CHAPTER 3

NetFlow Records: Formats and Field Contents

Revised: October 21, 2011, OL-21066-04

Introduction

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

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

- Using the Generic Usage RDR to Report IPv6 Usage, page 2-29 (NUR)
- Package Usage RDR, page 2-41 (PUR)
- Link Usage RDR, page 2-36 (LUR)
- NetFlow, page 3-1
- NetFlow Field Types, page 3-2

NetFlow

- The Cisco Service Control Application for Broadband (SCA BB) supports NetFlow v9.
- For more information about NetFlow, see: RFC 3954.

NetFlow Field Types

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

Table 3-1 NetFlow Fields

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

Table 3-1 NetFlow Fields (continued)

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

Table 3-1 NetFlow Fields (continued)

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

Table 3-1 NetFlow Fields (continued)

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