AVC-Related Exported Fields

First Published: March 29, 2013
Revised: March 26, 2015

Table A-1 describes the Flexible NetFlow (FNF) fields and the CLI used to retrieve the value of the fields, added for Cisco AVC.

In addition to the these new fields, an AVC record can include FNF fields defined prior to IOS XE 3.8. For information about FNF fields, see: *Cisco IOS Flexible NetFlow Command Reference*.

Table A-1 New FNF Exported Fields

Field ID	Name	Enterprise Specific	Data Type	Data Type Semantics	Description	Units	CLI
56	sourceMacAddress	No	macAddress	identifier	IEEE 802 source MAC address field. This field is collected only for a monitor attached in the ingress direction.	MAC	<collect | match> datalink mac source address input
57	postDestinationMac Address	No	macAddress	identifier	The definition of this information element is identical to the definition of information element “destinationMacAddress,” except that it reports a potentially modified value caused by a middlebox function after the packet has passed the observation point.	MAC	<collect | match> datalink mac destination address output
58	vlanId	No	unsigned16	identifier	IEEE 802.1Q VLAN identifier (VID) extracted from the tag control Information field that was attached to the IP packet. This field is collected only for a monitor attached in the ingress direction.	number	<collect | match> datalink source-vlan-id

Table A-1 New FNF Exported Fields

Field ID	Name	Enterprise Specific	Data Type	Data Type Semantics	Description	Units	CLI
59	postVlanId	No	unsigned16	identifier	The definition of this information element is identical to the definition of information element “vlanId,” except that it reports a potentially modified value caused by a middlebox function after the packet has passed the observation point.	number	<collect | match> datalink destination-vlan-id
80	destinationMacAddress	No	macAddress	identifier	IEEE 802 destination MAC address field. This field is collected only for a monitor attached in the ingress direction.	MAC	<collect | match> datalink mac destination address input
81	postSourceMacAddress	No	macAddress	identifier	The definition of this information element is identical to the definition of information element “sourceMacAddress,” except that it reports a potentially modified value caused by a middlebox function after the packet has passed the observation point.	MAC	<collect | match> datalink mac source address output

Table A-1 New FNF Exported Fields

Field ID	Name	Enterprise Specific	Data Type	Data Type Semantics	Description	Units	CLI
138	observationPointId	No	unsigned64	identifier	An identifier of an observation point that is unique for each observation domain. It is recommended that this identifier be unique for each IPFIX device. Typically, this information element is used for limiting the scope of other information elements. The field contains 8 bytes: The 4 most significant bytes (MSBs) indicate the type. Currently, only type 1 is supported. When type is "1," the 4 least significant bytes (LSBs) indicate the interface SNMP index, which is also listed in the interface option template. **Example**: Observation Point Id: 4294967309 = 0x000000010000000D The 4 MSBs indicate a type of 1. The 4 LSBs indicate that the SNMP index for the interface is 0xD.	number	<collect | match> flow observation point
209	tcpOptions	No	unsigned64	flags	TCP options in packets of this flow. The information is encoded in a set of bit fields. For each TCP option, there is a bit in this set. The bit is set to 1 if any observed packet of this flow contains the corresponding TCP option. Otherwise, if no observed packet of this flow contained the respective TCP option, the value of the corresponding bit is 0.	bitmap	collect transport tcp option map
231	initiatorOctets	No	unsigned64	identifier	Total number of layer 4 payload bytes in a flow from the initiator. The initiator is the device that triggered the session creation, and remains the same for the life of the session.	octets	collect counter initiator bytes long

Table A-1 New FNF Exported Fields

Field ID	Name	Enterprise Specific	Data Type	Data Type Semantics	Description	Units	CLI
232	serverOctets	No	unsigned64	identifier	Total number of layer 4 payload bytes in a flow from the server. The server is the device that replies to the client, and remains the same for the life of the session.	octets	collect connection server counter bytes long
235	egressVRFID	No	unsigned32	identifier	Unique identifier of the VRF name where the packets of this flow are being sent. This identifier is unique per metering process.	number	<collect | match> routing vrf output
239	biflowDirection	No	unsigned8	identifier	A description of the direction assignment method used to assign the Biflow Source and Destination. This Information Element may be present in a Flow Data Record, or applied to all flows exported from an Exporting Process or Observation Domain using IPFIX Options. If this Information Element is not present in a Flow Record or associated with a Biflow via scope, it is assumed that the configuration of the direction assignment method is done out-of-band. Note that when using IPFIX Options to apply this Information Element to all flows within an Observation Domain or from an Exporting Process, the Option SHOULD be sent reliably. If reliable transport is not available (i.e., when using UDP), this Information Element SHOULD appear in each Flow Record.		collect connection initiator
278	connectionCountNew	No	unsigned32	deltaCounter	This information element counts the number of TCP or UDP connections which were opened during the observation period. The observation period may be specified by the flow start and end timestamps.	number	collect connection new-connections

Table A-1 New FNF Exported Fields

Field ID	Name	Enterprise Specific	Data Type	Data Type Semantics	Description	Units	CLI
279	connectionSumDurationSeconds	No	unsigned64		This information element aggregates the total time in seconds for all of the TCP or UDP connections which were in use during the observation period. For example if there are 5 concurrent connections each for 10 seconds, the value would be 50 s.	seconds	collect connection sum-duration
280	connectionTransactionId	No	unsigned64	identifier	Identifies a transaction within a connection. A transaction is a meaningful exchange of application data between two network devices or a client and server. A transactionId is assigned the first time a flow is reported, so that later reports for the same flow will have the same transactionId. A different transactionId is used for each transaction within a TCP or UDP connection. The identifiers need not be sequential.	number	match connection transaction-id
298	clientPackets	No	unsigned64	identifier	Total number of layer 4 packets in a flow from the client. The client is the device that triggered the session creation, and remains the same for the life of the session.	packets	collect connection client counter packets long
299	serverPackets	No	unsigned64	identifier	Total number of layer 4 packets in a flow from the server. The server is the device that replies to the client, and remains the same for the life of the session.	packets	collect connection server counter packets long
359	monitoringIntervalStartMilliSeconds	Yes	dateTimeMilliseconds		The absolute timestamp at which a monitoring interval starts. A monitoring interval is the period during which the metering Process is running.	milliseconds	match timestamp absolute monitoring-interval start
37083	tcpWindowSizeMin	Yes	unsigned32	identifier	Minimum TCP window size.	octets	collect transport tcp window-size minimum
37084	tcpWindowSizeMax	Yes	unsigned32	identifier	Maximum TCP window size.	octets	collect transport tcp window-size maximum

Table A-1 New FNF Exported Fields

Field ID	Name	Enterprise Specific	Data Type	Data Type Semantics	Description	Units	CLI
37086	tcpMaximumSegmentSize	Yes	unsigned16	identifier	TCP maximum segment size.	octets	collect transport tcp maximum-segment-size
37092	tcpWindowSizeSum	Yes	unsigned64	identifier	Sum of TCP window size values. Divide by packet counter to get average.	octets	collect transport tcp window-size sum
42036	retransPackets	Yes	unsigned32	deltaCounter	Number of packets retransmitted by the client	packets	collect connection client counter packets retransmitted
42040	transactionCountDelta	Yes	unsigned32	deltaCounter	Total number of completed transactions observed for this flow.		collect connection transaction counter complete
42041	sumTransactionTime	Yes	unsigned32	Duration	Transaction time is the time between the client request and the corresponding last response packet from the server, as observed at the observation point. The value is the sum of all transaction times observed for this flow. For the average, this field must be divided by transactionCountDelta (42040).	milliseconds	collect connection transaction duration sum
42042	maxTransactionTime	Yes	unsigned32	Duration	Maximum transaction time observed for this flow.	milliseconds	collect connection transaction duration max
42043	minTransactionTime	Yes	unsigned32	Duration	Minimum transaction time observed for this flow.	milliseconds	collect connection transaction duration min
42060	numRespsCountDelta	Yes	unsigned32	deltaCounter	Total number of responses sent by the server.	responses	collect connection server counter responses
42061	numResps1CountDelta	Yes	unsigned32	deltaCounter	Histogram Bucket 1 for response time. The bucket boundary should be specified in an option template or predefined in the reporting entity.	responses	collect connection delay response to-server histogram
42062	numResps2CountDelta	Yes	unsigned32	deltaCounter	Histogram Bucket 2 for response time. The bucket boundary should be specified in an option template or predefined in the reporting entity.	responses	collect connection delay response to-server histogram

Table A-1 New FNF Exported Fields

Field ID	Name	Enterprise Specific	Data Type	Data Type Semantics	Description	Units	CLI
42063	numResps3CountDelta	Yes	unsigned32	deltaCounter	Histogram Bucket 3 for response time. The bucket boundary should be specified in an option template or predefined in the reporting entity.	responses	collect connection delay response to-server histogram
42064	numResps4CountDelta	Yes	unsigned32	deltaCounter	Histogram Bucket 4 for response time. The bucket boundary should be specified in an option template or predefined in the reporting entity.	responses	collect connection delay response to-server histogram
42065	numResps5CountDelta	Yes	unsigned32	deltaCounter	Histogram Bucket 5 for response time. The bucket boundary should be specified in an option template or predefined in the reporting entity.	responses	collect connection delay response to-server histogram
42066	numResps6CountDelta	Yes	unsigned32	deltaCounter	Histogram Bucket 6 for response time. The bucket boundary should be specified in an option template or predefined in the reporting entity.	responses	collect connection delay response to-server histogram
42067	numResps7CountDelta	Yes	unsigned32	deltaCounter	Histogram Bucket 7 for response time. The bucket boundary should be specified in an option template or predefined in the reporting entity.	responses	collect connection delay response to-server histogram
42068	numLateRespsCountDelta	Yes	unsigned32	deltaCounter	Total number of late responses sent by the server. A late response is a response whose time is greater than the last bucket. This informational element can be treated as the last bucket that has no end limit.	responses	collect connection delay response to-server histogram
42071	sumRespTime	Yes	unsigned32	Delay	Response time is the time between the client request and the corresponding first response packet from the server, as observed at the observation point. The value of this information element is the sum of all response times observed for the responses of this flow. For the average, this field must be divided by numRespsCountDelta (42060).	milliseconds	collect connection delay response to-server sum
42072	maxRespTime	Yes	unsigned32	Delay	Maximum response time observed for this flow.	milliseconds	collect connection delay response to-server max

Table A-1 New FNF Exported Fields

Field ID	Name	Enterprise Specific	Data Type	Data Type Semantics	Description	Units	CLI
42073	minRespTime	Yes	unsigned32	Delay	Minimum response time observed for this flow.	milliseconds	collect connection delay response to-server min
42074	sumServerRespTime	Yes	unsigned32	Delay	Yes	milliseconds	collect connection delay application sum
42075	maxServerRespTime	Yes	unsigned32	Delay	Maximum application delay observed for the responses of this flow.	milliseconds	collect connection delay application max
42076	minServerRespTime	Yes	unsigned32	Delay	Minimum application delay observed for the responses of this flow.	milliseconds	collect connection delay application min
42077	sumTotalRespTime	Yes	unsigned32	Delay	Total delay is the time between the client request and the first response packet from the server, as seen by the client. This is the sum of all total delays observed for the responses of this flow. For the average, this field must be divided by numRespsCountDelta (42060)	milliseconds	collect connection delay response client-to-server sum
42078	maxTotalRespTime	Yes	unsigned32	Delay	Maximum total delay observed for the responses of this flow.	milliseconds	collect connection delay response client-to-server max
42079	minTotalRespTime	Yes	unsigned32	Delay	Minimum total delay observed for the responses of this flow.	milliseconds	collect connection delay response client-to-server min
42081	sumNwkTime	Yes	unsigned32	Delay	Network delay is the round-trip time between the client and the server, as measured by the observation point, calculated once per session. The value of this information element is the sum of all network delays observed for the sessions of this flow. For the average, this field must be divided by connectionCountNew (278).	milliseconds	collect connection delay network client-to-server sum
42082	maxNwkTime	Yes	unsigned32	Delay	Yes	milliseconds	collect connection delay network client-to-server max

Table A-1 New FNF Exported Fields

Field ID	Name	Enterprise Specific	Data Type	Data Type Semantics	Description	Units	CLI
42083	minNwkTime	Yes	unsigned32	Delay	Yes	milliseconds	collect connection delay network client-to-server min
42084	sumClientNwkTime	Yes	unsigned32	Delay	Client network delay is the round-trip time between the observation point and the client, calculated once per session. The value of this information element is the sum of all client network delays observed for the sessions of this flow. For the average, this field must be divided by connectionCountNew (278).	milliseconds	collect connection delay network to-client sum
42085	maxClientNwkTime	Yes	unsigned32	Delay	Maximum client network delay observed for the sessions of this flow.	milliseconds	collect connection delay network to-client max
42086	minClientNwkTime	Yes	unsigned32	Delay	Minimum client network delay observed for the sessions of this flow.	milliseconds	collect connection delay network to-client min
42087	sumServerNwkTime	Yes	unsigned32	Delay	Server network delay is the round-trip time between the observation point and the server, calculated once per session. The value of this information element is the sum of all server network delays observed for the sessions of this flow. For the average, this field must be divided by connectionCountNew (278)	milliseconds	collect connection delay network to-server sum
42088	maxServerNwkTime	Yes	unsigned32	Delay	Maximum server network delay observed for the sessions of this flow.	milliseconds	collect connection delay network to-server max
42089	minServerNwkTime	Yes	unsigned32	Delay	Minimum server network delay observed for the sessions of this flow.	milliseconds	collect connection delay network to-server min

Table A-1 New FNF Exported Fields

Field ID	Name	Enterprise Specific	Data Type	Data Type Semantics	Description	Units	CLI
45004	clientIPv4Address	Yes	ipv4Address	identifier	The IPv4 client address in the IP packet header. This may be the source or destination IP address, depending on the first packet of the connection. The client is the device that triggered the session creation, and remains the same for the life of the session.	address	<collect | match> client ipv4 address
45005	serverIPv4Address	Yes	ipv4Address	identifier	The IPv4 server address in the IP packet header. The server is the device that replies to the client, and remains the same for the life of the session.	address	<collect | match> server ipv4 address
45006	clientIPv6Address	Yes	ipv6Address	identifier	The IPv6 client address in the IP packet header. The client is the device that triggered the session creation, and remains the same for the life of the session.	address	<collect | match> client ipv6 address
45007	serverIPv6Address	Yes	ipv6address	identifier	IPv6 server address in the IP packer header. The server is the device that replies to the client, and remains the same for the life of the session.	address	<collect | match> server ipv6 address
45008	clientTransportPort	Yes	unsigned16	identifier	Client transport port identifier. This may be the source or destination transport port. The client is the device that triggered the session creation, and remains the same for the life of the session.	number	<collect | match> client transport port
45009	serverTransportPort	Yes	unsigned16	identifier	Server transport port identifier. This may be the source or destination transport port. The server is the device that replies to the client, and remains the same for the life of the session.	number	<collect | match> server transport port
41000	classHierarchy	Yes	Var-Len	identifier	Identifies the policy-map hierarchy for different policy-map types. The field contains the policy-id, followed by a list of classes representing the policy hierarchy: {Pi | Ck … Cl}. A dedicated option template contains the policy and class id mapping to name and type.	number	<collect | match> policy performance-monitor classification hierarchy

Table A-1 New FNF Exported Fields

Field ID	Name	Enterprise Specific	Data Type	Data Type Semantics	Description	Units	CLI
42020	servicesWaasSegment	Yes	unsigned8	identifier	WAAS optimization "segment" can have one of the following values:	number	<collect | match> services waas segment
					Unknown	0	
					Client Unoptimized	1	
					Server Optimized	2	
					Client Optimized	4	
					Server Unoptimized	8	
					Pass-Through	16	
42021	servicesWaasPassThroughReason	Yes	unsigned8	identifier	WAAS optimization pass-through reason can have one of the following values:	number	collect services waas passthrough-reason
					PT_NO_PEER	1	
					PT_RJCT_CAP	2	
					PT_RJCT_RSRCS	3	
					PT_RJCT_NO_LICENSE	4	
					PT_APP_CONFIG	5	
					PT_GLB_CONFIG	6	
					PT_ASYMMETRIC	7	
					PT_IN_PROGRESS	8	
					PT_INTERMEDIATE	9	

Table A-1 New FNF Exported Fields

Field ID	Name	Enterprise Specific	Data Type	Data Type Semantics	Description	Units	CLI
					PT_OVERLOAD	10	
					PT_INT_ERROR	11	
					PT_APP_OVERRIDE	12	
					PT_SVR_BLACKLIST	13	
					PT_AD_VER_MISMTCH	14	
					PT_AD_AO_INCOMPAT	15	
					PT_AD_AOIM_PROGRESS	16	
					PT_DIRM_VER_MISMTCH	17	
					PT_PEER_OVERRIDE	18	
					PT_AD_OPT_PARSE_FAIL	19	
					PT_AD_PT_SERIAL_-MODE	20	
					PT_SN_INTERCEP-TION_ACL	21	
					PT_IP_FRAG_UNSUP-P_PEER	22	
					PT_CLUSTER_MEM-BER_INDX	23	
					PT_FLOW_QUERY_-FAIL_INDX	24	
					PT_FLOWSW_INT_A-CL_DENY_INX	25	
					PT_UNKNOWN_INDX	26	
					PT_FLOWSW_PL-CY_INDX	27	
					PT_SNG_OVER-LOAD_INDX	28	
					PT_CLUSTER_DE-GRADE_INDX	29	
					PT_FLOW_LEARN_-FAIL_INDX	30	
					PT_OVERALL_INDX	31	
					PT_ZBFW	32	
					PT_RTSP_ALG	33	
42128	policyQosQueueID	No	unsigned32	identifier	QoS Policy queue ID	number	match policy qos queue id
42129	policyQosQueueDrop	No	unsigned64	counter	QoS Policy drops per queue	number	collect policy qos queue drops
45010	connectionId	Yes	unsigned32	identifier	Identifies a connection. A connection identifier is created when a new TCP or UDP flow is created between server and client. A single connection can hold several transactions.	number	match connection id