Raw Data Records: Formats and Field Contents

Revised: March 06, 2015

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

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 2-149.
- 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 2-149.
- 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 2-149

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
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
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-SESSION-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 10000. 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

HTTPS Transaction Usage RDR

The HTTPS_TRANSACTION_USAGE_RDR is a TUR specifically used for HTTPS transactions.

- RDR Purpose—Log HTTPS 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 HTTPS transaction; its connection attributes, extracted Layer 7 attributes, duration, and volume.
- RDR Generation Logic—Generated at the end of an HTTPS 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—0xf0f0f43B / 4042323003

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 HTTPS Transaction Usage RDR fields and their descriptions.

Table 2-7 HTTPS 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.	17 [HTTPS]

Table 2-7 HTTPS 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.	358 [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	EMPTY STRING.	
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 2-7 HTTPS 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.	0x0A010000 [HTTPS]
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

Related Topics

- Universal RDR Fields, page 2-4

Anonymized HTTPS Transaction Usage RDR

The ANONYMIZED_HTTPS_TRANSACTION_USAGE_RDR is a TUR specifically used for HTTPS transactions.

- RDR Purpose—Log HTTPS 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 HTTPS transaction; its connection attributes, extracted Layer 7 attributes, duration, and volume.
- RDR Generation Logic—Generated at the end of an HTTPS 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—0xf0f0f53B / 4042323259

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 2-8 lists the Anonymized HTTPS Transaction Usage RDR fields and their descriptions.

Table 2-8 Anonymized HTTPS Transaction Usage RDR Fields

RDR Field Name	Type	Description	Example value
HASHED_SUBSCRIBER_ID	STRING	Subscriber identification string, may be passed through hashing algorithm.	john
PACKAGE_ID	INT16	ID of the package assigned to the subscriber whose traffic is being reported.	0 [Default Package]
SERVICE_ID	INT32	Service classification of the reported session.	17 [HTTPS]
PROTOCOL_ID	INT16	Unique ID of the protocol associated with the reported session.	358 [HTTP]
SKIPPED_SESSIONS	UINT32	Always 1.	1 [SESSION_END]
SERVER_IP	UINT32	HTTPS server IP. 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 networking session.	80

Table 2-8 Anonymized HTTPS Transaction Usage 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	EMPTY STRING	
CLIENT_IP	UINT32	HTTPS client IP. 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 networking session.	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.	—
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 stream 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

Table 2-8 Anonymized HTTPS Transaction Usage RDR Fields (continued)

RDR Field Name	Type	Description	Example value
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	UINT32	ID of the protocol signature associated with this session.	0x0A010000 [HTTPS]
ZONE_ID	UINT32	ID of the zone associated with this session.	0
FLAVOR_ID	UINT32	ID of the flavor associated with this session.	0
FLOW_CLOSE_MODE	UINT8	Reason for the end of flow.	0

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

Table 2-9 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 2-9 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 2-9 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

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 2-10 lists the Anonymized RTSP Transaction Usage RDR fields and their descriptions.

Table 2-10 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 2-10 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 2-10 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 2-10 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 2-36

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

Table 2-11 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 2-11 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 2-11 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 47)	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 47)	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 47)	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 47)	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 2-11 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 2-48

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 2-12 lists the Anonymized VoIP Transaction Usage RDR fields and their descriptions.

Table 2-12 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 2-12 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 2-12 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 47)	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 47)	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 47)	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 47)	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 2-12 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 2-44

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 2-13 lists the VIDEO_TRANSACTION_USAGE_RDR fields and their descriptions.

Table 2-13 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 2-13 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 2-13 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 2-13 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 2-13 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 10000. 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 2-14 lists the Anonymized Video Transaction Usage RDR fields and their descriptions.

Table 2-14 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 2-14 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 2-14 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 2-14 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 2-14 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-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 10000. 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 2-15 lists the Generic Usage RDR fields and their descriptions.

Table 2-15 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	It is always an empty string. After the support of IPv6 usage from 3.7.5 in other RDRs, support for subscriber identification string is not provided in this RDR. In earlier versions before 3.7.5 this may be always empty string as IPv6/IPv6 tunneled traffic may be tagged under unknown subscribers.
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.

Table 2-15 Generic Usage RDR Fields (continued)

Key/Data	RDR Field Name	Type	Description
Key	SIGNATURE_ID	INT32	ID of the protocol signature associated with this session.
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 2-15 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 2-16 describes the specific fields of the pure-IPv6 and tunneled-IPv6 reports. (Any GUR fields not listed in the table are not used.)

Table 2-16 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 2-17 lists the Subscriber Usage RDR fields and their descriptions.

Table 2-17 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 2-17 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 2-17 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 10000. 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 2-156

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 2-156). 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 2-18 lists the Real-Time Subscriber Usage RDR fields and their descriptions.

Table 2-18 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 2-18 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 2-156

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 2-156). 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 2-19 lists the Link Usage RDR fields and their descriptions.

Table 2-19 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 10000** 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.
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.

Table 2-19 Link Usage RDR Fields (continued)

RDR Field Name	Type	Description
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 2-156

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 2-156). 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 2-20 lists the Zone Usage RDR fields and their descriptions.

Table 2-20 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 2-156

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 2-156). 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 2-21 lists the Package Usage RDR fields and their descriptions.

Table 2-21 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 2-21 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 2-156

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 2-156). 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 2-22 lists the Virtual Links Usage RDR fields and their descriptions.

Table 2-22 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 2-22 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 2-156

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

Table 2-23 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 2-23 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	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

- Block Reason (uint8), page 2-149
- Anonymized Blocking RDR, page 2-88

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 2-24 lists the Anonymized Blocking RDR fields and their descriptions.

Table 2-24 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 2-24 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 2-149
- Blocking RDR, page 2-86

Redirection History RDR

The REDIRECTION_HISTORY_RDR is generated whenever a redirection happens for a subscriber on breaching the quota and the redirection information is sent from Cisco SCOS to the Subscriber Manager (SM). The redirection information is stored in the Subscriber Manager database.

When next pull request or push login is received, the SM sends the buckets details that are already redirected to SCOS as part of the login (new native API call). After login operation, SCOS updates the redirected information sent as part of the login and avoids redirecting for those buckets. When new quota is updated or replenished for subscribers or package switch happens, SCOS sends a Redirection History RDR to SM with reset details. When SM receives the RDR, it updates the latest value received with the existing value. When subscriber is removed from SM, redirection information is also removed.

The following pre-configuration are required to enable the “Flexible redirection across login” feature:

- Apply PQB
- Change the redirection history RDR from Category -1 to Category - 3 (as Subscriber Manager receives Category-3 RDR only)

```
SCE8000#>conf
SCE8000(config)#>rdr-formatter rdr-mapping tag-ID 0xf0f0f061 category-number 3
SCE8000(config)#>no rdr-formatter rdr-mapping tag-ID 0xf0f0f061 category-number 1
```

- Configure the RDR-formatter

```
SCE8000#>configure
SCE8000(config)#>RDR-formatter forwarding-mode multicast
SCE8000(config)#>RDR-formatter destination [SM-IP Address] port 33145 category number
3 priority 100
```

Note The default port number for redirection is 33145. If you want to change the port number other than the default port number, you need to change the port number both on the Subscriber Manager side and RDR-formatter side.

Note One subscriber can have up to 128 profiles redirected.

In redirection section, the following two parameters will be added in p3sm.cfg file of Subscriber Manager:

- enable—This parameter is used to enable the Profile Redirection Feature. The values are yes/no.
- redirection_rdr_port—This parameter validates the port number. The default value is 33145.

Sample Configuration

```
    #The following parameters define Profile Redirection feature options
    [Redirection]
    #To enable Profile Redirection Feature this should be used. By default no.
    enable=no
    #The port on which redirect rdr server to be run. By default 33145
redirection_rdr_port=33145
```

The RDR tag of the REDIRECTION_HISTORY_RDR is 4042322017 (0xf0f0f061).

Table 2-23 lists the Redirection History RDR fields and their descriptions.

Table 2-25 Redirection History 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.
Redirection history bits(96-127)	Uint32	Redirection history bit numbers corresponding to redirection profile ID.
Redirection history bits(64-95)	Uint32	Redirection history bit numbers corresponding to redirection profile ID.
Redirection history bits(32-63)	Uint32	Redirection history bit numbers corresponding to redirection profile ID.
Redirection history bits(0-31)	Uint32	Redirection history bit numbers corresponding to redirection profile ID.
Reason	Uint8	0-Redirection History on Quota breach 1-Redirection History Reset on EOD 2-Redirection History Reset on EOW 3-Redirection History Reset on EOM 4-Redirection History Reset on Package Switch 5-Redirection History Reset on Quota top up
ADD_ON_PACKAGE_ID	STRING	ID of the base package assigned to the subscriber followed by ID's of the add-on packages. Example: 1000,2,3 1000—Base Package 2—Add-on Package1 3—Add-on Package2

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

Table 2-26 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 2-26 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. This unit is represented in Kbytes.

Table 2-26 Quota Breach RDR Fields (continued)

RDR Field Name	Type	Description
UNIT_AMOUNT_OUT	UINT32	Consumed upstream volume in volume units. This unit is represented in Kbytes. 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. This unit is represented in Kbytes. 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. This unit is represented in Kbytes.
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.
ADD_ON_PACKAGE_ID	STRING	ID of the base package assigned to the subscriber followed by ID's of the add-on packages. Example: 1000,2,3 1000—Base Package 2—Add-on Package1 3—Add-on Package2

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 2-27 lists the Quota Status RDR fields and descriptions.

Table 2-27 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 2-27 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 2-27 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
UNIT_AMOUNT_IN	UINT32	Consumed volume in volume units/ Seconds/ Sessions. For Gy quota model—downstream volume.

Table 2-27 Quota Status RDR Fields (continued)

RDR Field Name	Type	Description
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).
ADD_ON_PACKAGE_ID	STRING	ID of the base package assigned to the subscriber followed by ID's of the add-on packages. Example: 1000,2,3 1000—Base Package 2—Add-on Package1 3—Add-on Package2

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 2-28 lists the Quota Threshold Breach RDR fields and their descriptions.

Table 2-28 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.
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 2-28 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 2-28 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.
ADD_ON_PACKAGE_ID	STRING	ID of the base package assigned to the subscriber followed by ID's of the add-on packages. Example: 1000,2,3 1000—Base Package 2—Add-on Package1 3—Add-on Package2

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 2-29 lists the Session Creation RDR fields and their descriptions.

Table 2-29 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.
UNIT_AMOUNT_IN	UINT32	Not used.

Table 2-29 Session Creation RDR Fields (continued)

RDR Field Name	Type	Description
UNIT_AMOUNT_OUT	UINT32	Not used.
ADD_ON_PACKAGE_ID	STRING	ID of the base package assigned to the subscriber followed by ID's of the add-on packages. Example: 1000,2,3 1000—Base Package 2—Add-on Package1 3—Add-on Package2

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 2-30 lists the DHCP RDR fields and descriptions.

Table 2-30 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 2-31 lists the DHCPv6 RDR fields and descriptions.

Table 2-31 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 2-31 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 2-32 lists the RADIUS RDR fields and descriptions.

Table 2-32 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 2-33 lists the Flow Start RDR fields and their descriptions.

Table 2-33 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 2-33 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 2-34 lists the Anonymized Flow Start RDR fields and their descriptions.

Table 2-34 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 2-34 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 2-35 lists the Flow End RDR fields and their descriptions.

Table 2-35 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 2-35 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 2-36 lists the Anonymized Flow End RDR fields and their descriptions.

Table 2-36 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 2-36 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 2-37 lists the Flow Ongoing RDR fields and their descriptions.

Table 2-37 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 2-37 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 2-38 lists the Anonymized Flow Ongoing RDR fields and their descriptions.

Table 2-38 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 2-38 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 2-39 lists the Media Flow RDR fields and their descriptions.

Table 2-39 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 2-39 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 2-39 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 2-39 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 2-39 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 2-39 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 2-39 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 2-39 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 2-40 lists the Anonymized Media Flow RDR fields and their descriptions.

Table 2-40 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 2-40 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 2-40 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 2-40 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 2-40 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 2-40 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 2-40 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 2-40 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 2-41 lists the Attack Start RDR fields and their descriptions.

Table 2-41 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.
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.

Table 2-41 Attack Start 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.
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.

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 2-42 lists the Attack End RDR fields and their descriptions.

Table 2-42 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.
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.

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 2-43 lists the Malicious Traffic Periodic RDR fields and their descriptions.

Table 2-43 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 2-43 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 2-44 lists the Spam RDR fields and their descriptions.

Table 2-44 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 2-44 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 2-44 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 2-146

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 2-45 lists the Anonymized Spam RDR fields and their descriptions.

Table 2-45 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 2-45 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 2-45 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 2-143

Information About RDR Enumeration Fields

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

Block Reason (uint8)

The BLOCK_REASON field is a bit field. Table 2-46 lists the meanings of the bits of this field.

Table 2-46 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 2-47 lists the ACCESS_STRING and INFO_STRING field values.

Table 2-47 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 2-47 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 2-47 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 2-48 lists the AGG_PERIOD field values.

Table 2-48 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 2-49 lists the FLOW_CLOSE_MODE field values.

Table 2-49 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 2-50 lists the TIME_FRAME field values.

Table 2-50 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 2-51 summarizes RDR tag assignments.

Table 2-51 RDR Tag Assignments

RDR Name	Default Category (see Table 2-52)	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 2-51 RDR Tag Assignments (continued)

RDR Name	Default Category (see Table 2-52)	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" chapter of *Cisco SCE 10000 Software Configuration Guide*.

Table 2-52 summarizes the RDR tag default categories.

Table 2-52 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.