### decodesflow

Decodes the sFlow packets.

#### Syntax

decodesflow

#### Description

The output fields are as follows:

* **agent\_addr**: IP address of sFlow agent
* **agent\_id**: Agent identifier
* **counters**: When **sample\_type** is counters, the following map-type information is output.
* **admin\_status**: Whether the administrator port is enabled (true, false)
* **if\_direction**(0: unknown, 1: Full-duplex, 2: Half-duplex, 3: Receive, 4: Send)
* **if\_index**: Interface identifier
* **if\_speed**: Connection link speed in bps
* **if\_type**: Ethernet is 6, Refer to the interface type standard number assigned by IANA: "IANAifType ::= TEXTUAL-CONVENTION" and "SYNTAX INTEGER" sections in <https://ietf.org/assignments/ianaiftype-mib/ianaiftype-mib>
* **in\_bcast\_pkts**: Number of broadcast packets received
* **in\_discards**: Number of discarded packets received
* **in\_errors**: Number of packets with errors received
* **in\_mcast\_pkts**: Number of multicast packets received
* **in\_octets**: Total bytes received (bytes)
* **in\_ucast\_pkts**: Number of unicast packets received
* **in\_unknown\_protos**: Number of packets whose protocols are unknown among the received packets
* **oper\_status**: Whether the actual link is enabled (true, false)
* **out\_bcast\_pkts**: Number of broadcast packets sent
* **out\_discards**: Number of discarded packets to be sent
* **out\_errors**: Number of packets with errors among the packets to be sent
* **out\_mcast\_pkts**: Number of multicast packets sent
* **out\_octets**: Bytes sent
* **out\_ucast\_pkts**: Number of unicast packets sent
* **promisc\_mode**: Whether promiscuous mode is enabled (true, false)
* **drops**: Number of packets lost due to lack of performance. This outputs information when **sample\_type** is flow.
* **dst\_ip**: Destination IP address. Typically, the address of the sFlow collenction server.
* **dst\_port**: Destination port number
* **flow**: A packet randomly sampled according to **sampling\_rate**
* **flow\_seq**: Increases by 1 each time a sample created for each **src\_id**
* **flows**: Outputs the flow data information sampled when **sample\_type** is flow.
* **counters**: Inerface counters that transmit at regular intervals
* **frame\_length**: Length in byte of the packet before sampling
* **header**: Ethernet header octet byte stream
* **protocol**: Connection layer protocol (e.g., ethernet)
* **stripped**: Number of octets removed from the packet before extracting the data link layer header octets
* **input\_if\_index**: Outputs the interface identifier information received when **sample\_type** is flow
* **output\_if\_index**: Outputs the interface identifier information sent when **sample\_type** is flow
* **protocol**: Transport layer protocol. udp only.
* **sample\_pool**: Number of sources to be sampled. This outputs information when **sample\_type** is flow.
* **sample\_type**: Type of sampling
* **sampling\_rate**: Sampling rate. One from the specified number of packets is extracted. This outputs information when **sample\_type** is flow.
* **src\_id**: Interface identification number
* **src\_id\_type**: Interface type defined in RFC 2613 (0: ifIndex, 1: smonVlanDataSource, 2: entPhysicalEntry). Refer to 3.1.1 DataSource Objects in RFC 2613: <https://tools.ietf.org/html/rfc2613>
* **src\_ip**: Source IP address. Typically, the address of the sFlow agent.
* **src\_port**: Source port number
* **uptime**: Uptime after the agetn starts
* **ver**: sflow version. Only version 5 supported.

#### Usage

Decode sFlow packets from sflow.pcap file.

pcapfile /opt/logpresso/sonar/sflow.cap | decodesflow