDR	CM-CSV (1)	4,042,323,264	F0 F0 F5 40
ANONYMIZED VIDEO TRANSACTION USAGE RDR	CM-CSV (1)	4,042,323,265	F0 F0 F5 41
ANONYMIZED RTSP TRANSACTION USAGE RDR	CM-CSV (1)	4,042,323,266	F0 F0 F5 42
ANONYMIZED BLOCKING RDR	CM-CSV (1)	4,042,323,267	F0 F0 F5 43
ANONYMIZED VOIP TRANSACTION USAGE RDR	CM-CSV (1)	4,042,323,268	F0 F0 F5 44
ANONYMIZED TRANSACTION USAGE RDR	CM-CSV (1)	4,042,323,270	F0 F0 F5 46
ANONYMIZED FLOW START RDR	CM-CSV (1)	4,042,323,273	F0 F0 F5 49
ANONYMIZED FLOW END RDR	CM-CSV (1)	4,042,323,274	F0 F0 F5 4A
ANONYMIZED FLOW ONGOING RDR	CM-CSV (1)	4,042,323,275	F0 F0 F5 4B
ANONYMIZED MEDIA FLOW RDR	CM-CSV (1)	4,042,323,276	F0 F0 F5 4C
ANONYMIZED SPAM RDR	CM-CSV (1)	4,042,323,279	F0 F0 F5 4F

RDR categories are the mechanism by which different types of RDRs can be sent to different collectors. You can configure the RDR categories by using the SCE CLI. For more information, see the following relevant document:

- "Raw Data Formatting: The RDR Formatter and NetFlow Exporting" chapter of *Cisco SCE 2000 and SCE 1000 Software Configuration Guide*.
- "Raw Data Formatting: The RDR Formatter and NetFlow Exporting" chapter of *Cisco SCE 8000 10GBE Software Configuration Guide*.
- "Raw Data Formatting: The RDR Formatter and NetFlow Exporting" chapter of *Cisco SCE 8000 GBE Software Configuration Guide*.

Table 2-50 summarizes the RDR tag default categories.

Table 2-50 RDR Tag Default Categories

Default Category	Intended Destination and Use
CM-DB (1)	CM database. Used by Cisco Insight to generate reports.
CM-CSV (1)	CM. Stored as CSV files.
RT (2)	Other network devices. Typically, used for functionality that requires a real-time response, such as QoS, provisioning, and deletion.
SM (3)	DHCP and RADIUS LEGs of the SM.
QP (4)	External quota provisioning systems. Used as notifications of the SCE Subscribers API.

Periodic RDR Zero Adjustment Mechanism

The Periodic RDRs (or Network Usage RDRs) include the Link Usage, Package Usage, and Real-Time Subscriber Usage RDRs. When there is traffic for a particular service or package, the appropriate Usage RDRs are generated periodically, according to user-configured intervals. The RDR includes a time stamp of the end of the interval during which the traffic was recorded.

When there is *no* traffic (and therefore no consumed resources) for a particular service or package during a given period, the Cisco SCA BB application uses the Periodic RDR Zero Adjustment Mechanism, also called the zeroing methodology. This methodology is used to reduce the number of Usage RDRs generated for that service or package. This technique also simplifies collection for external systems by reducing the number of RDRs that they need to handle.

Note Unlike other Usage RDRs, the generation logic for Subscriber Usage RDRs does not use the zeroing methodology.

The zeroing methodology algorithm works as follows: for any number of consecutive time intervals having no traffic for a particular service or package, zero-consumption RDRs are generated for the first and last zero-consumption time intervals, but not for the intermediate time intervals. These two zero-consumption RDRs are generated when the next traffic arrives.

Example 1

The Real-Time Subscriber Usage RDR (for a given subscriber) has a generation period of 30 minutes. There is subscriber traffic during the interval 1200–1230, no subscriber traffic during the following five intervals (1230–1300, 1300–1330, 1330–1400, 1400–1430, and 1430–1500), and the next subscriber traffic occurs at 1522. The following Real-Time Subscriber Usage RDRs are generated:

- At 1230, one RDR with the values of the consumed resources for the interval 1200–1230, and with the time stamp 1230.
- At 1522, one zero-consumption RDR having the time stamp (1300) of the end of the first interval (1230–1300), and with no traffic for that subscriber.
- At 1522, one zero-consumption RDR having the time stamp (1500) of the end of the last interval (1430–1500), and with no traffic for that subscriber.

  No RDR is generated for the three intermediate zero-consumption intervals (1300–1330, 1330–1400, and 1400–1430).
- At 1530, one RDR with the values of the consumed resources for the interval 1500–1530, and with the time stamp 1530.

Example 2

The Real-Time Subscriber Usage RDR (for a given subscriber) has a generation period of 30 minutes. There is subscriber traffic during the interval 1200–1230, no subscriber traffic during the following interval 1230–1300, and the next subscriber traffic occurs at 1322. The following Real-Time Subscriber Usage RDRs are generated:

- At 1230, one RDR with the values of the consumed resources for the interval 1200–1230, and with the time stamp 1230.
- At 1322, one zero-consumption RDR having the time stamp (1300) of the single interval (1230–1300), and with no traffic for that subscriber.
- At 1330, one RDR with the values of the consumed resources for the interval 1300–1330, and with the time stamp 1330.

NetFlow Records: Formats and Field Contents

Published: December 23, 2013

Introduction

This chapter describes the fields that may be contained in a NetFlow record.

NetFlow records can be generated for the data contained in the following RDRs:

- Using the Generic Usage RDR to Report IPv6 Usage, page 2-63 (NUR)
- Package Usage RDR, page 2-77 (PUR)
- Link Usage RDR, page 2-71 (LUR)
- NetFlow, page 3-1
- NetFlow Field Types, page 3-2
- NetFlow Ports, page 3-6

NetFlow

The Cisco SCA BB supports NetFlow v9. For more information about NetFlow, see RFC 3954.

NetFlow Field Types

Table 3-1 lists the possible fields in a NetFlow record and their descriptions.

Table 3-1 NetFlow Fields

Field Type	Value	Length (Bytes)	Description
scTag	32769	4	—
scTrafficProcessorId	32770	1	—
scSourceIpSample	32771	1	—
scDestinationIpSampl	32772	1	—
scFlowContextId	32773	4	—
scSubscriberId	32774	64	Subscriber identification string, introduced through the subscriber management interfaces. For an unknown subscriber, this field may contain an empty string. The string is padded with zeros.
scPackageId	32775	4	ID of the service configuration package/profile assigned to the subscriber.
scServiceId	32776	4	Service classification of the reported session.
scProtocolId	32777	2	Unique ID of the protocol associated with the reported session. The PROTOCOL_ID is the Generic IP / Generic TCP / Generic UDP protocol ID value, according to the specific transport protocol of the transaction, unless a more specific protocol definition (such as a signature-based or a port-based protocol) that matches the reported session is assigned to a service.
scSkipppedSessions	32778	4	Number of unreported sessions since the previous reporting record of this kind.
scInitiatingSide	32779	1	Initiating side of the transaction: • 0—Subscriber side • 1—Network side
scReportTime	32780	4	Ending time stamp of this reporting record. The field is in UNIX time_t format, which is the number of seconds since midnight of 1 January 1970.
scTransaction DurationMillisec	32781	4	Duration, in milliseconds, of the transaction reported in this reporting record.

Table 3-1 NetFlow Fields (continued)

Field Type	Value	Length (Bytes)	Description
scTimeFrame	32782	1	Which of the four possible time frames was used for the period during which the reporting record was generated. The field takes a value in the range 0 - 3.
scSessionUpstream Volume	32783	4	Upstream volume of the transaction, in bytes. The volume refers to the aggregated upstream volume on both links of all the flows bundled in the transaction.
scSessionDownstream Volume	32784	4	Downstream volume of the transaction, in bytes. The volume refers to the aggregated downstream volume on both links of all the flows bundled in the transaction.
scProtocolSignature	32785	4	ID of the protocol signature associated with this session.
scZoneId	32786	4	ID of the zone associated with this session.
scFlavorId	32787	4	ID of the protocol signatures with flavor associated with this session.
scFlowCloseMode	32788	1	Reason for the end of the flow.
scAccessString	32789	128, 256, 512, 1024	Layer 7 property, extracted from the transaction.
scInfoString	32790	128, 256, 512, 1024	Layer 7 property, extracted from the transaction.
scClientPort	32791	2	—
scServerPort	32792	2	—
scSubscriberCounterId	32793	2	—
scServiceUsageCounter Id	32794	2	—
scBreachState	32795	1	Indicates whether the quota allocated to the subscriber was breached: • 0—Quota was not breached • 1—Quota was breached
scReason	32796	1	The reason that the reporting record was generated: • 0—Periodic record • 1—Subscriber logout • 2—Package switch • 3—Wraparound • 4—End of aggregation period

Table 3-1 NetFlow Fields (continued)

Field Type	Value	Length (Bytes)	Description
scConfiguredDuration	32797	4	Configured period, in seconds, between successive reporting records.
scDuration	32798	4	Number of seconds that have passed since the previous reporting record of this type.
scEndTime	32799	4	Ending time stamp of this reporting record. The field is in UNIX time_t format, which is the number of seconds since midnight of 1 January 1970.
scUpstreamVolume	32800	4	Aggregated upstream volume on both links of all sessions, in kilobytes, for the current reporting period.
scDownstreamVolume	32801	4	Aggregated downstream volume on both links of all sessions, in kilobytes, for the current reporting period.
scSessions	32802	4	Aggregated number of sessions for the reported service, for the current reporting period.
scSeconds	32803	4	Aggregated number of session seconds for the reported service, for the current reporting period.
scPackageCounterId	32804	2	Counter to which each service is mapped. There are 64 package usage counters.
scGeneratorId	32805	1	Numeric value identifying the processor generating the reporting record.
scServiceGlobal CounterId	32806	2	Counter to which each service is mapped. There are 128 global usage counters.
scConcurrentSessions	32807	4	Concurrent number of sessions using the reported service when this reporting record was generated.
scActiveSubscribers	32808	4	Concurrent number of subscribers using the reported service when this reporting record was generated.
scTotalActive Subscribers	32809	4	Concurrent number of subscribers in the system when this reporting record was generated.
scLinkId	32810	1	Numeric value associated with the reported network link: • 0—Physical link 1 • 1—Physical link 2
—	32811-32818	Reserved.	—
scAttackId	32819	4	Unique attack ID.
scAttackIp	32820	4	IP address related to this attack.

Table 3-1 NetFlow Fields (continued)

Field Type	Value	Length (Bytes)	Description
scAttackOtherIp	32821	4	Other IP address related to this attack if it exists; otherwise -1.
scAttackPortNumber	32822	2	Port number related to this attack if one exists (for example, IP scan); otherwise -1.
scAttackType	32823	4	Whom the AttackIp belongs to: • 0—Attacked • 1—Attacker
scAttackSide	32824	1	IP address side: • 0—Subscriber • 1—Network
scAttackIpProtoco	32825	1	IP protocol type: • 0—Other • 1—ICMP • 6—TCP • 17—UDP
scAttacks	32826	1	Number of attacks in the current reporting period. Because attack reports are generated per attack, the value is 0 or 1.
scAttackMalicious Sessions	32827	4	Aggregated number of sessions for the reported attack, for the current reporting period. If the SCE platform blocks the attack, this field takes the value –1.

NetFlow Ports

Table 3-2 provide details of ports used for NetFlow. The Collection Manager listens to this port constantly.

Table 3-2 NetFlow Ports

Port	Description
33002	Internal Cisco Collection Manager for Flexible NetFlow.
2055	UDP port used by ASR 1000 to send Flexible NetFlow records for data collection.
9093	HTTP technician interface for Flexible NetFlow.
14376	PRPC.

Database Tables: Formats and Field Contents

Published: December 23, 2013

Introduction

Each RDR is sent to the Cisco SCMS Collection Manager. On the Collection Manager, adapters convert the RDRs and store them in database tables. There is a separate table for each RDR type. This chapter presents these tables and their columns (field names and types).

For additional information, such as RDR structure, RDR column, and field descriptions, and how the RDRs are generated, see the "Raw Data Records: Formats and Field Contents" section on page 2-1.

- Database Tables Overview, page 4-2
- Table RPT_NUR, page 4-3
- Table RPT_SUR, page 4-3
- Table RPT_PUR, page 4-5
- Table RPT_LUR, page 4-6
- Table RPT_GUR, page 4-7
- Table RPT_TR, page 4-9
- Table RPT_OSFP, page 4-10
- Table OSFP_TYPES, page 4-10
- Table RPT_MEDIA, page 4-11
- Table RPT_MALUR, page 4-12
- Table RPT_TOPS_PERIOD0, page 4-13
- Table RPT_TOPS_PERIOD1, page 4-14
- Table RPT_TOPS_PERIOD0_CUMULATIVE, page 4-15
- Table RPT_TOPS_PERIOD1_CUMULATIVE, page 4-16
- Table RPT_TOPS_PEAK_PERIOD, page 4-17
- Table RPT_TOPS_PEAK_CUMULATIVE, page 4-18
- Table RPT_VLUR, page 4-19
- Table INI_VALUES, page 4-20
- Table VLINK_INI, page 4-23

- Table CONF_SE_TZ_OFFSET, page 4-23
- Table RPT_TOP_APN, page 4-24
- Table RPT_TOP_DEVICE_TYPE, page 4-24
- Table RPT_TOP_NETWORK_TYPE, page 4-25
- Table RPT_TOP_SGSN, page 4-25
- Table RPT_TOP_USER_LOCATION, page 4-26
- Table RPT_DVLINK, page 4-27
- Table RPT_UVLINK, page 4-28
- Table RPT_TOP_HTTP_DOMAINS, page 4-29
- Table RPT_TOP_HTTP_HOSTS, page 4-30
- Table RPT_TOP_VIDEO_DOMAINS, page 4-31
- Table RPT_TOP_VIDEO_HOSTS, page 4-32
- Table RPT_ZUR, page 4-33
- Table RPT_SPAM, page 4-34
- Table RPT_FUR, page 4-35
- Table IMEI_DEVICETYPE, page 4-36

Database Tables Overview

Each RDR is routed to the appropriate adapter—the Java Database Connectivity (JDBC), Topper/Aggregator (TA), or Real-Time Aggregating (RAG) adapter—converted, and written into a database table row. There is a separate table for each RDR type, with a column designated for each RDR field.

In addition to the RDR fields that are specific to each RDR type, the RPT_NUR, RPT_SUR, RPT_PUR, RPT_LUR, and RPT_TR tables contain two universal columns TIME_STAMP and RECORD_SOURCE. The following values are placed in these two universal columns (field numbers 1 and 2, respectively):

- TIME_STAMP—The RDR time stamp assigned by the SCMS Collection Manager. The field is in UNIX time_t format, which is the number of seconds since midnight of 1 January 1970.
- RECORD_SOURCE—Contains the IP address of the Cisco SCE platform that generated the RDR.

  The IP address is in 32-bit binary format (displayed as a 4-byte integer).

Table RPT_NUR

Database table RPT_NUR stores data from SUBSCRIBER_USAGE_RDRs.

Note This table is not part of the default configuration.

These RDRs have the tag 4042321920.

Table 4-1 list the columns of Table RPT_NUR.

Table 4-1 Columns of Table RPT_NUR

Field Name	Type
TIME_STAMP	Date_Time
RECORD_SOURCE	Number
SUBSCRIBER_ID	String
PACKAGE_ID	Number
SUBS_USG_CNT_ID	Number
BREACH_STATE	Number
REASON	Number
CONFIGURED_DURATION	Number
DURATION	Number
END_TIME	Number
UPSTREAM_VOLUME	Number
DOWNSTREAM_VOLUME	Number
SESSIONS	Number
SECONDS	Number
UP_VLINK_ID	Number
DOWN_VLINK_ID	Number
OS_FINGER_PRINTING	String
IP_TYPE	Number

Table RPT_SUR

Database table RPT_SUR stores data from REALTIME_SUBSCRIBER_USAGE_RDRs.

These RDRs have the tag 4042321922.

Table 4-2 list the columns of Table RPT_SUR.

Table 4-2 Columns of Table RPT_SUR

Field Name	Type
TIME_STAMP	Date_Time
RECORD_SOURCE	Number
SUBSCRIBER_ID	String
PACKAGE_ID	Number
SUBS_USG_CNT_ID	Number
MONITORED_OBJECT_ID	Number
BREACH_STATE	Number
REASON	Number
CONFIGURED_DURATION	Number
DURATION	Number
END_TIME	Number
UPSTREAM_VOLUME	Number
DOWNSTREAM_VOLUME	Number
SESSIONS	Number
SECONDS	Number
OS_FINGER_PRINTING	String
IP_TYPE	Number

Table RPT_PUR

Database table RPT_PUR stores data from PACKAGE_USAGE_RDRs.

These RDRs have the tag 4042321924.

Table 4-3 list the columns of Table RPT_PUR.

Table 4-3 Columns of Table RPT_PUR

Field Name	Type
TIME_STAMP	Date_Time
RECORD_SOURCE	Number
PKG_USG_CNT_ID	Number
GENERATOR_ID	Number
GLBL_USG_CNT_ID	Number
CONFIGURED_DURATION	Number
DURATION	Number
END_TIME	Number
UPSTREAM_VOLUME	Number
DOWNSTREAM_VOLUME	Number
SESSIONS	Number
SECONDS	Number
CONCURRENT_SESSIONS	Number
ACTIVE_SUBSCRIBERS	Number
TOTAL_ACTIVE_SUBSCRIBERS	Number
IP_TYPE	Number

Table RPT_LUR

Database table RPT_LUR stores data from LINK_USAGE_RDRs.

These RDRs have the tag 4042321925.

Table 4-4 list the columns of Table RPT_LUR.

Table 4-4 Columns of Table RPT_LUR

Field Name	Type
TIME_STAMP	Date_Time
RECORD_SOURCE	Number
LINK_ID	Number
GENERATOR_ID	Number
GLBL_USG_CNT_ID	Number
CONFIGURED_DURATION	Number
DURATION	Number
END_TIME	Number
UPSTREAM_VOLUME	Number
DOWNSTREAM_VOLUME	Number
SESSIONS	Number
SECONDS	Number
CONCURRENT_SESSIONS	Number
ACTIVE_SUBSCRIBERS	Number
TOTAL_ACTIVE_SUBSCRIBERS	Number
IP_TYPE	Number

Table RPT_GUR

Database table RPT_GUR stores data from GENERIC USAGE_RDRs.

These RDRs have the tag 4042322064.

Table 4-5 list the columns of Table RPT_GUR.

Table 4-5 Columns of Table RPT_GUR

Field Name	Type
TIME_STAMP	Date_Time
RECORD_SOURCE	Number
GUR_TYPE	Number
LINK_ID	Number
GENERATOR_ID	Number
GLBL_USG_CNT_ID	Number
SUBS_USG_CNT_ID	Number
PKG_USG_CNT_ID	Number
SERVICE_ID	Number
SUBSCRIBER_ID	String
PACKAGE_ID	Number
PROTOCOL_ID	Number
SIGNATURE_ID	Number
PEER_IP	Number
PEER_PORT	Number
SOURCE_IP	Number
SOURCE_PORT	Number
INITIATING_SIDE	Number
ZONE_ID	Number
FLAVOR_ID	Number
SESSION_ID	Number
START_TIME	Number
END_TIME	Number
ACCESS_STRING	String
INFO_STRING	String
INT_KEY0	Number
INT_KEY1	Number
INT_KEY2	Number
INT_KEY3	Number
STR_KEY0	String
STR_KEY1	String

Table 4-5 Columns of Table RPT_GUR (continued)

Field Name	Type
UPSTREAM_VOLUME	Number
DOWNSTREAM_VOLUME	Number
TOTAL_VOLUME	Number
SESSIONS	Number
SECONDS	Number
CONCURRENT_SESSIONS	Number
ACTIVE_SUBSCRIBERS	Number
TOTAL_ACTIVE_SUBSCRIBERS	Number
CONFIGURED_DURATION	Number
DURATION	Number
DATA0	Number
DATA1	Number
DATA2	Number
DATA3	Number

Table RPT_TR

Database table RPT_TR stores data from TRANSACTION_RDRs.

These RDRs have the tag 4042321936.

Table 4-6 list the columns of Table RPT_TR.

Table 4-6 Columns of Table RPT_TR

Field Name	Type
TIME_STAMP	Date_Time
RECORD_SOURCE	Number
SUBSCRIBER_ID	String
PACKAGE_ID	Number
SERVICE_ID	Number
PROTOCOL_ID	Number
SAMPLE_SIZE	Number
PEER_IP	Number
PEER_PORT	Number
ACCESS_String	String
INFO_String	String
SOURCE_IP	Number
SOURCE_PORT	Number
INITIATING_SIDE	Number
END_TIME	Number
MILISEC_DURATION	Number
TIME_FRAME	Number
UPSTREAM_VOLUME	Number
DOWNSTREAM_VOLUME	Number
SUBS_CNT_ID	Number
GLBL_CNT_ID	Number
GLBL_CNT_ID	Number
IP_PROTOCOL	Number
PROTOCOL_SIGNATURE	Number
ZONE_ID	Number
FLAVOR_ID	Number
FLOW_CLOSE_MODE	Number
IP_TYPE	Number
PEER_IP_V6	String
SOURCE_IP_V6	String

Table RPT_OSFP

Database Table RPT_OSFP stores the operating system usage information for each subscriber.

Table 4-7 Columns of Table RPT_OSFP

Field Name	Type
TIME_STAMP	Date_Time
RECORD_SOURCE	Number
SUBSCRIBER_ID	String
OSFP_ID	Number
NAT_ENV	Number

Table OSFP_TYPES

Database Table OSFP_TYPES stores the operating system mapping information.

Table 4-8 Columns of Table OSFP_Types

Field Name	Type
TIME_STAMP	Date_Time
OSFP_ID	Number
OSFP_DESC	String

Table RPT_MEDIA

Database table RPT_MEDIA stores data from MEDIA_FLOW_RDRs.

These RDRs have the tag 4042323052.

Table 4-9 list the columns of Table RPT_MEDIA.

Table 4-9 Columns of Table RPT_MEDIA

Field Name	Type
TIME_STAMP	Date_Time
RECORD_SOURCE	Number
SUBSCRIBER_ID	String
PACKAGE_ID	Number
SERVICE_ID	Number
PROTOCOL_ID	Number
PEER_IP	Number
PEER_PORT	Number
SOURCE_IP	Number
SOURCE_PORT	Number
INITIATING_SIDE	Number
ZONE_ID	Number
FLAVOR_ID	Number
SIP_DOMAIN	String
SIP_USER_AGENT	String
MGCP_DOMAIN	String
MGCP_USER_AGENT	String
START_TIME	Number
END_TIME	Number
SEC_DURATION	Number
UPSTREAM_VOLUME	Number
DOWNSTREAM_VOLUME	Number
IP_PROTOCOL	Number
FLOW_TYPE	Number
SESSION_ID	Number
UPSTREAM_AVERAGE_JITTER	Number
DOWNSTREAM_AVERAGE_JITTER	Number
UPSTREAM_PACKET_LOSS	Number
DOWNSTREAM_PACKET_LOSS	Number
UPSTREAM_PAYLOAD_TYPE	Number
DOWNSTREAM_PAYLOAD_TYPE	Number

Table RPT_MALUR

Database table RPT_MALUR stores data from MALICIOUS_TRAFFIC_PERIODIC_RDRs.

These RDRs have the tag 4042322000.

Table 4-10 list the columns of Table RPT_MALUR.

Table 4-10 Columns of Table RPT_MALUR

Field Name	Type
TIME_STAMP	Date_Time
RECORD_SOURCE	Number
ATTACK_ID	Number
SUBSCRIBER_ID	String
ATTACK_IP	Number
OTHER_IP	Number
PORT_NUMBER	Number
ATTACK_TYPE	Number
SIDE	Number
IP_PROTOCOL	Number
CONFIGURED_DURATION	Number
DURATION	Number
END_TIME	Number
ATTACKS	Number
MALICIOUS_SESSIONS	Number

Table RPT_TOPS_PERIOD0

The TA adapter generates database table RPT_TOPS_PERIOD0 for its shorter aggregation interval (by default, one hour).

Table 4-11 list the columns of Table RPT_TOPS_PERIOD0.

Table 4-11 Columns of Table RPT_TOPS_PERIOD0

Field Name	Type
RECORD_SOURCE	Number
METRIC_ID	Number
SUBS_USG_CNT_ID	Number
TIME_STAMP	Date_Time
AGG_PERIOD	Number
SUBSCRIBER_ID	String
CONSUMPTION	Number
PACKAGE_ID	Number

For each Top Report, the TA adapter sorts the subscriber/consumption pairs from the highest consumption to lowest. At the end of each report is a statistic giving the sum of all subscribers for this metric.

If the report is empty, typically when no traffic is reported for the designated service/metric pair during the aggregation period, the database is updated, but only the final row in the report is updated to show a total consumption of zero.

Table 4-12 list the possible values for the METRIC_ID field.

Table 4-12 Metric_ID Values

Metric_ID	Metric
0	Up Volume
1	Down Volume
2	Combined Volume
3	Sessions
4	Seconds

Table RPT_TOPS_PERIOD1

The TA adapter generates database table RPT_TOPS_PERIOD1 for its longer aggregation interval (by default, 24 hour).

Table 4-13 list the columns of Table RPT_TOPS_PERIOD1.

Table 4-13 Columns of Table RPT_TOPS_PERIOD1

Field Name	Type
RECORD_SOURCE	Number
METRIC_ID	Number
SUBS_USG_CNT_ID	Number
TIME_STAMP	Date_Time
AGG_PERIOD	Number
SUBSCRIBER_ID	String
CONSUMPTION	Number
PACKAGE_ID	Number

For each Top Report, the TA adapter sorts the subscriber/consumption pairs from the highest consumption to lowest. At the end of each report is a statistic giving the sum of all subscribers for this metric.

If the report is empty, typically when no traffic was reported for the designated service/metric pair during the aggregation period, the database is still updated, but the only row in the report is the final row showing a total consumption of zero.

Table 4-14 lists the possible values for the METRIC_ID field.

Table 4-14 Metric_ID Values

Metric_ID	Metric
0	Up Volume
1	Down Volume
2	Combined Volume
3	Sessions
4	Seconds

Table RPT_TOPS_PERIOD0_CUMULATIVE

The TA adapter generates database table RPT_TOPS_PERIOD0_CUMULATIVE for its shorter aggregation interval (by default, one hour).

Table 4-15 list the columns of Table RPT_TOPS_PERIOD0_CUMULATIVE.

Table 4-15 Columns of Table RPT_TOPS_PERIOD0_CUMULATIVE

Field Name	Type
RECORD_SOURCE	Number
METRIC_ID	Number
SUBS_USG_CNT_ID	Number
TIME_STAMP	Date_Time
AGG_PERIOD	Number
SUBSCRIBERS	Number
CONSUMPTION	Number
TOTAL_SUBSCRIBERS	Number
TOTAL_CONSUMPTION	Number
LAST_SUBS_CONSUMPTION	Number
PACKAGE_ID	Number

Table 4-16 list the possible values for the METRIC_ID field.

Table 4-16 Metric_ID Values

Metric_ID	Metric
0	Up Volume
1	Down Volume

Table RPT_TOPS_PERIOD1_CUMULATIVE

The TA adapter generates database table RPT_TOPS_PERIOD1_CUMULATIVE for its longer aggregation interval (by default, one day).

Table 4-17 list the columns of Table RPT_TOPS_PERIOD1_CUMULATIVE.

Table 4-17 Columns of Table RPT_TOPS_PERIOD1_CUMULATIVE

Field Name	Type
RECORD_SOURCE	Number
METRIC_ID	Number
SUBS_USG_CNT_ID	Number
TIME_STAMP	Date_Time
AGG_PERIOD	Number
SUBSCRIBERS	Number
CONSUMPTION	Number
TOTAL_SUBSCRIBERS	Number
TOTAL_CONSUMPTION	Number
LAST_SUBS_CONSUMPTION	Number
PACKAGE_ID	Number

Table 4-18 lists the possible values for the METRIC_ID field.

Table 4-18 Metric_ID Values

Metric_ID	Metric
0	Up Volume
1	Down Volume

Table RPT_TOPS_PEAK_PERIOD

The TA adapter generates database table RPT_TOPS_PEAK_PERIOD for the configured period in the peak_hours section in taadapter.conf.

Table 4-19 lists the columns of the RPT_TOPS_PEAK_PERIOD table.

Table 4-19 Columns of Table RPT_TOPS_PEAK_PERIOD

Field Name	Type
RECORD_SOURCE	Number
METRIC_ID	Number
SUBS_USG_CNT_ID	Number
TIME_STAMP	Date_Time
AGG_PERIOD	Number
SUBSCRIBER_ID	String
CONSUMPTION	Number
PACKAGE_ID	Number

Table 4-20 lists the possible values for the METRIC_ID field.

Table 4-20 Metric_ID Values

Metric_ID	Metric
0	Up Volume
1	Down Volume

Table RPT_TOPS_PEAK_CUMULATIVE

The TA adapter generates database table RPT_TOPS_PEAK_CUMULATIVE for the configured period in the peak_hours section in taadapter.conf.

Table 4-21 lists the columns of the RPT_TOPS_PEAK_CUMULATIVE table.

Table 4-21 Columns of Table RPT_TOPS_PEAK_CUMULATIVE

Field Name	Type
RECORD_SOURCE	Number
METRIC_ID	Number
SUBS_USG_CNT_ID	Number
TIME_STAMP	Date_Time
AGG_PERIOD	Number
SUBSCRIBERS	Number
CONSUMPTION	Number
TOTAL_SUBSCRIBERS	Number
TOTAL_CONSUMPTION	Number
LAST_SUBS_CONSUMPTION	Number
PACKAGE_ID	Number

Table 4-22 lists the possible values for the METRIC_ID field.

Table 4-22 METRIC_ID Values

Metric_ID	Metric
0	Up Volume
1	Down Volume

Table RPT_VLUR

Database table RPT_VLUR stores data from VIRTUAL_LINKS_USAGE_RDRs.

These RDRs have the tag 4042321926.

Table 4-23 lists the columns of the RPT_VLUR table.

Table 4-23 Columns of Table RPT_VLUR

Name	Type
TIME_STAMP	Date_Time
RECORD_SOURCE	Number
VLINK_ID	Number
VLINK_DIRECTION	Number
GENERATOR_ID	Number
SRVC_USG_CNT_ID	Number
CONFIGURED_DURATION	Number
DURATION	Number
END_TIME	Number
UPSTREAM_VOLUME	Number
DOWNSTREAM_VOLUME	Number
SESSIONS	Number
SECONDS	Number
CONCURRENT_SESSIONS	Number
ACTIVE_SUBSCRIBERS	Number
TOTAL_ACTIVE_SUBSCRIBERS	Number

Table INI_VALUES

Database table INI_VALUES is updated whenever the service configuration is applied to the SCE platform. This table contains, for each SCE IP address, mappings between numeric identifiers and textual representation for services, packages, and other service configuration components. The mapping is represented as a standard properties file in string form, where each mapping file is stored in one row. Cisco Insight uses the mappings contained in this table.

Table 4-24 lists the columns of the INI_VALUES table.

Table 4-24 Columns of Table INI_VALUES

Field Name	Type	Description
TIME_STAMP	Date_Time	—
SE_IP	String	Identification of the SCE platform where these values were applied.
VALUE_TYPE	Number	Key/Value family type.
VALUE_KEY	String	Key name. For example, Gold, Silver, or Adult Browsing.
VALUE	Number	Numeric reference.

Possible values for VALUE_TYPE field are:

- 1—Service ID/service name
- 2—Package ID/package name
- 3—TCP port number/port name
- 4—Time frame ID/time frame name
- 5—SCE address 32-bit/dotted notation
- 6—IP protocol number/IP protocol name
- 7—Signature protocol ID/protocol name
- 8—P2P signature protocol ID/protocol name
- 11—Global service usage counter ID/counter name
- 12—Subscriber service usage counter ID/counter name
- 13—Package usage counter ID/counter name
- 15—UDP port number/port name
- 16—Policy/Flags
- 17—Service Names
- 18—All links
- 19—Zone name/Zone Id
- 20—Zone name/Zone counter
- 21—Operating System name/Operating System index
- 1002—VoIP protocol family/Protocol name
- 1003—Worm protocol family/Protocol name

- 1005—Packet Stream Pattern-Based Protocols/Protocol name
- 1006—Bundled protocol family/Protocol name
- 1007—Unidirectionally Detected protocol family/Protocol name
- 1008—RTCP protocol family/Protocol name
- 1009—SPAM Detected protocol family/Protocol name
- 1010—Behavioral protocol family/Protocol name
- 1011—E-mail and Newsgroups protocol family/Protocol v
- 1012—Gaming protocol family/Protocol name
- 1013—Generic protocol family/Protocol name
- 1014—HTTP protocol family/Protocol name
- 1015—Instant Messaging protocol family/Protocol name
- 1016—Net Admin protocol family/Protocol name
- 1017—Video protocol family/Protocol name
- 1018—Tunneling protocol family/Protocol name
- 1019—ClickStream protocol family/Protocol name
- 2001—P2P protocol family/Global Counter name
- 2002—VoIP protocol family/Global Counter name
- 2003—Worm protocol family/Global Counter name
- 2005—Packet Stream Pattern-Based Protocols/Global Counter name
- 2006—Bundled protocol family/Global Counter name
- 2007—Unidirectionally Detected protocol family/Global Counter name
- 2008—RTCP protocol family/Global Counter name
- 2009—SPAM Detected protocol family/Global Counter name
- 2010—Behavioral protocol family/Global Counter name
- 2011—E-mail and Newsgroups protocol family/Global Counter name
- 2013—Generic protocol family/Global Counter name
- 2014—HTTP protocol family/Global Counter name
- 2015—Instant Messaging protocol family/Global Counter name
- 2017—Video protocol family/Global Counter name
- 2018—Tunneling protocol family/Global Counter name
- 2019—ClickStream protocol family/Global Counter name
- 3001—P2P protocol family/Subscriber Counter name
- 3002—VoIP protocol family/Subscriber Counter name
- 3005—Packet Stream Pattern-Based Protocols/Subscriber Counter name
- 3007—Unidirectionally Detected protocol family/Subscriber Counter name
- 3010—Behavioral protocol family/Subscriber Counter name
- 3013—Generic protocol family/Subscriber Counter name
- 3014—HTTP protocol family/Subscriber Counter name

- 3015—Instant Messaging protocol family/Subscriber Counter name
- 3017—Video protocol family/Subscriber Counter name
- 3019—Tunneling protocol family/Subscriber Counter name
- 4001—P2P protocol family/Signature
- 4002—VoIP protocol family/Signature
- 4003—Worm protocol family/Signature
- 4005—Packet Stream Pattern-Based Protocols/Signature
- 4006—Bundled protocol family/Signature
- 4007—Unidirectionally Detected protocol family/Signature
- 4008—RTCP protocol family/Signature
- 4009—SPAM Detected protocol family/Signature
- 4010—Behavioral protocol family/Signature
- 4011—E-mail and Newsgroups protocol family/Signature
- 4012—Gaming protocol family/Signature
- 4013—Generic protocol family/Signature
- 4014—HTTP protocol family/Signature
- 4015—Instant Messaging protocol family/Signature
- 4016—Net Admin protocol family/Signature
- 4017—Video protocol family/Signature
- 4018—Tunneling protocol family/Signature
- 4019—ClickStream protocol family/Signature

Table VLINK_INI

Database table VLINK_INI is updated when the Collection Manager utility update_vlinks.sh is run. This table contains the name and ID of each virtual link defined in the SCE platform. Cisco Insight uses the mappings contained in this table for the Virtual Links reports.

Table 4-25 lists the columns of the VLINK_INI table.

Table 4-25 Columns of Table VLINK_INI

Field Name	Type	Description
TIME_STAMP	Date_Time	
SE_IP	String	Identification of the SCE platform where these values were applied.
VLINK_ID	UINT16	Virtual link ID.
VLINK_DIRECTION	INT8	Virtual link direction.
VLINK_NAME	String	Virtual link name.
CHANNEL_ID	UINT16	Channel ID.
CHANNEL_NAME	String	Name of the channel.
CMTS_NAME	String	Name of the CMTS.

Table CONF_SE_TZ_OFFSET

Database table CONF_SE_TZ_OFFSET contains the time-zone offset in minutes for the clock of each SCE platform as configured by the select-sce-tz.sh script.

Table 4-26 lists the columns of table CONF_SE_TZ_OFFSET.

Table 4-26 Columns of Table CONF_SE_TZ_OFFSET

Field Name	Type
TIME_STAMP	Date_Time
OFFSET_MIN	Number

Table RPT_TOP_APN

The RAG adapter generates database table RPT_TOP_APN for the configured aggregation interval (1 hour by default) as configured in vsa_SURs.xml.

Table 4-27 lists the columns of the RPT_TOP_APN table.

Table 4-27 Columns of Table RPT_TOP_APN

Field Name	Type
TIME_STAMP	Date_Time
AGG_PERIOD	Number
APN	String
SERVICE_USAGE_COUNTER_ID	Number
UPSTREAM_VOLUME	Number
DOWNSTREAM_VOLUME	Number
RANK_VOLUME	Number

At the end of the each aggregation period, the Cisco SCMS Collection Manager inserts the aggregated records into the table. Rank is a sequential numerical value that indicates the top entries. The ranks of VSA attributes are based on usage (downstream, upstream) of particular services.

From the RPT_TOP_APN table, you can generate reports such as Usage per APN and Application Usage per APN.

Table RPT_TOP_DEVICE_TYPE

The RAG adapter generates database table RPT_TOP_DEVICE_TYPE for the configured aggregation interval (1 hour by default) as configured in vsa_SURs.xml.

Table 4-28 lists the columns of the RPT_TOP_DEVICE_TYPE table.

Table 4-28 Columns of Table RPT_TOP_DEVICE_TYPE

Field Name	Type
TIME_STAMP	Date_Time
AGG_PERIOD	Number
IMEI_TAC	String
SERVICE_USAGE_COUNTER_ID	Number
UPSTREAM_VOLUME	Number
DOWNSTREAM_VOLUME	Number
UNIQ_SUBS	Number
RANK_VOLUME	Number
RANK_UNIQ_SUBS	Number

At the end of the each aggregation period, the Collection Manager inserts the aggregated records into the table. Rank is a sequential numerical value that indicates the top entries. RANK_VOLUME is derived based on the usage (downstream, upstream) of particular services. RANK_UNIQ_SUBS is derived based on the total number of unique subscribers on a particular service.

From the RPT_TOP_DEVICE_TYPE table, we can generate reports such as Device Type Distribution (IMEI), Usage per Device, and Application Usage per Device.

Table RPT_TOP_NETWORK_TYPE

The RAG adapter generates database table RPT_TOP_NETWORK_TYPE for the configured aggregation interval (1 hour by default) as configured in vsa_SURs.xml.

Table 4-29 lists the columns of the RPT_TOP_NETWORK_TYPE table.

Table 4-29 Columns of Table RPT_TOP_NETWORK_TYPE

Field Name	Type
TIME_STAMP	Date_Time
AGG_PERIOD	Number
NETWORK_TYPE	String
SERVICE_USAGE_COUNTER_ID	Number
UPSTREAM_VOLUME	Number
DOWNSTREAM_VOLUME	Number
RANK_VOLUME	Number

At the end of the each aggregation period, the Collection Manager inserts the aggregated records into the table. Rank is a sequential numerical value that indicates the top entries. RANK_VOLUME is derived based on the usage (downstream, upstream) of particular services.

From the RPT_TOP_NETWORK_TYPE table, you can generate reports such as Usage per Network Type and Application Usage per Network Type.

Table RPT_TOP_SGSN

The RAG adapter generates database table RPT_TOP_SGSN for the configured aggregation interval (1 hour by default) as configured in vsa_SURs.xml.

Table 4-30 lists the columns of the RPT_TOP_SGSN table.

Table 4-30 Columns of Table RPT_TOP_SGSN

Field Name	Type
TIME_STAMP	Date_Time
AGG_PERIOD	Number
SGSN	String
SERVICE_USAGE_COUNTER_ID	Number

Table 4-30 Columns of Table RPT_TOP_SGSN (continued)

Field Name	Type
UPSTREAM_VOLUME	Number
DOWNSTREAM_VOLUME	Number
RANK_VOLUME	Number

At the end of the each aggregation period, the Collection Manager inserts the aggregated records into the table. Rank is a sequential numerical value that indicates the top entries. RANK_VOLUME is derived based on the usage (downstream, upstream) of particular services.

From the RPT_TOP_SGSN table, you can generate a Usage per SGSN report.

Table RPT_TOP_USER_LOCATION

The RAG adapter generates database table RPT_TOP_USER_LOCATION for the configured aggregation interval (1 hour by default) as configured in vsa_SURs.xml.

Table 4-31 lists the columns of the RPT_TOP_USER_LOCATION table.

Table 4-31 Columns of Table RPT_TOP_USER_LOCATION

Field Name	Type
TIME_STAMP	Date_Time
AGG_PERIOD	Number
USER_LOCATION	String
SERVICE_USAGE_COUNTER_ID	Number
UPSTREAM_VOLUME	Number
DOWNSTREAM_VOLUME	Number
UNIQ_SUBS	Number
RANK_VOLUME	Number

At the end of the each aggregation period, the Collection Manager inserts the aggregated records into the table. Rank is a sequential numerical value that indicates the top entries. RANK_VOLUME is derived based on the usage (downstream, upstream) of particular services.

From the RPT_TOP_USER_LOCATION table, you can generate reports such as Number of Subscribers per Location and Usage per Location.

Table RPT_DVLINK

The RAG adapter generates database table RPT_DVLINK. It aggregates the subscriber usage RDR data. Aggregation is based on per package and per VLINK (DOWN VLINK). You can generate a report.

Table 4-32 lists the columns of the RPT_DVLINK table.

Table 4-32 Columns of Table RPT_DVLINK

Field Name	Type
TIME_STAMP	Date_Time
RECORD_SOURCE	Number
SUBSCRIBER_ID	String
PACKAGE_ID	Number
SUBS_USG_CNT_ID	Number
BREACH_STATE	Number
REASON	Number
CONFIGURED_DURATION	Number
DURATION	Number
END_TIME	Number
UPSTREAM_VOLUME	Number
DOWNSTREAM_VOLUME	Number
SESSIONS	Number
SECONDS	Number
UP_VLINK_ID	Number
DOWN_VLINK_ID	Number

Table RPT_UVLINK

The RAG adapter generates database table RPT_UVLINK. It aggregates the subscriber usage RDR data. Aggregation is based on per package and per VLINK (UP VLINK). You can generate a report.

Table 4-33 lists the columns of the RPT_UVLINK table.

Table 4-33 Columns of Table RPT_UVLINK

Field Name	Type
TIME_STAMP	Date_Time
RECORD_SOURCE	Number
SUBSCRIBER_ID	String
PACKAGE_ID	Number
SUBS_USG_CNT_ID	Number
BREACH_STATE	Number
REASON	Number
CONFIGURED_DURATION	Number
DURATION	Number
END_TIME	Number
UPSTREAM_VOLUME	Number
DOWNSTREAM_VOLUME	Number
SESSIONS	Number
SECONDS	Number
UP_VLINK_ID	Number
DOWN_VLINK_ID	Number

Table RPT_TOP_HTTP_DOMAINS

The RAG adapter generates database table RPT_TOP_HTTP_DOMAINS for the configured aggregation interval (1 hour by default) as configured in http_TURs.xml. It aggregates the HTTP transaction usage RDR data. Aggregation is based on domain, service, and package. You can generate reports.

Table 4-34 lists the columns of the RPT_TOP_HTTP_DOMAINS table.

Table 4-34 Columns of Table RPT_TOP_HTTP_DOMAINS

Field Name	Type
TIME_STAMP	Date_Time
AGG_PERIOD	Number
DOMAIN	String
SERVICE_ID	Number
PACKAGE_ID	Number
SESSIONS	Number
UPSTREAM_VOLUME	Number
DOWNSTREAM_VOLUME	Number
DURATION	Number
UNIQ_SUBS	Number
RANK_VOLUME	Number
RANK_SESSIONS	Number
RANK_UNIQ_SUBS	Number

At the end of the each aggregation period, the Collection Manager inserts the aggregated records into the table. Rank is a sequential numerical value that indicates the top entries. RANK_VOLUME is derived based on the usage (downstream, upstream), package, and service. RANK_SESSIONS is derived based on the total sessions, package, and service. RANK_UNIQ_SUBS is derived based on the total number of unique subscribers, package, and service.

Table RPT_TOP_HTTP_HOSTS

The RAG adapter generates database table RPT_TOP_HTTP_HOSTS for the configured aggregation interval (1 hour by default) as configured in http_TURs.xml. It aggregates the HTTP transaction usage RDR data. Aggregation is based on domain, service, and package. You can generate reports.

Table 4-35 lists the columns of the RPT_TOP_HTTP_HOSTS table.

Table 4-35 Columns of Table RPT_TOP_HTTP_HOSTS

Field Name	Type
TIME_STAMP	Date_Time
AGG_PERIOD	Number
HOST	String
SERVICE_ID	Number
PACKAGE_ID	Number
SESSIONS	Number
UPSTREAM_VOLUME	Number
DOWNSTREAM_VOLUME	Number
DURATION	Number
UNIQ_SUBS	Number
RANK_VOLUME	Number
RANK_SESSIONS	Number
RANK_UNIQ_SUBS	Number
DOMAIN	String

At the end of the each aggregation period, the Collection Manager inserts the aggregated records into the table. Rank is a sequential numerical value that indicates the top entries. RANK_VOLUME is derived based on the usage (downstream, upstream), package, and service. RANK_SESSIONS is derived based on the total sessions, package, and service. RANK_UNIQ_SUBS is derived based on the total number of unique subscribers, package, and service.

Table RPT_TOP_VIDEO_DOMAINS

The RAG adapter generates database table RPT_TOP_VIDEO_DOMAINS for the configured aggregation interval (1 hour by default) as configured in video_TURs.xml. It aggregates the video transaction usage RDR data. Aggregation is based on domain, service, and package. You can generate reports.

Table 4-36 lists the columns of the RPT_TOP_VIDEO_DOMAINS table.

Table 4-36 Columns of Table RPT_TOP_VIDEO_DOMAINS

Field Name	Type
TIME_STAMP	Date_Time
AGG_PERIOD	Number
DOMAIN	String
SERVICE_ID	Number
PACKAGE_ID	Number
SESSIONS	Number
UPSTREAM_VOLUME	Number
DOWNSTREAM_VOLUME	Number
DURATION	Number
UNIQ_SUBS	Number
RANK_VOLUME	Number
RANK_SESSIONS	Number
RANK_UNIQ_SUBS	Number

At the end of the each aggregation period, the Collection Manager inserts the aggregated records into the table. Rank is a sequential numerical value that indicates the top entries. RANK_VOLUME is derived based on the usage (downstream, upstream), package, and service. RANK_SESSIONS is derived based on the total sessions, package, and service. RANK_UNIQ_SUBS is derived based on the total number of unique subscribers, package, and service.

Table RPT_TOP_VIDEO_HOSTS

The RAG adapter generates database table RPT_TOP_VIDEO_HOSTS for the configured aggregation interval (1 hour by default) as configured in video_TURs.xml. It aggregates the video transaction usage RDR data. Aggregation is based on domain, service, and package. You can generate reports.

Table 4-37 lists the columns of the RPT_TOP_VIDEO_HOSTS table.

Table 4-37 Columns of Table RPT_TOP_VIDEO_HOSTS

Field Name	Type
TIME_STAMP	Date_Time
AGG_PERIOD	Number
HOST	String
SERVICE_ID	Number
PACKAGE_ID	Number
SESSIONS	Number
UPSTREAM_VOLUME	Number
DOWNSTREAM_VOLUME	Number
DURATION	Number
UNIQ_SUBS	Number
RANK_VOLUME	Number
RANK_SESSIONS	Number
RANK_UNIQ_SUBS	Number
DOMAIN	String

At the end of the each aggregation period, the Collection Manager inserts the aggregated records into the table. Rank is a sequential numerical value that indicates the top entries. RANK_VOLUME is derived based on the usage (downstream, upstream), package, and service. RANK_SESSIONS is derived based on the total sessions, package, and service. RANK_UNIQ_SUBS is derived based on the total number of unique subscribers, package, and service.

Table RPT_ZUR

The RPT_ZUR database table stores data from ZONE_USAGE_RDRs.

These RDRs have the tag 4042321928.

Table 4-38 lists the columns of the RPT_ZUR table.

Table 4-38 Columns of Table RPT_ZUR

Field Name	Type
ZONE_COUNTER_ID	Number
GENERATOR_ID	Number
GLBL_USG_CNT_ID	Number
CONFIGURED_DURATION	Number
DURATION	Number
END_TIME	Number
UPSTREAM_VOLUME	Number
DOWNSTREAM_VOLUME	Number
SESSIONS	Number
SECONDS	Number
CONCURRENT_SESSIONS	Number
ACTIVE_SUBSCRIBERS	Number
TOTAL_ACTIVE_SUBSCRIBERS	Number
IP_TYPE	Number

Table RPT_SPAM

The RPT_SPAM database table stores data from SPAM_RDRs.

These RDRs have the tag 4042322048.

Table 4-39 lists the columns of the RPT_SPAM table.

Table 4-39 Columns of Table RPT_SPAM

Field Name	Type
SUBSCRIBER_ID	String
PACKAGE_ID	Number
SERVICE_ID	Number
PROTOCOL_ID	Number
CLIENT_IP	Number
CLIENT_PORT	Number
SERVER_IP	Number
SERVER_PORT	Number
INITIATING_SIDE	Number
ACCESS_STRING	String
INFO_STRING	String
SPAM_FOUND	Number
THRESHOLD_LEVEL	Number
SESSION_COUNTER	Number
TIME_INTERVAL	Number
DEFINED_SESSION_COUNTER	Number
DEFINED_TIME_INTERVAL	Number
REPORT_TIME	Number
AGGR_MESSAGES_COUNTER	Number
TIME_INTERVAL_MSG_COUNTER	Number
NO_OF_MSG_SMTP_SESSION	Number
NO_OF_FAILED_MSG_SMTP_SESSION	Number
FAILED_MSG_SMTP_SESSION	Number
PROTOCOL_NON_COMPLIANCE	Number
DEFINED_MSG_COUNTER	Number
DEFINED_MSG_TIME_INTERVAL	Number
DEFINED_NO_OF_MSG_SMTP_SESSION	Number
EMAIL_HARVEST_MSGSMTP_SESSION	Number
DEFINED_FAILED_MSGSMTP_SESSION	Number
PROTOCOL_COMPLIANCE	Number

Table RPT_FUR

The RPT_SPAM database table stores data from Online_Flow_Usage_RDRs.

These RDRs have the tag 4042321927.

Table 4-40 lists the columns of the RPT_FUR table.

Table 4-40 Columns of Table RPT_FUR

Field Name	Type
SUBSCRIBER_ID	String
PACKAGE_ID	Number
SERVICE_ID	Number
PROTOCOL_ID	Number
REASON	Number
SERVER_IP	Number
SERVER_PORT	Number
ACCESS_STRING	String
INFO_STRING	String
CLIENT_IP	Number
CLIENT_PORT	Number
INITIATING_SIDE	Number
END_TIME	Number
MILLISEC_DURATION	Number
TIME_FRAME	Number
SESSION_UPSTREAM_VOLUME	Number
SESSION_DOWNSTREAM_VOLUME	Number
SUBSCRIBER_COUNTER_ID	Number
GLOBAL_COUNTER_ID	Number
PACKAGE_COUNTER_ID	Number
IP_PROTOCOL	Number
PROTOCOL_SIGNATURE	Number
ZONE_ID	Number
FLAVOR_ID	Number
FLOW_CLOSE_MODE	Number
FLOW_ID	Number
SESSION_ID	Number

Table IMEI_DEVICETYPE

The IMEI_DEVICETYPE database table contains mappings for the device types with IMEI_TAC. Cisco Insight uses the IMEI_TAC column for the Device Type Reports.

Table 4-41 lists the columns of the IMEI_DEVICETYPE table.

Table 4-41 Columns of Table IMEI_DEVICETYPE

Field Name	Type
TIME_STAMP	Timestamp
IMEI_TAC	String
DEVICE_TYPE	String

Table RTP_VIDEO_QOE

The RTP_VIDEO_QOE database table contains the video quality of experience (QoE) rate and the number of videos watched by the subscriber.

Table 4-42 lists the columns of the RTP_VIDEO_QOE table.

Table 4-42 Columns of Table RTP_VIDEO_QOE

Field Name	Type
TIME_STAMP	Timestamp
PACKAGE_ID	INT16
SERVICE_ID	INT16
VIDEO_COUNT	UINT32
QOE_RATING	UINT8
AGG_PERIOD	UINT8

Table RPT_VIDEO_DURATION

The RPT_VIDEO_DURATION database table contains the video quality information based on the video duration.

Table 4-43 lists the columns of the RPT_VIDEO_DURATION table.

Table 4-43 Columns of Table RPT_VIDEO_DURATION

Field Name	Type
TIME_STAMP	Timestamp
PACKAGE_ID	INT16
SERVICE_ID	INT16
VIDEO_MONITOR_ID	UINT8

Table 4-43 Columns of Table RPT_VIDEO_DURATION

Field Name	Type
UPSTREAM_VOLUME	UINT32
DOWNSTREAM_VOLUME	UINT32
VIDEO_COUNT	UINT32
AGG_PERIOD	UINT16

Table RPT_VIDEO_RESOLUTION

The RPT_VIDEO_RESOLUTION database table contains the video quality information based on the video resolution.

Table 4-44 lists the columns of the RPT_VIDEO_RESOLUTION table.

Table 4-44 Columns of Table RPT_VIDEO_RESOLUTION

Field Name	Type
TIME_STAMP	Timestamp
PACKAGE_ID	INT16
SERVICE_ID	INT16
VIDEO_MONITOR_ID	UINT8
UPSTREAM_VOLUME	UINT32
DOWNSTREAM_VOLUME	UINT32
VIDEO_COUNT	UINT32
AVG_BIT_RATE	UINT32
AGG_PERIOD	UINT16

Table RPT_VIDEO_BITRATE

The RPT_VIDEO_BITRATE database table contains the video quality information based on the video bitrate.

Table 4-45 lists the columns of the RPT_VIDEO_BITRATE table.

Table 4-45 Columns of Table RPT_VIDEO_BITRATE

Field Name	Type
TIME_STAMP	Timestamp
PACKAGE_ID	INT16
SERVICE_ID	INT16
VIDEO_MONITOR_ID	UINT8
UPSTREAM_VOLUME	UINT32
DOWNSTREAM_VOLUME	UINT32

Table 4-45 Columns of Table RPT_VIDEO_BITRATE

Field Name	Type
VIDEO_COUNT	UINT32
AGG_PERIOD	UINT16

Table VIDEO_MONITOR_TYPES

The VIDEO_MONITOR_TYPES contains the mapping information for video duration, bitrate, and resolution for reporting.

Table 4-46 lists the columns of the VIDEO_MONITOR_TYPES table.

Table 4-46 Columns of Table VIDEO_MONITOR_TYPES

Field Name	Type
TIME_STAMP	Timestamp
VIDEO_MONITOR_ID	UINT8
VIDEO_MONITOR_DESC	String
VIDEO_MONITOR_TYPE	UINT8

Table RPT_DEVICE_COUNT

The RPT_DEVICE_COUNT database table contains the unique subscriber details and information about the consumed volume of devices during an aggregation period.

Table 4-47 lists the columns of the RPT_DEVICE_COUNT table.

Table 4-47 Columns of Table RPT_DEVICE_COUNT

Field Name	Type
TIME_STAMP	Timestamp
PACKAGE_ID	INT16
DEVICE_ID	INT16
UPSTREAM_VOLUME	UINT32
DOWNSTREAM_VOLUME	UINT32
UNIQ_SUBS	UINT32
AGG_PERIOD	UINT16

Table RPT_DEVICE_TYPES

The RPT_DEVICE_TYPES database table contains mapping infomation for device counting based reporting.

Table 4-48 lists the columns of the RPT_DEVICE_TYPES table.

Table 4-48 Columns of Table RPT_DEVICE_TYPES

Field Name	Type
DEVICE_ID	String
DEVICE_DESC	String
DEVICE_TYPE	UNIT8

CSV File Formats

Published: December 23, 2013

Introduction

The Cisco SCA BB provides several types of CSV flat files. You can review and configure these files using third-party applications such as Excel.

This chapter consists of these sections:

- Information About Service Configuration Entities CSV File Formats, page 5-2
- Information About Subscriber CSV File Formats, page 5-7
- Information About Collection Manager CSV File Formats, page 5-9

Information About Service Configuration Entities CSV File Formats

This section describes the file formats of the CSV files created when exporting service configuration entities into CSV files. The same format must be used for importing such entities into service configurations.

For more information about exporting and importing service configuration entities, see the "Managing Service Configurations" section in the "Using the Service Configuration Editor" chapter of *Cisco Service Control Application for Broadband User Guide*.

Note There is no need to repeat the same values in subsequent rows of the CSV file. If a field is left empty in a row, the value of that field from the previous row is used.

This section consists of these sub-sections:

- Service CSV Files, page 5-2
- Protocol CSV Files, page 5-3
- Zone CSV Files, page 5-3
- Information About Flavor CSV Files, page 5-3

Service CSV Files

Lines in Service CSV files have the following fixed format:

```
service name,service numeric ID,[description],sample rate,parent name,global counter
index,subscriber counter index,[flavor],initiating side,protocol,[zone]
```

- The only service that does not have a parent service is the default service.
- The default service is the parent of all other services.
- If the service is counted with its parent, it must have a counter index of –1.
- One service can have multiple entries in the file (see the following example). There is no need to state the service properties for each of its items.
- Some fields can take a null value (see the last line of the following example).

The following is an example of a Service CSV file:

```
P2P,9,,10,Default Service,9,9,,EitherSide,DirectConnect,zone1
P2P,9,,10,Default Service,9,9,flavor1,EitherSide,Manolito, zone1
,,,,,,,,EitherSide,Hotline, zone1
,,,,,,, flavor2,EitherSide,Share, zone1
Generic,1,,10,Default Service,-1,-1,No items,null,null,null
```

Protocol CSV Files

Lines in Protocol CSV files have the following fixed format:

```
protocol name,protocol index,[IP protocol],[port range],signature
```

One protocol can have multiple entries in the file (see the following example).

Port range has the format MinPort-MaxPort. For example, 1024-5000 means port 1024 to port 5000.

The following is an example of a Protocol CSV file:

```
HTTP Browsing,2,TCP,80-80,Generic
HTTP Browsing,2,TCP,8080-8080,Generic
HTTP Browsing,2,,,HTTP
```

Zone CSV Files

Two formats—Standard and Easy—are available for Zone CSV files.

Standard Format

Lines in Zone CSV files in Standard format have the following fixed format:

```
zone name,zone index,IP range
```

Where IP range is an IP address in dotted notation, followed by a mask.

The following is an example of a Zone CSV file in Standard format:

```
zone1,1,10.1.1.0/24
,,10.1.2.0/24
Zone2, 14,2001:0db8:f0fd:a0bd:1234:98dc:cccc:aa24/48
```

Easy Format

Lines in Zone CSV files in Easy format have only Zone items.

The following is an example of a Zone CSV file in Easy format:

```
1.0.0.0/32
1.0.0.1/32
1.0.0.2/32
2001:0db8:f0fd:a0bd:1234:98dc:cccc:aa24/48
```

Information About Flavor CSV Files

The format of Flavor CSV files depends on the flavor type.

Each line of every Flavor CSV files begins with the same three fields:

```
flavor name,flavor index,flavor type[,flavor specific field[s]]
```

The formats of the CSV files of different flavors are described in the following sections.

The following is an example of a line from a Flavor CSV file:

```
HttpUrlFlavor,1,HTTP_URL
```


- HTTP URL CSV Files, page 5-4
- HTTP Referer CSV Files, page 5-4
- HTTP User Agent CSV Files, page 5-5
- HTTP Composite CSV Files, page 5-5
- RTSP User Agent CSV Files, page 5-5
- RTSP Host Name CSV Files, page 5-5
- RTSP Composite CSV Files, page 5-6
- SIP Destination Domain CSV Files, page 5-6
- SIP Source Domain CSV Files, page 5-6
- SIP Composite CSV Files, page 5-6
- SMTP Host Name CSV Files, page 5-6
- ToS CSV Files, page 5-6

For information on flavors, see the "Managing Flavors" section in the "Using the Service Configuration Editor: Traffic Classification" chapter of *Cisco Service Control Application for Broadband User Guide*.

HTTP URL CSV Files

Two formats—Standard and Easy—are available for HTTP URL CSV files.

Standard Format

Lines in HTTP URL CSV files in Standard format have the following fixed format:

```
flavor name,flavor index,flavor type,host suffix,params prefix,URI suffix,URI prefix
```

The following is an example of an HTTP URL CSV file in Standard format:

```
NEWS,0,HTTP_URL,*.reuters.com,,,/news/*
,,,*.msnbc.msn.com,,,
,,,*.wired.com,,,/news/technology/*
,,,*.cbsnews.com,,,/sections/world/*
,,,*.cnn.com,,,/WORLD/*
```

Easy Format

Lines in HTTP URL CSV files in Easy format have a single URL format.

The following is an example of an HTTP URL CSV file in Easy format:

```
http://*.rapidshare.com/cgi-bin/upload*
http://*.rapidshare.com/files*
```

HTTP Referer CSV Files

Two formats—Standard and Easy—are available for HTTP Referer CSV files.

Standard Format

Lines in HTTP Referer CSV files in Standard format have the following fixed format:

```
flavor name,flavor index,flavor type,host suffix,params prefix,URI suffix,URI prefix
```

The following is an example of an HTTP Referer CSV file in Standard format:

```
NEWS,0,HTTP_Referer,*.reuters.com,,,/news/*
,,,*.msnbc.msn.com,,,
,,,*.wired.com,,,/news/technology/*
,,,*.cbsnews.com,,,/sections/world/*
,,,*.cnn.com,,,/WORLD/*
```

Easy Format

Lines in HTTP Referer CSV files in Easy format have a single URL format.

The following is an example of an HTTP Referer CSV file in Easy format:

```
http://*.rapidshare.com/cgi-bin/upload*
http://*.rapidshare.com/files*
```

HTTP User Agent CSV Files

Lines in HTTP User Agent CSV files have the following fixed format:

```
flavor name,flavor index,flavor type,user agent
```

HTTP Composite CSV Files

Lines in HTTP Composite CSV files have the following fixed format:

```
flavor name,flavor index,flavor type,HTTP_URL_name,HTTP_User_Agent_name
```

Where HTTP_URL_name and HTTP_User_Agent_name are the names of existing flavors of types HTTP URL and HTTP User Agent, respectively.

RTSP User Agent CSV Files

Lines in RTSP User Agent CSV files have the following fixed format:

```
flavor name,flavor index,flavor type,user agent
```

RTSP Host Name CSV Files

Lines in RTSP Host Name CSV files have the following fixed format:

```
flavor name,flavor index,flavor type,host suffix
```

RTSP Composite CSV Files

Lines in RTSP Composite CSV files have the following fixed format:

```
flavor name,flavor index,flavor type,RTSP_Host_Name,RTSP_User_Agent_name
```

Where RTSP_Host_Name and RTSP_User_Agent_name are the names of existing flavors of types RTSP Host Name and RTSP User Agent, respectively.

SIP Destination Domain CSV Files

Lines in SIP Destination Domain CSV files have the following fixed format:

```
flavor name,flavor index,flavor type,host suffix
```

SIP Source Domain CSV Files

Lines in SIP Source Domain CSV files have the following fixed format:

```
flavor name,flavor index,flavor type,host suffix
```

SIP Composite CSV Files

Lines in HTTP Composite CSV files have the following fixed format:

```
flavor name,flavor index,flavor type,SIP_Destination_Domain_name,SIP_Source_Domain_name
```

Where SIP_Destination_Domain_name and SIP_Source_Domain_name are the names of existing flavors of types SIP Destination Domain and SIP Source Domain, respectively.

SMTP Host Name CSV Files

Lines in SMTP Host Name CSV files have the following fixed format:

```
flavor name,flavor index,flavor type,host suffix
```

ToS CSV Files

Lines in ToS CSV files have the following fixed format:

```
flavor name,flavor index,flavor type,ToS value
```

Information About Subscriber CSV File Formats

This section describes the file formats of various subscriber CSV files used by the Cisco SCMS Subscriber Manager.

This section consists of these subsections:

- Import/Export File: Format of the Mappings Field, page 5-7
- SCE Subscriber CSV Files, page 5-8
- SCMS SM Subscriber CSV Files, page 5-8
- SCE Anonymous Group CSV Files, page 5-8
- Cisco SCA BB Anonymous Group Import CSV File, page 5-9
- SCE Subscriber Template CSV File, page 5-9

For more information about these CSV file formats, see the following documents:

- "Subscriber Files" section in the "Managing Subscribers" chapter of *Cisco SCE 8000 10GBE Software Configuration Guide*.
- "Subscriber Files" section in the "Managing Subscribers" chapter of *Cisco SCE 8000 GBE Software Configuration Guide*.
- *Cisco Service Control Management Suite Subscriber Manager User Guide*.

Import/Export File: Format of the Mappings Field

Some of the CSV files include a mappings field. This field can include one or more of the following values delimited by colons (":") or semicolons (";"):

- Single IP address in dotted notation (xx.xx.xx.xx).
- IP address ranges in dotted notation (xx.xx.xx.xx/mask).
- Single VLAN (xx) as an integer in decimal notation in the range of 0 - 2044.
- VLAN ranges (xx-yy), where both values are integers in decimal notation in the range of 0 - 2044.

Note Specifying VLAN and IP mappings together in the same line is not allowed.

The following are examples of the mappings field:

- Multiple IP mappings—10.1.1.0/24;10.1.2.238
- Multiple VLAN mappings—450:896-907

SCE Subscriber CSV Files

The lines in the Cisco SCE Subscriber CSV files have the following fixed format:

```
subscriber-id,mappings,package-id,upstream Virtual Link id,downstream Virtual Link id
```

The following is a sample CSV file for use with the Cisco SCE CLI:

```
JerryS,80.179.152.159;80.179.152.179,0,1,3
ElainB,194.90.12.2,3,55,87
sub_ipv6,,1080:1e01:e902::/48,10,0,0,0
sub_dualstack,10.20.12.123/32,2001:0db8:f0fd:a0bd:1234:98dc:cccc:aa24/48,20,0,0,0
```

SCMS SM Subscriber CSV Files

The lines in the Cisco Service Control SM Subscriber CSV files have the following fixed format:

```
subscriber-id,domain,mappings,package-id,upstream Virtual Link id,downstream Virtual Link
id
```

If no domain is specified, the default domain (subscribers) is assigned.

The following is an example CSV file for use with the SM CLI:

```
JerryS,subscribers,80.179.152.159,0,0,0
ElainB,,194.90.12.2,3,12,1
sub_ipv6,subscribers,fe80:0:1::/64,1,,,
```

SCE Anonymous Group CSV Files

Lines in SCE Anonymous Group CSV files have the following fixed format:

```
anonymous-group-name,IP-range,[subscriber-template-number]
```

If no subscriber-template-number is specified, the anonymous subscribers of that group use the default template (equivalent to using a subscriber-template-number value of zero).

The mapping between subscriber-template-number and package-id is defined in the SCE Subscriber Template CSV file, which is described in the "SCE Subscriber Template CSV File" section on page 5-9.

The following is an example of an anonymous group CSV file:

```
group1,176.23.34.0/24,3
group2,10.7.0.0/16
```

Cisco SCA BB Anonymous Group Import CSV File

Lines in the Cisco SCA BB Anonymous Group Import CSV files have the following fixed format:

```
anonymous-group-name,IP-range,[subscriber-template-number],[subscriber Manager]
```

All fields are mandatory while importing to Cisco SCA BB console.

The following is a sample anonymous group CSV file for Cisco SCA BB:

```
group1,176.23.34.0/24,3,SM
group2,10.7.0.0/16,SM
group2,2001:0db8:f0fd:a0bd:1234:98dc:cccc:aa24/48,2,SM
```

SCE Subscriber Template CSV File

Lines in Subscriber Template CSV files have the following fixed format:

```
subscriber-template-number,package-id
```

Cisco SCA BB includes a default one-to-one mapping between package-id and subscriber-template-number for values from 0 to 199.

Subscriber-template-numbers can take values from 0 through 199. You can map more than one subscriber-template-number to the same package-id.

For more information about this file, see either the *Cisco SCE 8000 10GBE Software Configuration Guide* or the *Cisco SCE 8000 GBE Software Configuration Guide*.

Information About Collection Manager CSV File Formats

This section describes the file formats of the CSV files created by adapters of the Cisco SCMS Collection Manager.

Each RDR is routed to the appropriate adapter—the CSV Adapter, the TA Adapter, or the RAG Adapter—converted, and written to a CSV file.

- CSV Adapter CSV Files, page 5-9
- TA Adapter CSV Files, page 5-10
- RAG Adapter CSV Files, page 5-10

For more information about the Collection Manager and its adapters, see *Cisco Service Control Management Suite Collection Manager User Guide*.

CSV Adapter CSV Files

By default, the CSV Adapter writes files to subdirectories of ~/cm/adapters/CSVAdapter/csvfiles, where each subdirectory name is the RDR tag of the RDR that generated the CSV file.

Each CSV file created by the CSV Adapter has a structure matching the RDR represented in the file. It is possible to include the SE IP (for example, record source) which generated the RDR in the CSV line. To turn this option on, edit the csvadapter.conf file and set the value of includeRecordSource property under [csvadapter] section to true.

Related Topics

- Raw Data Records: Formats and Field Contents, page 2-1

TA Adapter CSV Files

The TA Adapter receives Subscriber Usage RDRs, aggregates the data they contain, and outputs statistics to CSV files. By default, these files are created once every 24 hours, at midnight.

The name of the CSV file is the date and time of its creation. The default format of the file name is *yyyy-MM-dd_HH-mm-ss.csv* (for example, *2005-09-27_18-30-01.csv*). By default, the location of the CSV files is /cm/adapters/TAAdapter/csvfiles.

By default, the fields in each row of the CSV file are as follows:

```
subsID,svcALLup,svcALLdown,svcALLsessions,svcALLseconds,
svc0up,svc0down,svc0sessions,svc0seconds,svc1up,svc1down,svc1sessions,
svc1seconds,...,svcNup,svcNdown,svcNsessions,svcNseconds
```

Where subsID is the Subscriber ID and svcXY is the aggregated volume of metric Y for service X. (The N in svcN is the highest service number, which is the configured number of services minus 1.)

The combined volume is not stored in the CSV file, because it is easily obtained by adding the upstream and downstream volumes.

You can configure the adapter to insert a comment at the beginning of every CSV file. This comment contains a time stamp showing when the file was created, and an explanation of its format. By default, this feature is disabled. To turn on this option, edit the taadapter.conf file and set the value of the write_headers property under the [csv] section to true.

RAG Adapter CSV Files

The RAG Adapter processes RDRs of one or more types and aggregates the data from predesignated field positions into buckets. When a RAG Adapter bucket is flushed, its content is written as a single line into a CSV file, one file per RDR, in the CSV repository of the adapter.

The name of the CSV file is the date and time of its creation. The default format of the file name is yyyy-MM-dd_HH-mm-ss.csv (for example, *2005-09-27_18-30-01.csv*). By default, the CSV repository is flat (all CSV files in one directory), and located at /cm/adapters/RAGAdapter/csvfiles. Alternatively, you can configure the adapter to use a subdirectory structure. The CSV files are written to subdirectories of /cm/adapters/RAGAdapter/csvfiles, where each subdirectory name is the RDR tag of the RDR type that was written to this CSV file.

Each line written to the CSV file may have some synthesized fields added to it, such as time stamps of the first and last RDRs that contributed to this bucket and the total number of RDRs in this bucket. Other fields may be removed altogether. Fields in the output line that are not used for aggregation have values corresponding to the values in the first RDR that contributed to the bucket. However, the time stamp field that is prepended to the line in the CSV file has a value corresponding to the time stamp of the last RDR in the bucket.

Cisco SCA BB Proprietary MIB Reference

Published: December 23, 2013

Introduction

This chapter describes the proprietary CISCO-SCAS-BB Management Information Base (MIB) supported by the Cisco SCE platform.

An MIB is a database of objects that can be monitored by a network management system (NMS). The SCE platform supports both the standard MIB-II and the proprietary Cisco Service Control Enterprise MIB. The CISCO-SCAS-BB MIB is the part of the Service Control Enterprise MIB that enables the external management system to monitor counters and metrics specific to Cisco SCA BB.

This chapter consists of these sections:

- Information About SNMP Configuration and Management, page 6-2
- Information About the Service Control Enterprise MIB, page 6-3
- Information About the CISCO-SCAS-BB MIB, page 6-4
- Guidelines for Using the CISCO-SCAS-BB MIB, page 6-23

Information About SNMP Configuration and Management

This section explains how to configure the SNMP interface, and how to load the MIB files:

- Configuring the SNMP Interface on the SCE Platform, page 6-2
- Related Information, page 6-2
- Required MIB Files, page 6-2
- The Order in Which to Load the MIB Files, page 6-3

Configuring the SNMP Interface on the SCE Platform

Before using the SNMP interface:

- Enable SNMP access on the SCE platform (by default, SNMP access is disabled).
- Set the values of SNMP parameters:
  - The community string to be used for client authentication.
  - (Optional, recommended as a security measure) An access list (ACL) of IP addresses. This limits access to SNMP information to a set of known locations. You can define a different community string for each ACL.
  - The destination IP address to which the SCE platform sends SNMP traps.

Note You can enable or disable specific traps.

Related Information

For more information about SNMP configuration, see the following documents:

- "Configuring and Managing the SNMP Interface" section in "Configuring the Management Interface and Security" chapter of *Cisco SCE 8000 10GBE Software Configuration Guide*.
- "Configuring and Managing the SNMP Interface" section in the "Configuring the Management Interface and Security" chapter of *Cisco SCE 8000 GBE Software Configuration Guide*.

Required MIB Files

To access the SNMP variables on the SCE platform, you must load the SNMP browser with a standard MIB file (*SNMPv2.mib*) and proprietary Cisco MIB files (*pcube.mib*, *pcubeSEMib.mib*, and *PCubeEngageMib.mib*).

Note You can download the CISCO-SCAS-BB MIB file (*PCubeEngageMib.mib*) and other MIB files (*pcube.mib* and *pcubeSEMib.mib*) from ftp://ftp.cisco.com/pub/mibs/.

The Order in Which to Load the MIB Files

The Cisco SCA BB proprietary MIB uses definitions that are defined in other MIBs, such as SNMPv2.mib and pcube.mib.

This means that the order in which the MIBs are loaded is important; to avoid errors, the MIBs must be loaded in the correct order.

Load the MIBs in the following order:

1. SNMPv2.mib
2. pcube.mib
3. pcubeSEMib.mib
4. PCubeEngageMib.mib

Information About the Service Control Enterprise MIB

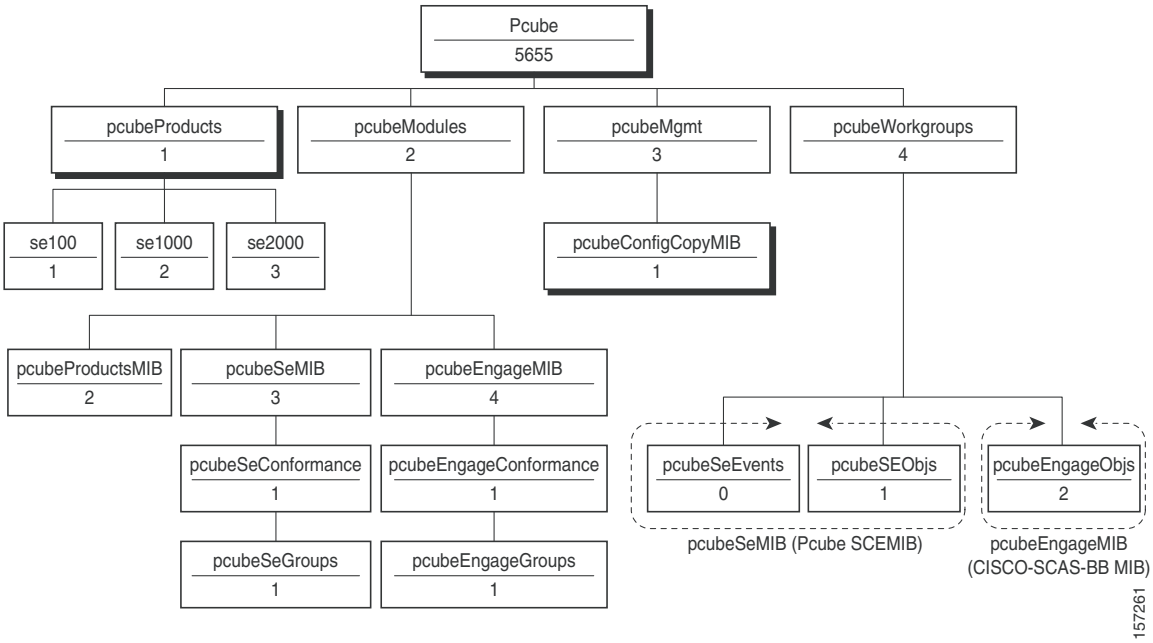
The Service Control Enterprise MIB includes four main groups: Products, Modules, Management, and Workgroup. The Service Control enterprise tree structure is defined in a MIB file named *pcube.mib*.

- pcubeProducts subtree contains the sysObjectIDs of the Service Control products.

  Service Control product sysObjectIDs are defined in a MIB file named *Pcube-Products-MIB*.
- pcubeModules subtree provides a root object identifier from which MIB modules are defined.
- pcubeMgmt subtree contains the configuration copy MIB:
  - *pcubeConfigCopyMib* enables saving the running configuration of Cisco products. This MIB is documented in the "Cisco Service Control MIBs" appendix of *Cisco SCE 8000 10GBE Software Configuration Guide* or in the "Cisco Service Control MIBs" appendix of *Cisco SCE 8000 GBE Software Configuration Guide*.
- pcubeWorkgroup subtree contains:
  - *pcubeSeEvents* and *pcubeSEObjs* —*pcubeSeMib*, the SCE MIB, is the main MIB for the Service Control products and provides a wide variety of configuration and runtime statistics. This MIB is also documented in the "Cisco Service Control MIBs" appendix of *Cisco SCE 8000 10GBE Software Configuration Guide* and in the "Cisco Service Control MIBs" appendix of *Cisco SCE 8000 GBE Software Configuration Guide*.
  - *pcubeEngageObjs*—CISCO-SCAS-BB MIB provides configuration and run-time status for Cisco SCA BB, and is described in the "Information About the CISCO-SCAS-BB MIB" section on page 6-4.

Figure 6-1 illustrates the Service Control Enterprise MIB structure.

Figure 6-1 Service Control Enterprise MIB Structure



Note The following object identifier represents the Service Control Enterprise MIB: *1.3.6.1.4.1.5655* or *so.org.dod.internet.private.enterprise.pcube*.

Information About the CISCO-SCAS-BB MIB

The CISCO-SCAS-BB MIB provides access to service usage counters through the SNMP interface. Using this MIB, a network administrator can collect usage information per service at link, package, or subscriber granularity.

The CISCO-SCAS-BB MIB is defined in the file *PCubeEngageMib.mib*.

The MIB is documented in the remainder of this chapter.

- Using This Reference, page 6-4
- pcubeEngageObjs (pcubeWorkgroup 2), page 6-5

Using This Reference

This reference is divided into sections according to the MIB object groups. For each object, information is presented in the following format:

<Description of the object>

Access	access control associated with the object
Units	unit of measurement used for the object

Index

```
{Indexes used by the table}
```

Syntax

```
OBJECT DATA TYPE {
The general format of the object
}
```

pcubeEngageObjs (pcubeWorkgroup 2)

The pcubeEngageObjs objects provide current information about packages, service, and subscribers.

- pcubeEngageObjs Objects, page 6-5
- pcubeEngageObjs Structure, page 6-5
- Service Group: serviceGrp (pcubeEngageObjs 1), page 6-6
- Link Group: linkGrp (pcubeEngageObjs 2), page 6-7
- Package Group: packageGrp (pcubeEngageObjs 3), page 6-11
- Subscriber Group: subscriberGrp (pcubeEngageObjs 4), page 6-17
- Service Counter Group: serviceCounterGrp (pcubeEngageObjs 5), page 6-20

pcubeEngageObjs Objects

Table 6-1 lists the pcubeEngageObjs objects. Each object consists of a number of subordinate object types, which are summarized in the following section.

Table 6-1 pcubeEngageObjs Objects

serviceGrp	{pcubeEngageObjs 1}
linkGrp	{pcubeEngageObjs 2}
packageGrp	{pcubeEngageObjs 3}
subscriberGrp	{pcubeEngageObjs 4}
serviceCounterGrp	{pcubeEngageObjs 5}

pcubeEngageObjs Structure

This is a summary of the structure of pcubeEngageObjs. Note the table structure for objects that may have multiple entries.

```
serviceGrp
           serviceTable-deprecated

           linkGrp
           linkServiceUsageTable
               linkServiceUsageEntry
                   linkServiceUsageUpVolume
                   linkServiceUsageDownVolume
                   linkServiceUsageNumSessions
                   linkServiceUsageDuration
                   linkServiceUsageConcurrentSessions
```

```
        linkServiceUsageActiveSubscribers
        linkServiceUpDroppedPackets
        linkServiceDownDroppedPackets
        linkServiceUpDroppedBytes
        linkServiceDownDroppedBytes
packageGrp
packageCounterTable
    packageCounterEntry
        packageCounterIndex
        packageCounterStatus
        packageCounterName
        packageCounterActiveSubscribers
        packageServiceUsageTable
        packageServiceUsageEntry
        packageServiceUsageUpVolume
        packageServiceUsageDownVolume
        packageServiceUsageNumSessions
        packageServiceUsageDuration
        packageServiceUsageConcurrentSessions
        packageServiceUsageActiveSubscribers
        packageServiceUpDroppedPackets
        packageServiceDownDroppedPackets
        packageServiceUpDroppedBytes
        packageServiceDownDroppedBytes
subscriberGrp
subscribersTable
    subscriberEntry
        subscriberPackageIndex
        subscriberServiceUsageTable
        subscriberServiceUsageEntry
        subscriberServiceUsageUpVolume
        subscriberServiceUsageDownVolume
        subscriberServiceUsageNumSessions
        subscriberServiceUsageDuration
serviceCounterGrp
    globalScopeServiceCounterTable
        globalScopeServiceCounterEntry
        globalScopeServiceCounterIndex
        globalScopeServiceCounterStatus
        globalScopeServiceCounterName
subscriberScopeServiceCounterTable
    subscriberScopeServiceCounterEntry
        subscriberScopeServiceCounterIndex
        subscriberScopeServiceCounterStatus
        subscriberScopeServiceCounterName
```

Service Group: serviceGrp (pcubeEngageObjs 1)

The Service group is deprecated. Use the Service Counter group.

serviceTable (serviceGrp 1)

Deprecated—Use the tables in the Service Counter group.

Access	not accessible

Syntax

```
Counter32
```

Link Group: linkGrp (pcubeEngageObjs 2)

The Link Service group provides usage information per link for each global-scope service usage counter. For example, traffic statistics of a service for all subscribers using a particular link.

- linkServiceUsageTable (linkGrp 1), page 6-7
- linkServiceUsageEntry (linkServiceUsageTable 1), page 6-7
- linkServiceUsageUpVolume (linkServiceUsageEntry 1), page 6-8
- linkServiceUsageDownVolume (linkServiceUsageEntry 2), page 6-8
- linkServiceUsageNumSessions (linkServiceUsageEntry 3), page 6-8
- linkServiceUsageDuration (linkServiceUsageEntry 4), page 6-9
- linkServiceUsageConcurrentSessions (linkServiceUsageEntry 5), page 6-9
- linkServiceUsageActiveSubscribers (linkServiceUsageEntry 6), page 6-9
- linkServiceUpDroppedPackets (linkServiceUsageEntry 7), page 6-9
- linkServiceDownDroppedPackets (linkServiceUsageEntry 8), page 6-10
- linkServiceUpDroppedBytes (linkServiceUsageEntry 9), page 6-10
- linkServiceDownDroppedBytes (linkServiceUsageEntry 10), page 6-10

linkServiceUsageTable (linkGrp 1)

The Link Service Usage table provides usage information per link for each global-scope service usage counter.

Access	not accessible

Syntax

```
SEQUENCE OF linkServiceUsageEntry
```

linkServiceUsageEntry (linkServiceUsageTable 1)

A Link Service Usage table entry containing parameters defining resource usage of one link for services included in one global-scope service usage counter.

Access	not accessible

Index

```
{linkModuleIndex, linkIndex, globalScopeServiceCounterIndex}
```

Syntax

```
SEQUENCE{
linkServiceUsageUpVolume
linkServiceUsageDownVolume
linkServiceUsageNumSessions
linkServiceUsageDuration
linkServiceUsageConcurrentSessions
linkServiceUsageActiveSubscribers
linkServiceUpDroppedPackets
```

```
linkServiceDownDroppedPackets
linkServiceUpDroppedBytes
linkServiceDownDroppedBytes
}
```

linkServiceUsageUpVolume (linkServiceUsageEntry 1)

The upstream volume of services in this service usage counter carried over the link.

Access	read-only
Units	kilobytes

Syntax

```
Counter32
```

Note Although volume counters on the SCE platform hold 32-bit integers, CISCO-SCAS-BB MIB volume counters wraparound (turn back to zero) when the maximum 29-bit integer value (0x1FFFFFFF) is reached.

linkServiceUsageDownVolume (linkServiceUsageEntry 2)

The downstream volume of services in this service usage counter carried over the link.

Access	read-only
Units	kilobytes

Syntax

```
Counter32
```

Note Although volume counters on the SCE platform hold 32-bit integers, CISCO-SCAS-BB MIB volume counters wraparound (turn back to zero) when the maximum 29-bit integer value (0x1FFFFFFF) is reached.

linkServiceUsageNumSessions (linkServiceUsageEntry 3)

The number of sessions of services in this service usage counter carried over the link.

Access	read-only
Units	Sessions

Syntax

```
Counter32
```

linkServiceUsageDuration (linkServiceUsageEntry 4)

The aggregated session duration of services in this service usage counter carried over the link.

Access	read-only
Units	seconds

Syntax

`Counter32`

linkServiceUsageConcurrentSessions (linkServiceUsageEntry 5)

The number of concurrent sessions of services in this service usage counter carried over the link.

Access	read-only
Units	sessions

Syntax

`Counter32`

linkServiceUsageActiveSubscribers (linkServiceUsageEntry 6)

The number of active subscribers of services in this service usage counter carried over the link.

Access	read-only
Units	subscribers

Syntax

`Counter32`

linkServiceUpDroppedPackets (linkServiceUsageEntry 7)

The number of dropped upstream packets of services in this service usage counter carried over the link.

Access	read-only
Units	packets

Syntax

`Counter32`

Note To enable the SCE application to count dropped packets and dropped bytes, disable the accelerate-packet-drops feature on the SCE platform; if accelerate-packet-drops is enabled, the MIB dropped packets and dropped bytes counters constantly show the value 0xFFFFFFFF. For more information about the accelerate-packet-drops feature, see either the “Counting Dropped Packets”

section in the "Configuring the Line Interface" chapter of *Cisco SCE 8000 10GBE Software Configuration Guide* or the "Counting Dropped Packets" section in the "Configuring the Line Interface" chapter of *Cisco SCE 8000 GBE Software Configuration Guide*.

linkServiceDownDroppedPackets (linkServiceUsageEntry 8)

The number of dropped downstream packets of services in this service usage counter carried over the link.

Access	read-only
Units	packets

Syntax

```
Counter32
```

Note To enable the SCE application to count dropped packets and dropped bytes, disable the accelerate-packet-drops feature on the SCE platform; if accelerate-packet-drops is enabled, the MIB dropped packets and dropped bytes counters constantly show the value 0xFFFFFFFF. For more information about the accelerate-packet-drops feature, see either the "Counting Dropped Packets" section in the "Configuring the Line Interface" chapter of *Cisco SCE 8000 10GBE Software Configuration Guide* or the "Counting Dropped Packets" section in the "Configuring the Line Interface" chapter of *Cisco SCE 8000 GBE Software Configuration Guide*.

linkServiceUpDroppedBytes (linkServiceUsageEntry 9)

The number of dropped upstream bytes of services in this service usage counter carried over the link.

Access	read-only
Units	bytes

Syntax

```
Counter32
```

Note To enable the SCE application to count dropped packets and dropped bytes, disable the accelerate-packet-drops feature on the SCE platform; if accelerate-packet-drops is enabled, the MIB dropped packets and dropped bytes counters constantly show the value 0xFFFFFFFF. For more information about the accelerate-packet-drops feature, see either the "Counting Dropped Packets" section in the "Configuring the Line Interface" chapter of *Cisco SCE 8000 10GBE Software Configuration Guide* or the "Counting Dropped Packets" section in the "Configuring the Line Interface" chapter of *Cisco SCE 8000 GBE Software Configuration Guide*.

linkServiceDownDroppedBytes (linkServiceUsageEntry 10)

The link service-counter number of dropped downstream bytes of services in this service usage counter carried over the link.

Access	read-only
Units	bytes

Syntax

`Counter32`

Note To enable the SCE application to count dropped packets and dropped bytes, disable the accelerate-packet-drops feature on the SCE platform; if accelerate-packet-drops is enabled, the MIB dropped packets and dropped bytes counters constantly show the value 0xFFFFFFFF. For more information about the accelerate-packet-drops feature, see either the "Counting Dropped Packets" section in the "Configuring the Line Interface" chapter of *Cisco SCE 8000 10GBE Software Configuration Guide* or the "Counting Dropped Packets" section in the "Configuring the Line Interface" chapter of *Cisco SCE 8000 GBE Software Configuration Guide*.

Package Group: packageGrp (pcubeEngageObjs 3)

The Package group provides general and usage information for each global-scope package usage counter (for example, traffic statistics of a service for all subscribers assigned to a particular package or group of packages).

- packageCounterTable (packageGrp 1), page 6-11
- packageCounterEntry (packageCounterTable 1), page 6-12
- packageCounterIndex (packageCounterEntry 1), page 6-12
- packageCounterStatus (packageCounterEntry 2), page 6-12
- packageCounterName (packageCounterEntry 3), page 6-12
- packageCounterActiveSubscribers (packageCounterEntry 4), page 6-13
- packageServiceUsageTable (packageGrp 2), page 6-13
- packageServiceUsageEntry (packageServiceUsageTable 1), page 6-13
- packageServiceUsageUpVolume (packageServiceUsageEntry 1), page 6-14
- packageServiceUsageDownVolume (packageServiceUsageEntry 2), page 6-14
- packageServiceUsageNumSessions (packageServiceUsageEntry 3), page 6-14
- packageServiceUsageDuration (packageServiceUsageEntry 4), page 6-14
- packageServiceUsageConcurrentSessions (packageServiceUsageEntry 5), page 6-15
- packageServiceUsageActiveSubscribers (packageServiceUsageEntry 6), page 6-15
- packageServiceUpDroppedPackets (packageServiceUsageEntry 7), page 6-15
- packageServiceDownDroppedPackets (packageServiceUsageEntry 8), page 6-16
- packageServiceUpDroppedBytes (packageServiceUsageEntry 9), page 6-16
- packageServiceDownDroppedBytes (packageServiceUsageEntry 10), page 6-16

packageCounterTable (packageGrp 1)

The Package Counter table provides information for each package usage counter.

Access	nonaccessible

Syntax

```
SEQUENCE OF packageCounterEntry
```

packageCounterEntry (packageCounterTable 1)

A Package Counter table entry containing parameters defining one package usage counter.

Access	nonaccessible

Index

```
{pmoduleIndex, packageCounterIndex}
```

Syntax

```
SEQUENCE {
packageCounterIndex
packageCounterStatus
packageCounterName
packageCounterActiveSubscribers
}
```

packageCounterIndex (packageCounterEntry 1)

The package usage counter index.

Access	not accessible

Syntax

```
Integer32 (1...1023)
```

packageCounterStatus (packageCounterEntry 2)

The package usage counter status.

Access	read-only

Syntax

```
INTEGER {
0 (disabled)
1 (enabled)
}
```

packageCounterName (packageCounterEntry 3)

The name of the package usage counter.

Access	read-only

Syntax

```
SnmpAdminString
```

packageCounterActiveSubscribers (packageCounterEntry 4)

The total number of active subscribers of packages included in the package usage counter.

Access	read-only

Syntax

```
Counter32
```

packageServiceUsageTable (packageGrp 2)

The Package Service Usage table provides usage information for each global-scope package usage counter.

Access	not accessible

Syntax

```
SEQUENCE OF packageServiceUsageEntry
```

packageServiceUsageEntry (packageServiceUsageTable 1)

A Package Service Usage table entry containing parameters defining resource usage of packages included in one global-scope package usage counter.

Access	nonaccessible

Index

```
{pmoduleIndex, packageCounterIndex, globalScopeServiceCounterIndex}
```

Syntax

```
SEQUENCE {
packageServiceUsageUpVolume
packageServiceUsageDownVolume
packageServiceUsageNumSessions
packageServiceUsageDuration
packageServiceUsageConcurrentSessions
packageServiceUsageActiveSubscribers
packageServiceUpDroppedPackets
packageServiceDownDroppedPackets
packageServiceUpDroppedBytes
packageServiceDownDroppedBytes
}
```

packageServiceUsageUpVolume (packageServiceUsageEntry 1)

The upstream volume of packages in this package usage counter.

Access	read-only
Units	kilobytes

Syntax

```
Counter32
```

Note Although volume counters on the SCE platform hold 32-bit integers, CISCO-SCAS-BB MIB volume counters wraparound (turn back to zero) when the maximum 29-bit integer value (0x1FFFFFFF) is reached.

packageServiceUsageDownVolume (packageServiceUsageEntry 2)

The downstream volume of packages in this package usage counter.

Access	read-only
Units	kilobytes

Syntax

```
Counter32
```

Note Although volume counters on the SCE platform hold 32-bit integers, CISCO-SCAS-BB MIB volume counters wraparound (turn back to zero) when the maximum 29-bit integer value (0x1FFFFFFF) is reached.

packageServiceUsageNumSessions (packageServiceUsageEntry 3)

The number of sessions of packages in this package usage counter.

Access	read-only
Units	sessions

Syntax

```
Counter32
```

packageServiceUsageDuration (packageServiceUsageEntry 4)

The aggregated session duration seconds of packages in this package usage counter.

Access	read-only
Units	seconds

Syntax

`Counter32`

packageServiceUsageConcurrentSessions (packageServiceUsageEntry 5)

The number of concurrent sessions of packages in this package usage counter.

Access	read-only
Units	sessions

Syntax

`Counter32`

packageServiceUsageActiveSubscribers (packageServiceUsageEntry 6)

The number of active subscribers of packages in this package usage counter.

Access	read-only
Units	subscribers

Syntax

`Counter32`

packageServiceUpDroppedPackets (packageServiceUsageEntry 7)

The number of dropped upstream packets of packages in this package usage counter.

Access	read-only
Units	packets

Syntax

`Counter32`

Note To enable the SCE application to count dropped packets and dropped bytes, disable the accelerate-packet-drops feature on the SCE platform; if accelerate-packet-drops is enabled, the MIB dropped packets and dropped bytes counters constantly show the value 0xFFFFFFFF. For more information about the accelerate-packet-drops feature, see either the “Counting Dropped Packets”

section in the "Configuring the Line Interface" chapter of *Cisco SCE 8000 10GBE Software Configuration Guide* or the "Counting Dropped Packets" section in the "Configuring the Line Interface" chapter of *Cisco SCE 8000 GBE Software Configuration Guide*.

packageServiceDownDroppedPackets (packageServiceUsageEntry 8)

The number of dropped downstream packets of packages in this package usage counter.

Access	read-only
Units	packets

Syntax

```
Counter32
```

Note To enable the SCE application to count dropped packets and dropped bytes, disable the accelerate-packet-drops feature on the SCE platform; if accelerate-packet-drops is enabled, the MIB dropped packets and dropped bytes counters constantly show the value 0xFFFFFFFF. For more information about the accelerate-packet-drops feature, see either the "Counting Dropped Packets" section in the "Configuring the Line Interface" chapter of *Cisco SCE 8000 10GBE Software Configuration Guide* or the "Counting Dropped Packets" section in the "Configuring the Line Interface" chapter of *Cisco SCE 8000 GBE Software Configuration Guide*.

packageServiceUpDroppedBytes (packageServiceUsageEntry 9)

The number of dropped upstream bytes of packages in this package usage counter.

Access	read-only
Units	bytes

Syntax

```
Counter32
```

Note To enable the SCE application to count dropped packets and dropped bytes, disable the accelerate-packet-drops feature on the SCE platform; if accelerate-packet-drops is enabled, the MIB dropped packets and dropped bytes counters constantly show the value 0xFFFFFFFF. For more information about the accelerate-packet-drops feature, see either the "Counting Dropped Packets" section in the "Configuring the Line Interface" chapter of *Cisco SCE 8000 10GBE Software Configuration Guide* or the "Counting Dropped Packets" section in the "Configuring the Line Interface" chapter of *Cisco SCE 8000 GBE Software Configuration Guide*.

packageServiceDownDroppedBytes (packageServiceUsageEntry 10)

The number of dropped downstream bytes of packages in this package usage counter.

Access	read-only
Units	bytes

Syntax

`Counter32`

Note To enable the SCE application to count dropped packets and dropped bytes, disable the accelerate-packet-drops feature on the SCE platform; if accelerate-packet-drops is enabled, the MIB dropped packets and dropped bytes counters constantly show the value 0xFFFFFFFF. For more information about the accelerate-packet-drops feature, see either the "Counting Dropped Packets" section in the "Configuring the Line Interface" chapter of *Cisco SCE 8000 10GBE Software Configuration Guide* or the "Counting Dropped Packets" section in the "Configuring the Line Interface" chapter of *Cisco SCE 8000 GBE Software Configuration Guide*.

Subscriber Group: subscriberGrp (pcubeEngageObjs 4)

The Subscriber group provides general information for each subscriber and usage information per service usage counter for each subscriber (for example, traffic statistics of a service for a particular subscriber defined in the system).

Note **For the SCE 8000:** To use the tables in this group, first create an entry to reference a particular subscriber in the cServiceControlSubscribersTable object of the CISCO-SERVICE-CONTROL-SUBSCRIBERS MIB (not the CISCO-SCAS-BB MIB). Using the index of this table (cServiceControlSubscribersIndex), information about the subscriber can be collected.

Note **For the SCE 2000:** To use the tables in this group, first create an entry to reference a particular subscriber in the subscribersPropertiesValueTable object of the subscriberGrp in the SCE MIB (not the CISCO-SCAS-BB MIB). Using the index of this table (spvIndex), information about the subscriber can be collected.

- subscribersTable (subscriberGrp 1), page 6-17
- subscribersEntry (subscribersTable 1), page 6-18
- subscriberPackageIndex (subscribersEntry 1), page 6-18
- subscriberServiceUsageTable (subscriberGrp 2), page 6-18
- subscriberServiceUsageEntry (subscriberServiceUsageTable 1), page 6-18
- subscriberServiceUsageEntry (subscriberServiceUsageTable 1), page 6-19
- subscriberServiceUsageDownVolume (subscriberServiceUsageEntry 2), page 6-19
- subscriberServiceUsageNumSessions (subscriberServiceUsageEntry 3), page 6-19
- subscriberServiceUsageDuration (subscriberServiceUsageEntry 4), page 6-20

Related Topics

- Accessing Subscriber Information (the spvIndex), page 6-24

subscribersTable (subscriberGrp 1)

The Subscribers Table provides information for each subscriber.

Access	not accessible

Syntax

```
SEQUENCE OF subscribersEntry
```

subscribersEntry (subscribersTable 1)

A Subscribers Table entry containing the package index of each subscriber.

Access	not accessible

Index

```
{pmoduleIndex, spvIndex}
```

Syntax

```
SEQUENCE {
subscriberPackageIndex
}
```

subscriberPackageIndex (subscribersEntry 1)

The index of the subscriber package.

Access	read-only

Syntax

```
Integer32 (1...255)
```

subscriberServiceUsageTable (subscriberGrp 2)

The Subscriber Service Usage table provides usage information per service usage counter for each subscriber.

Access	not accessible

Syntax

```
Sequence of subscriberServiceUsageEntry
```

subscriberServiceUsageEntry (subscriberServiceUsageTable 1)

A Subscriber Service Usage table entry containing parameters defining resource usage by one subscriber of services included in one service usage counter.

Access	not accessible

Index

```
{pmoduleIndex, spvIndex, subscriberScopeServiceCounterIndex}
```

Syntax

```
SEQUENCE {
subscriberServiceUsageUpVolume
subscriberServiceUsageDownVolume
subscriberServiceUsageNumSessions
subscriberServiceUsageDuration
```

subscriberServiceUsageEntry (subscriberServiceUsageTable 1)

A Subscriber Service Usage table entry containing parameters defining resource usage by one subscriber of services included in one service usage counter.

Access	not accessible

Index

```
{pmoduleIndex, spvIndex, subscriberScopeServiceCounterIndex}
```

Syntax

```
SEQUENCE {
subscriberServiceUsageUpVolume
subscriberServiceUsageDownVolume
subscriberServiceUsageNumSessions
subscriberServiceUsageDuration
```

subscriberServiceUsageDownVolume (subscriberServiceUsageEntry 2)

The downstream volume of services in this service usage counter used by this subscriber.

Access	read-only
Units	kilobytes

Syntax

```
Counter32
```

Note Although volume counters on the SCE platform hold 32-bit integers, CISCO-SCAS-BB MIB volume counters wraparound (turn back to zero) when the maximum 29-bit integer value (0x1FFFFFFF) is reached.

subscriberServiceUsageNumSessions (subscriberServiceUsageEntry 3)

The number of sessions of services in this service usage counter used by this subscriber.

Access	read-only
Units	sessions

Syntax

```
Integer32 (1...65535)
```

subscriberServiceUsageDuration (subscriberServiceUsageEntry 4)

Aggregated session duration of services in this service usage counter used by this subscriber.

Access	read-only
Units	seconds

Syntax

```
Integer32 (1...65535)
```

Service Counter Group: serviceCounterGrp (pcubeEngageObjs 5)

The Service Counter group provides general information for each global-scope and subscriber-scope service usage counter. You can use it, for example, to read the names of the services as defined in a Cisco SCA BB service configuration.

- globalScopeServiceCounterTable (serviceCounterGrp 1), page 6-20
- globalScopeServiceCounterEntry (globalScopeServiceCounterTable 1), page 6-20
- globalScopeServiceCounterIndex (globalScopeServiceCounterEntry 1), page 6-21
- globalScopeServiceCounterStatus (globalScopeServiceCounterEntry 2), page 6-21
- globalScopeServiceCounterName (globalScopeServiceCounterEntry 3), page 6-21
- subscriberScopeServiceCounterTable (serviceCounterGrp 2), page 6-21
- subscriberScopeServiceCounterEntry (subscriberScopeServiceCounterTable 1), page 6-22
- subscriberScopeServiceCounterIndex (subscriberScopeServiceCounterEntry 1), page 6-22
- subscriberScopeServiceCounterStatus (subscriberScopeServiceCounterEntry 2), page 6-22
- subscriberScopeServiceCounterName (subscriberScopeServiceCounterEntry 3), page 6-22

globalScopeServiceCounterTable (serviceCounterGrp 1)

The Global-Scope Service Counter table consists of data about each service usage counter used by the link and by packages.

Access	nonaccessible

Syntax

```
SEQUENCE OF globalScopeServiceCounterEntry
```

globalScopeServiceCounterEntry (globalScopeServiceCounterTable 1)

A Global-Scope Service Counter table entry containing parameters defining one global-scope service usage counter.

Access	not accessible

Index

```
{pmoduleIndex, globalScopeServiceCounterIndex}
```

Syntax

```
SEQUENCE {
globalScopeServiceCounterIndex
globalScopeServiceCounterStatus
globalScopeServiceCounterName
}
```

globalScopeServiceCounterIndex (globalScopeServiceCounterEntry 1)

The global-scope service usage counter index.

Access	not accessible

Syntax

```
Integer32 (1...255)
```

globalScopeServiceCounterStatus (globalScopeServiceCounterEntry 2)

The global-scope service usage counter status.

Access	read-only

Syntax

```
INTEGER {
0 (disabled)
1 (enabled)
}
```

globalScopeServiceCounterName (globalScopeServiceCounterEntry 3)

The name of the global-scope service usage counter.

Access	read-only

Syntax

```
SnmpAdminString
```

subscriberScopeServiceCounterTable (serviceCounterGrp 2)

The Subscriber-Scope Service Counter table consists of data about each service usage counter used by subscribers.

Access	not accessible

Syntax

```
SEQUENCE OF subscriberScopeServiceCounterEntry
```

subscriberScopeServiceCounterEntry (subscriberScopeServiceCounterTable 1)

A Subscriber-Scope Service Counter table entry containing parameters defining one subscriber-scope service usage counter.

Access	not accessible

Index

```
{pmoduleIndex, subscriberScopeServiceCounterIndex}
```

Syntax

```
SEQUENCE {
subscriberScopeServiceCounterIndex
subscriberScopeServiceCounterStatus
subscriberScopeServiceCounterName
}
```

subscriberScopeServiceCounterIndex (subscriberScopeServiceCounterEntry 1)

The subscriber-scope service usage counter index.

Access	not accessible

Syntax

```
Integer32 (1...255)
```

subscriberScopeServiceCounterStatus (subscriberScopeServiceCounterEntry 2)

The subscriber-scope service usage counter status.

Access	read-only

Syntax

```
INTEGER {
0 (disabled)
1 (enabled)
}
```

subscriberScopeServiceCounterName (subscriberScopeServiceCounterEntry 3)

The name of the subscriber-scope service usage counter.

Access	read-only

Syntax

`SnmpAdminString`

Guidelines for Using the CISCO-SCAS-BB MIB

This section provides guidelines to help access SNMP information about the SCE platform using the CISCO-SCAS-BB MIB.

- globalScopeServiceCounterTable and subscriberScopeServiceCounterTable, page 6-23
- packageCounterTable, page 6-24
- Accessing Subscriber Information (the spvIndex), page 6-24

Note Indices in SNMP start from 1; Cisco SCA BB indices start from 0. When accessing a counter in the Cisco SCA BB SNMP MIB by its index, add 1 to the index of the entity. For example, the global usage counter with index 0 is located at globalScopeServiceCounter index 1.

Note Although volume counters on the SCE platform hold 32-bit integers, CISCO-SCAS-BB MIB volume counters wraparound (turn back to zero) when the maximum 29-bit integer value (0x1FFFFFFF) is reached.

Note To enable the SCE application to count dropped packets and dropped bytes, disable the accelerate-packet-drops feature on the SCE platform; if accelerate-packet-drops is enabled, the MIB dropped packets and dropped bytes counters constantly show the value 0xFFFFFFFF. For more information about the accelerate-packet-drops feature, see either the “Counting Dropped Packets” section in the “Configuring the Line Interface” chapter of *Cisco SCE 8000 10GBE Software Configuration Guide* or the “Counting Dropped Packets” section in the “Configuring the Line Interface” chapter of *Cisco SCE 8000 GBE Software Configuration Guide*.

globalScopeServiceCounterTable and subscriberScopeServiceCounterTable

The index of a service usage counter as defined in a Cisco SCA BB service configuration is used to reference services in the CISCO-SCAS-BB MIB. Because MIB index values count from 1, but Cisco SCA BB indices count from 0, the index used in the MIB must always be one greater than the index of the service it is referencing.

For example, to get the number of upstream bytes used by a service on a link, use LinkServiceTable.lnkServiceUpVolume (part of the linkGrp). The value assigned to serviceIndex for this table must be one greater than service index defined for this service in the service configuration.

To identify or change the index of a service, go to the Advanced tab of the Service Settings dialog box in the Cisco SCA BB Console (see the "Using the Service Configuration Editor: Traffic Classification" chapter of *Cisco Service Control Application for Broadband User Guide*). For example, to reference the P2P service (which has a [default] service index of 9) in the MIB, a serviceIndex of 10 (= 9 + 1) must be used.

packageCounterTable

The package index, defined in a Cisco SCA BB service configuration, is used to reference entries in packageTable and packageServiceTable (part of the packageGrp). As with serviceIndex, the value assigned to packageIndex must be one greater than the package index in the service configuration.

To identify or change the index of a package, go to the Advanced tab of the Package Settings dialog box in the Cisco SCA BB Console (see the "Using the Service Configuration Editor: Traffic Classification" chapter of *Cisco Service Control Application for Broadband User Guide*). For example, to reference the default package (which has a package index of 0) in the MIB, a packageIndex of 1 (= 0 + 1) must be used.

Accessing Subscriber Information (the spvIndex)

To collect subscriber-level information using the SNMP interface, you must first create an entry in the proper subscriber MIB table and associate this entry with a subscriber name. Its index can then be referred to collect usage statistics for this subscriber.

The exact MIB objects vary, depending on the particular SCE platform, as described in the following sections.

Accessing Subscriber Information in Cisco SCE 2000

Create an entry in the subscriberPropertiesValuesTable part of the subscriberGrp in *pcubeSEMib* (not *PCubeEngageMib*). After an entry in this table is created and associated with a subscriber name, its index (spvIndex) can be referred to in *PCubeEngageMib* to collect usage statistics for this subscriber.

An entry is created in the subscriberPropertiesValuesTable by setting the entry spvRowStatus object with CreateAndGo(4), and then setting the name of the subscriber in the spvSubName property and the *spvIndex* variable to be used as an index to the subscriber.

For example, to poll the downstream volume of subscriber "sub123" for the P2P service using PCubeEngageMib, perform the following steps.

Step 1 Obtain the index of the P2P service from the Cisco SCA BB Console (this is a one-time operation that you should perform only if services are changed in the policy). In this example, assume that the P2P service index has its default value of 9.

Step 2 To create a subscriber entry, you must specify the index of the module and the desired *spvIndex* .

- Set pmoduleIndex = 1.
- In SEMib:subscriberGrp:subscriberPropertiesValuesTable, choose an index for spvIndex (for this example, arbitrarily choose index 7).

Step 3 Create an entry in SEMib:subscriberGrp:subscriberPropertiesValuesTable, at the index that you have chosen:

- Set *spvRowStatus* to 4 (using CreateAndGo).

- Set *spvSubName* to “sub123”.

Step 4 Read the subscriberServiceDownVolume property out of EngageMib:subscriberGrp:subscriberServiceTable where *spvIndex* is set to 7 and *serviceIndex* is set to 10. (In general, you may walk the cServiceControlSubscribersTable to find out the various subscriber indexes, but in this case, we have chosen it to be 7, so that we can directly use the same index for accessing the data of this subscriber).

Accessing Subscriber Information in Cisco SCE 8000

Create an entry in the cServiceControlSubscribersTable of the CISCO-SERVICE-CONTROL-SUBSCRIBERS MIB. After an entry in this table is created and associated with a subscriber name, its index (cServiceControlSubscribersIndex) can be referred to in PCubeEngageMib (as spvIndex) to collect usage statistics for this subscriber.

An entry is created in the cServiceControlSubscribersTable table (at an index chosen by the user) by setting the entry cServiceControlSubscribersRowStatus object with CreateAndGo(4), then setting the name of the subscriber in the cServiceControlSubscribersName property.

For example, to poll the downstream volume of subscriber “sub123” for the P2P service by using PCubeEngageMib, perform the following steps.

Step 1 Obtain the index of the P2P service from the Cisco SCA BB Console (this is a one-time operation that you should perform only if services are changed in the policy). In this example, assume that the P2P service index has its default value of 9.

Step 2 To create a subscriber entry, you must specify the indexes of the module and the desired cServiceControlSubscribersIndex.

- Set entPhyIndex according to the index of the Service Control Module (SCM) entry in the Entity MIB.
- Choose an index for cServiceControlSubscribersIndex (for this example, arbitrarily choose index 7).

Step 3 Create an entry in ciscoServiceControlSubscribersMIB:cServiceControlSubscribersTable, at the index that you have chosen:

- Set cServiceControlSubscribersRowStatus to 4 (using CreateAndGo).
- Set cServiceControlSubscribersName to “sub123”.

Step 4 Read the subscriberServiceUsageDownVolume property out of EngageMib:subscriberGrp:subscriberServiceUsageTable, where entPhyIndex is set as instructed, spvIndex is set to 7, and serviceIndex is set to 10. (In general, you may walk the cServiceControlSubscribersTable to find out the various subscriber indexes, but in this case we have chosen it to be 7, so that we can directly use the same index for accessing the data of this subscriber).