



# APPENDIX **C**

## NetFlow Records: Formats and Field Contents

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

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

- User Usage RDR (NUR)
- Policy Usage RDR (PUR)
- Link Usage RDR (LUR)

### NetFlow

- The Cisco Network Module Enhanced Application Support module supports NetFlow v5 and v9.
- For more information about NetFlow, refer to:
  - [RFC 3954](#)

### NetFlow Field Types

[Table C-1](#) lists the possible fields in a NetFlow record and their descriptions.

**Table C-1** NetFlow Fields

Field Type	Value	Length (Bytes)	Description
scTag	32769	4	
scTrafficProcessorId	32770	1	
scSourceIpSample	32771	1	
scDestinationIpSample	32772	1	
scFlowContextId	32773	4	
scSubscriberId	32774	64	The user identification string, introduced through the user management interfaces. For an unknown user this field may contain an empty string. The string is padded with zeros.
scPackageId	32775	4	The ID of the service configuration profile assigned to the user.

Table C-1 NetFlow Fields (continued)

Field Type	Value	Length (Bytes)	Description
scServiceId	32776	4	The service classification of the reported session.
scProtocolId	32777	2	The 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.
scSkippedSessions	32778	4	The number of unreported sessions since the previous reporting record of this kind.
scInitiatingSide	32779	1	The initiating side of the transaction: <ul style="list-style-type: none"> <li>• 0—User side</li> <li>• 1—Network side</li> </ul>
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.
scTransactionDurationMillisec	32781	4	Duration, in milliseconds, of the transaction reported in this reporting record.
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.
scSessionUpstreamVolume	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.
scSessionDownstreamVolume	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	The ID of the protocol signature associated with this session
scZoneId	32786	4	The ID of the zone associated with this session
scFlavorId	32787	4	For protocol signatures that have flavors, this field contains the ID of the flavor associated with this session.
scFlowCloseMode	32788	1	The reason for the end of the flow.
scAccessString	32789	128, 256, 512, 1024	A Layer 7 property, extracted from the transaction.
scInfoString	32790	128, 256, 512, 1024	A Layer 7 property, extracted from the transaction.
scClientPort	32791	2	
scServerPort	32792	2	

Table C-1 NetFlow Fields (continued)

Field Type	Value	Length (Bytes)	Description
scSubscriberCounterId	32793	2	
scServiceUsageCounterId	32794	2	
scBreachState	32795	1	Indicates whether the user's quota was breached: <ul style="list-style-type: none"> <li>• 0—The quota was not breached</li> <li>• 1—The quota was breached</li> </ul>
scReason	32796	1	The reason that the reporting record was generated: <ul style="list-style-type: none"> <li>• 0—Periodic record</li> <li>• 1—User logout</li> <li>• 2—Policy switch</li> <li>• 3—Wraparound</li> <li>• 4—End of aggregation period</li> </ul>
scConfiguredDuration	32797	4	Configured period, in seconds, between successive reporting records.
scDuration	32798	4	The 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	Each policy is mapped to a counter. There are 64 policy usage counters.
scGeneratorId	32805	1	A numeric value identifying the processor generating the reporting record.
scServiceGlobalCounterId	32806	2	Each service is mapped to a counter. There 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 users using the reported service when this reporting record was generated.
scTotalActiveSubscribers	32809	4	Concurrent number of users in the system when this reporting record was generated.

Table C-1 NetFlow Fields (continued)

Field Type	Value	Length (Bytes)	Description
scLinkId	32810	1	A numeric value associated with the reported network link: <ul style="list-style-type: none"> <li>• 0—Physical link 1</li> <li>• 1—Physical link 2</li> </ul>
	32811-32818		Reserved
scAttackId	32819	4	Unique attack ID.
scAttackIp	32820	4	The IP address related to this attack.
scAttackOtherIp	32821	4	The other IP address related to this attack if it exists, -1 otherwise.
scAttackPortNumber	32822	2	The port number related to this attack if one exists (if this is an IP scan, for example), -1 otherwise.
scAttackType	32823	4	Who scAttackIp belongs to: <ul style="list-style-type: none"> <li>• 0—Attacked</li> <li>• 1—Attacker</li> </ul>
scAttackSide	32824	1	The IP address side: <ul style="list-style-type: none"> <li>• 0—User</li> <li>• 1—Network</li> </ul>
scAttackIpProtocol	32825	1	The IP protocol type: <ul style="list-style-type: none"> <li>• 0—Other</li> <li>• 1—ICMP</li> <li>• 6—TCP</li> <li>• 17—UDP</li> </ul>
scAttacks	32826	1	The number of attacks in the current reporting period. Since attack reports are generated per attack, the value is 0 or 1.
scAttackMaliciousSessions	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.