STREAMCORE NETFLOW

Table des matières

1 Introduction

NetFlow is a service that provides valuable information to system administrators identifying the types and volume of application traffic traversing enterprise wide area data networks. NetFlow is used mainly for network troubleshooting, accounting, security and planning purposes.

Streamcore NetFlow tickets are generated by StreamGroomer appliances deployed in remote sites and data centers to intercept and process packet traffic flowing between LANs and WANs. In these locations, Streamcore appliances are already monitoring and controlling WAN flows, thus ideally suited to export NetFlow tickets for these monitored WAN flows.

It is simple to activate the Export of NetFlow tickets by enabling NetFlow on StreamGroomers at the sites of interest. The export destination is configured to direct traffic to a specific NetFlow collector IP address and port number.

This document details the content of the NetFlow v9 tickets produced by the Streamcore products. This technical document will help the network consultants understand the structure of the flow records designed to report statistics for any applications monitored by Streamcore. Statistics are reported for web applications (HTTP and HTTPs) and RTP/RTCP applications.

1.1 AUDIENCE

This document is intended for experienced network consultants and application developers. It is assumed that the reader understands IP, TCP and UDP protocols, HTTP/HTTPs, Real-Time Protocol (RTP), Real-Time Control Protocol (RTCP), Codecs, Type of Service (TOS), Round Trip Time (RTT), Application Response Time (ART), SSL protocols, SSL certificates, VoIP, MOS and MOS-LQ.

Knowledge of NetFlow purpose and specifications is required to understand the concepts mentioned in this document.

Streamcore concepts and products such as the StreamGroomers (SG), StreamGroomer Manager, rules and intermediate rules are also required because some information sent in the NetFlow tickets refer to Streamcore objects. It is assumed that the Streamcore administrator knows how to enable and configure NetFlow on the StreamGroomers.

1.2 STREAMCORE SOFTWARE RELEASES

This document applies to Streamcore Software Suite 6.2 and later versions.

1.3 DOCUMENTATION

For further details on the Streamcore Software Suite, refer to Streamcore documentation:

- StreamView user guide
- StreamGroomer Manager user guide

For further details about NetFlow v9, refer to the RFC3954.

For further details about HTTP/1.1, refer from RFC7230 to RFC7237.

For further details about the Transport Protocol for Real-Time Applications, refer to RFC 3550.

2 Streamcore NetFlow v9 specifications

This topic describes the structure of the Streamcore NetFlow tickets generated in V9 version.

The structure of a NetFlow ticket is composed of a header followed by several records that depend on the version of the NetFlow specification.

2.1 NETFLOW HEADER

The following figures describes the structure of the NetFlow header:

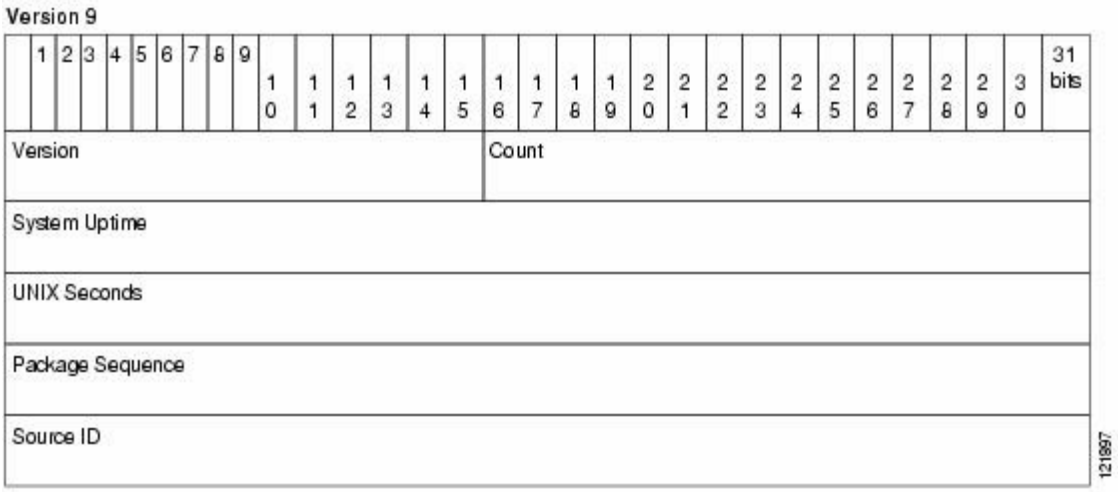


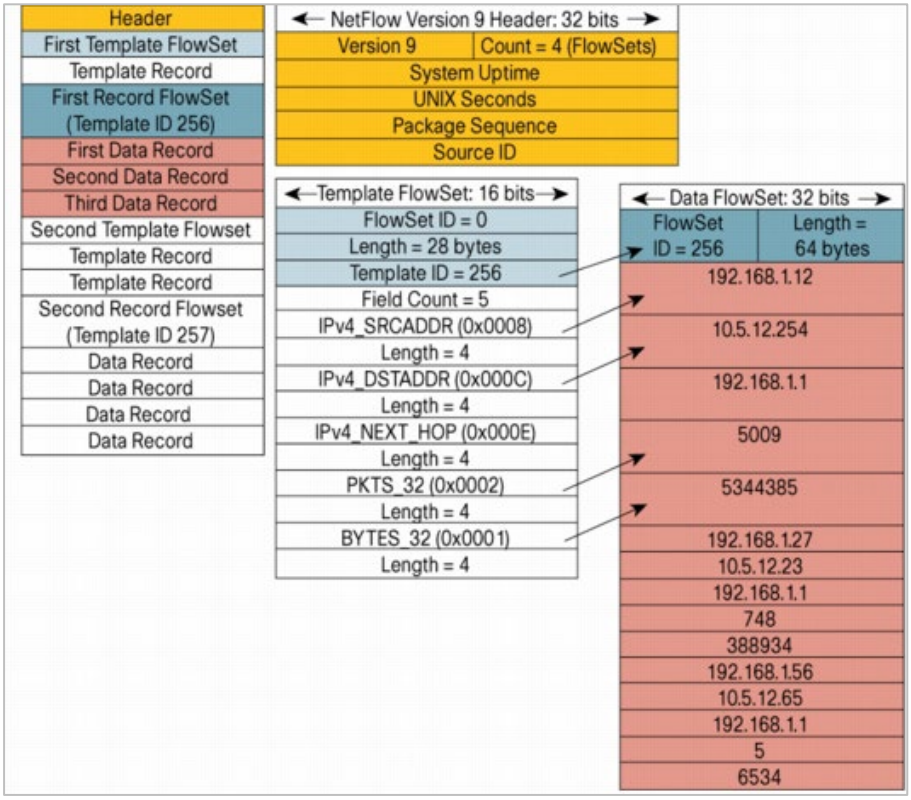
Figure 1 - Header of a NetFlow ticket (source Cisco)

The header fields are:

NetFlow Header	
Field Name	Value
Version	NetFlow version: 0x0009.
Count	Number of FlowSet records (both template and data) contained within this packet.
System Uptime	Time in milliseconds since this device was first booted.
UNIX Seconds	Seconds since 0000 Coordinated Universal Time (UTC) 1970.
Sequence Number	Incremental sequence counter of all export packets sent by this export device; this value is cumulative, and it can be used to identify whether any export packets have been missed. This is a change from the NetFlow Version 5 and Version 8 headers, where this number represented “total flows.
Source ID	This field is always set to 0, by the StreamGroomers.

2.2 FLOW RECORDS

Flow records in version 9 are more complex than in version 5. The figure below gives an example of a possible record (source Cisco).



2.3 STREAMCORE FLOW RECORD TYPES

Six flow templates have been defined which correspond to several types of sessions:

- If a flow is associated by the StreamGroomer to RTP+RTCP protocols, the flow template used in the NetFlow ticket is either **RTP Flow1 (template ID 258) or RTP Flow2 (template ID 259)**.

Figure 2 - Example of NetFlow v9 tickets (source Cisco)

- If a flow is associated by the StreamGroomer to HTTP or HTTPs, the flow template is either ***HTTP Flow*** **(template ID 260)** *or* ***HTTPs Flow*** **(template ID 261)**.
- If the If a flow is associated to other applications, the flow template is either **Other Flow1 (template ID 256)** or **Other Flow2 (template ID 257)**.

According to the level of the rule that is associated to the network flow by the StreamGroomer, the NetFlow ticket will contain different record types:

- When a flow is associated to a rule in the StreamView tree from level 1 to level 5, the StreamGroomer generates flow records 256 or 258 or 260.
- If the flow is associated to a rule in StreamView inserted at from the level 6 to 10, the StreamGroomer generates flow records 257 or 259 or 261.

2.3.1 Record types description

The following tables list the elements in the 6 templates.

This table lists the standard fields in v9 format:

Field Type	Value (decimal)	Length (bytes	Description		Other Flow1	Other Flow2	RTP Flow1	RTP Flow2	HTTP Flow	HTTPS Flow
				Template ID	256	257	258	259	260	261
IN_BYTES	1	8	Incoming counter with length N x 8 bits for number of bytes associated with an IP Flow.		X	X	X	X	X	X
IN_PKTS	2	4	Incoming counter with length N x 8 bits for the number of packets associated with an IP Flow		X	X	X	X	X	X
PROTOCOL	4	1	IP protocol byte		X	X	X	X	X	X
SRC_TOS	5	1	Type of Service byte setting when entering incoming interface		X	X	X	X	X	X
TCP_FLAGS	6	1	Cumulative of all the TCP flags seen for this flow		X	X			X	X
L4_SRC_PORT	7	2	TCP/UDP source port number i.e.: FTP, Telnet, or equivalent		X	X	X	X	X	X
IPV4_SRC_ADDR	8	4	IP v4 source address		X	X	X	X	X	X
INPUT_SNMP	10	2, 4	Input interface index; default for N is 2 but higher values could be used – STREAMCORE: 4B		X	X	X	X	X	X
L4_DST_PORT	11	2	TCP/UDP destination port number i.e.: FTP, Telnet, or equivalent		X	X	X	X	X	X
IPV4_DST_ADDR	12	4	IP v4 destination address		X	X	X	X	X	X
OUTPUT_SNMP	14	2, 4	Output interface index; default for N is 2 but higher values could be used – STREAMCORE: 4B		X	X	X	X	X	X
LAST_SWITCHED	21	4	System uptime at which the last packet of this flow was switched		X	X	X	X	X	X
FIRST_SWITCHED	22	4	System uptime at which the first packet of this flow was switched		X	X	X	X	X	X

This table lists the fields in v9 format specific to Streamcore NetFlow tickets.

The column "Average value" indicates that the value is the average of the metric that is recalculated for a session since the beginning of the session.

FIELDS SPECIFIC TO STREAMCORE				Description	Other Flow1	Other Flow2	RTP Flow1	RTP Flow2	HTTP Flow	HTTPS flow
	Value	Length	Average value	Template ID	256	257	258	259	260	261
WAN_RTT	8192	4	X	RTT of TCP flow. This is a numerical value in milliseconds.	X	X			X	X
NET_APP_RESP_TIME	8193	4	X	Network Application Response Time of TCP flow This is a numerical value in milliseconds.	X	X			X	X
TOTAL_APP-RESP_TIME	8194	4	X	Total Application Response Time of TCP flow. This is a numerical value in milliseconds.	X	X			X	X
TCP_RETRANS_RATE	8195	2	X	TCP retransmission rate. This is a numerical value in ‰. Divide this value by 10 to obtain a percentage.	X	X			X	X
CALL_DIRECTION	8196	1		Call direction for a session. This is a Boolean value. The value 0 means that the flow is sent from the client to the server. The value 1 means that the flow is sent by the server to the client side.	X	X	X	X	X	X
HOSTNAME	8256	40		40 last bytes of the HTTP request HOSTNAME. The value is a character string.					X	
URL	8257	0,60, 100,150		0 (just the hostname), 60, 100 or 150 first bytes of the HTTP request URL. The value is a character string (if not empty). Refer to the StreamView user guide to configure the length of the URL sent in the NetFlow record.					X	
SSL_CN	8258	30		30 last bytes of the SSL certificate Common Name. The value is a character string.						X
SSL_ORG	8259	30		30 first bytes of the SSL certificate Organization Name. The value is a character string.						X
MOS_LQ	8320	2	X	MOS LQ from the WAN for the VoIP communication. This is a numerical value. To obtain the measured MOS LQ between 0 and 5, divide this value by 1000.			X	X		
NET_DELAY	8321	2	X	Network Delay based on RTCP packets for the VoIP/Video communication. This is a numerical value in milliseconds.			X	X		
NET_LOSS	8322	2	X	Network Loss based on RTP packets for the VoIP/Video communication. This is a numerical value in ‰. Divide this value by 10 to obtain a percentage (%).			X	X		
NET_JITTER	8323	2	X	Network Jitter based on RTP packets for the VoIP/Video communication. This is a numerical value in milliseconds.			X	X		

FIELDS SPECIFIC TO STREAMCORE				Description		Other Flow1	Other Flow2	RTP Flow1	RTP Flow2	HTTP Flow	HTTPS flow
	Value	Length	Average value		Template ID	256	257	258	259	260	261
NET_DISCARD	8324	2	X	Network Discard rate based on RTP packets for the VoIP/Video communication. This is a numerical value in ‰. Divide this value by 10 to obtain a percentage (%).				X	X		
RTP_CLOCKRATE_IN	8325	1		RTP clock rate based on RTP packets for the VoIP/Video communication – Inbound. This is a numerical value in kHz.				X	X		
RTP_CLOCKRATE_OUT	8326	1		RTP clock rate based on RTP packets for the VoIP/Video communication – Outbound. This is a numerical value in kHz.				X	X		
CODEC_IN	8327	1		Codec used for the RTP communication – Inbound. This numerical value is the payload type of the flow. Refer to the paragraph Payload Types further in this document.				X	X		
CODEC_OUT	8328	1		Codec used for the RTP communication – Outbound. This numerical value is the payload type of the flow. Refer to the paragraph Payload Types further in this document.				X	X		
ID_RULE_1	8384	4		Streamcore Internal Rule ID Level 1 (Access Link). This is a numerical value. This is the ID of the first Streamcore rule in the StreamView tree. It represents the access link between the LAN and the WAN where the flows are monitored by the StreamGroomer. This field cannot be null.		X	X	X	X	X	X
ID_RULE_2	8385	4		Streamcore Internal Rule ID Level 2. This is a numerical value. This is the ID of the rule under the Access Link rule that matches the flow. Refer to the paragraph StreamView Tree for further details. It cannot be null.		X	X	X	X	X	X
ID_RULE_3	8386	4		Streamcore Internal Rule ID Level 3. This is a numerical value. This is the ID of the rule at the level 3 in the Rule Tree that matches the flow. Refer to the paragraph StreamView Tree for further details. It can be equal to 0 if there is no rule under level 2 in the Rule Tree.		X	X	X	X	X	X
ID_RULE_4	8387	4		Streamcore Internal Rule ID Level 4. This is a numerical value. This is the ID of the rule at the level 4 in the Rule Tree that matches the flow. Refer to the paragraph StreamView Tree for further details. It can be equal to 0 if there is no rule under level 3 in the Rule Tree.		X	X	X	X	X	X
ID_RULE_5	8388	4		Streamcore Internal Rule ID Level 5. This is a numerical value. This is the ID of the rule at the level 5 in the Rule Tree that matches the flow. Refer to the paragraph StreamView Tree for further details. It can be equal to 0 if there is no rule under level 4 in the Rule Tree.		X	X	X	X	X	X

FIELDS SPECIFIC TO STREAMCORE				Description		Other Flow1	Other Flow2	RTP Flow1	RTP Flow2	HTTP Flow	HTTPS flow
	Value	Length	Average value		Template ID	256	257	258	259	260	261
ID_RULE_6	8389	4		Streamcore Internal Rule ID Level 6. This is a numerical value. This is the ID of the rule at the level 6 in the Rule Tree that matches the flow. Refer to the paragraph StreamView Tree for further details. It cannot be null if it is sent in the Records 257 and 259.			X		X	X	X
ID_RULE_7	8390	4		Streamcore Internal Rule ID Level 7. This is a numerical value. It can be equal to 0 if there is no rule under level 6 in the Rule Tree.			X		X	X	X
ID_RULE_8	8391	4		Streamcore Internal Rule ID Level 8. This is a numerical value. It can be equal to 0 if there is no rule under level 7 in the Rule Tree.			X		X	X	X
ID_RULE_9	8392	4		Streamcore Internal Rule ID Level 9. This is a numerical value. It can be equal to 0 if there is no rule under level 8 in the Rule Tree.			X		X	X	X
ID_RULE_10	8393	4		Streamcore Internal Rule ID Level 10. This is a numerical value. It can be equal to 0 if there is no rule under level 9 in the Rule Tree.			X		X	X	X

2.3.2 RTP Payload Types

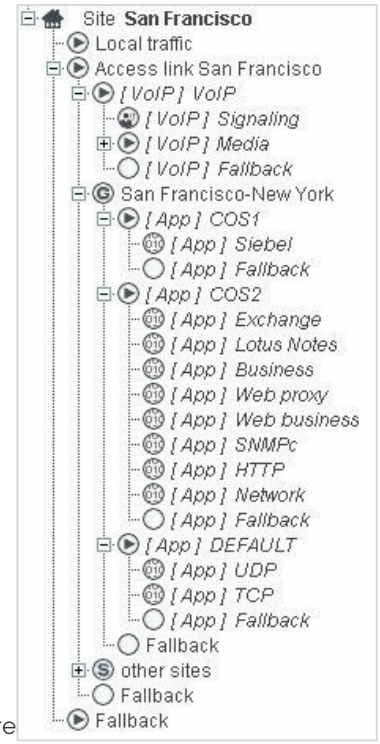
The payload type is a numerical value that identifies the audio and video codec used to encode the payload carried with RTP. The list of RTP payload types for audio and video encodings (codec types) is defined by IETF in the section 6 *Payload Type Definitions* of the RFC3551. The RFC3551 assigned values to every encoding method, for example:

Payload Types	
Payload Type value	Encoding method
0	PCMU
4	G723
8	PCMA
15	G728
31	H261
34	H263

2.3.3 StreamView Tree and Rules ID

The record types in V9 format refer to Streamcore objects with the fields ID_RULE_1 to ID_RULE_10. A Streamcore rule is a set of criteria to identify a type of network flow, for example, a TCP session to a given application server or more specifically a HTTPs session to a given application server using a specific SSL certificate.

Let's have a look at this StreamView Tree:



If a NetFlow ticket is sent by the Stre the HTTP sessions, the fields ID_RULE_1, ID_RULE_2, ID_RULE3 and ID_RULE_4 will identify the full path of the rule in the StreamView Tree:

- ID_RULE_1 = ID of "Access link San Francisco",
- ID_RULE_2 = ID of "San Francisco-New York" (a grooming rule),
- ID_RULE_3 = ID of "[APP] COS2"
- ID_RULE_4 = ID of "[APP] HTTP"
- ID_RULE_5, ID_RULE_6, ID_RULE_7, ID_RULE_8, ID_RULE_9, ID_RULE_10 are equal to 0

Since the StreamGroomer has identified a HTTP session, the record type is 260.

The ID of a rule is a numerical value (positive integer) assigned by StreamView when a rule is created. This ID is unique in a StreamGroomer Manager.

When analyzing the NetFlow ticket, it is possible to retrieve additional information in StreamView by building the path to the final rule with the identifiers carried in the records.

3 Technical Support

Streamcore Technical Support

By email: support@streamcore.com

By telephone: +33 (0)1.40.90.34.26

Please provide the following information:

- ☐ Maintenance contract number
- ☐ SG model number
- ☐ SG serial number found on bottom of the appliance and on the packing slip,
- ☐ The license report from SGMConf | system/licenses tab

Caution!

Do not open StreamGroomer cover. This operation should only be carried out by qualified maintenance staff who have received authorization from Streamcore.

WARNING!

There is a risk of explosion if the wrong replacement batteries are used – only use batteries of the same type or of a similar type recommended by the manufacturer. Used batteries must be recycled in accordance with the manufacturer's instructions.