### decodesflow

指定したパケットをsFlow基準で解析し、出力します。

#### 構文

decodesflow

#### 説明

出力されるフィールドは以下の通りです。

* **agent\_addr**: エージェントのIPアドレス
* **agent\_id**: エージェント識別子
* **counters**: **sampling\_type**がcountersの場合に、以下のようなマップ形式の情報を出力
* **admin\_status**: 管理ポートの有効状態（true、false）
* **if\_direction**（0: 不明、1: フルデュプレックス、2: ハーフデュプレックス、3: 受信、4: 送信）
* **if\_index**: インターフェース識別子
* **if\_speed**: 接続リンクのbps
* **if\_type**: イーサネットは6、その他の番号はIANAが割り当てたインターフェースタイプ標準番号を参照：<https://ietf.org/assignments/ianaiftype-mib/ianaiftype-mib>（"IANAifType ::= TEXTUAL-CONVENTION", "SYNTAX INTEGER"セクション）
* **in\_bcast\_pkts**: 受信したブロードキャストパケット数
* **in\_discards**: 受信パケットのうち破棄された数
* **in\_errors**: 受信パケットのうちエラーが発生したパケット数
* **in\_mcast\_pkts**: 受信したマルチキャストパケット数
* **in\_octets**: 受信した容量（バイト単位）
* **in\_ucast\_pkts**: 受信したユニキャストパケット数
* **in\_unknown\_protos**: 受信パケットのうちプロトコル不明のパケット数
* **oper\_status**: 実際のリンク有効状態（true、false）
* **out\_bcast\_pkts**: 送信したブロードキャストパケット数
* **out\_discards**: 送信パケットのうち破棄された数
* **out\_errors**: 送信パケットのうちエラーが発生したパケット数
* **out\_mcast\_pkts**: 送信したマルチキャストパケット数
* **out\_octets**: 送信した容量（バイト単位）
* **out\_ucast\_pkts**: 送信したユニキャストパケット数
* **promisc\_mode**: 全パケット受信の有効状態（true、false）
* **drops**: パフォーマンス不足によるパケット損失数。**sampling\_type**がflowの場合に出力
* **dst\_ip**: 宛先IPアドレス。通常はsFlow収集サーバーのアドレスを示します。
* **dst\_port**: 宛先ポート番号
* **flow**: **sampling\_rate**に基づきランダムにサンプリングされたパケット
* **flow\_seq**: **src\_id**ごとにサンプル生成時に1ずつ増加
* **flows**: **sampling\_type**がflowの場合にサンプリングされたフローデータ情報を出力
* **frame\_length**: サンプリング前のパケット長（バイト単位）
* **header**: イーサネットヘッダーのオクテットバイトストリーム
* **protocol**: リンク層プロトコル（例：ethernet）
* **stripped**: リンク層ヘッダーオクテット抽出前にパケットから除去されたオクテット数
* **input\_if\_index**: **sampling\_type**がflowの場合に受信インターフェース識別子情報を出力
* **output\_if\_index**: **sampling\_type**がflowの場合に送信インターフェース識別子情報を出力
* **protocol**: トランスポート層プロトコル（udp）
* **sample\_pool**: サンプリング対象の元データ数。**sampling\_type**がflowの場合に出力
* **sample\_type**: サンプリング種別
* **sampling\_rate**: サンプリング比率。指定されたパケット数のうち1つを抽出。**sampling\_type**がflowの場合に出力
* **src\_id**: インターフェース識別番号
* **src\_id\_type**: RFC 2613で定義されたインターフェースタイプ（0: ifIndex、1: smonVlanDataSource、2: entPhysicalEntry）。詳細はRFC 2613「Remote Network Monitoring MIB Extensions for Switched Networks Version 1.0」3.1.1 DataSource Objectsを参照：<https://tools.ietf.org/html/rfc2613>
* **src\_ip**: 送信元IPアドレス。通常はsFlowエージェントのアドレスを示します。
* **src\_port**: 送信元ポート番号
* **uptime**: エージェントの起動後稼働時間
* **ver**: sFlowバージョン（バージョン5のみ対応）

#### 使用例

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