Applying IPFIX to Network Measurement

Brian Trammell <brian@trammell.ch>
with thanks to Benoit Claise and Elisa Boschi

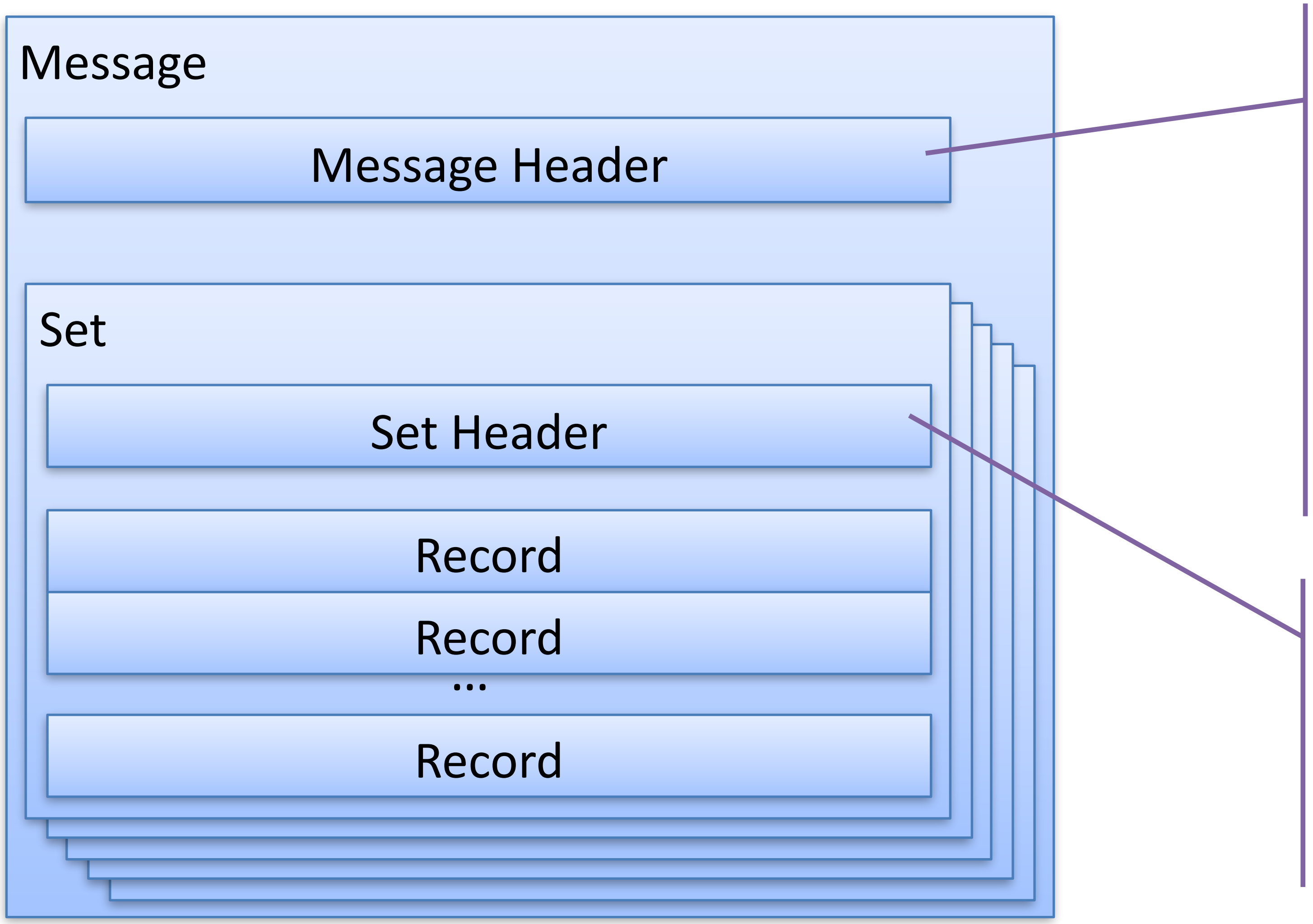
IPFIX

- “IP Flow Information eXport” (Internet Standard, STD 77/RFC 7011)
  - a unidirectional **protocol** for data export;
  - a **data format** providing efficient record-level self-description for this protocol;
    - applicable to any collection with large numbers of records sharing similar structures, including a file format definition (RFC 5655)
  - and an **information model** providing the vocabulary for this data format.
    - applicable to most measurement/logging tasks at transport and network layers, extensible beyond.

Data Format Terminology

- IPFIX transports flow data in (IPFIX) **Messages**.
  - A Message contains a **Message Header** and one or more Sets.
  - A Set contains a **Set Header** and may be one of:
    - a **Template Set**, containing Template Records;
    - an **Options Template Set**, containing Options Template Records; or
    - a **Data Set**, containing Data Records.
- The structure of these Data Records is described by a corresponding Template or Options Template.

Message Structure



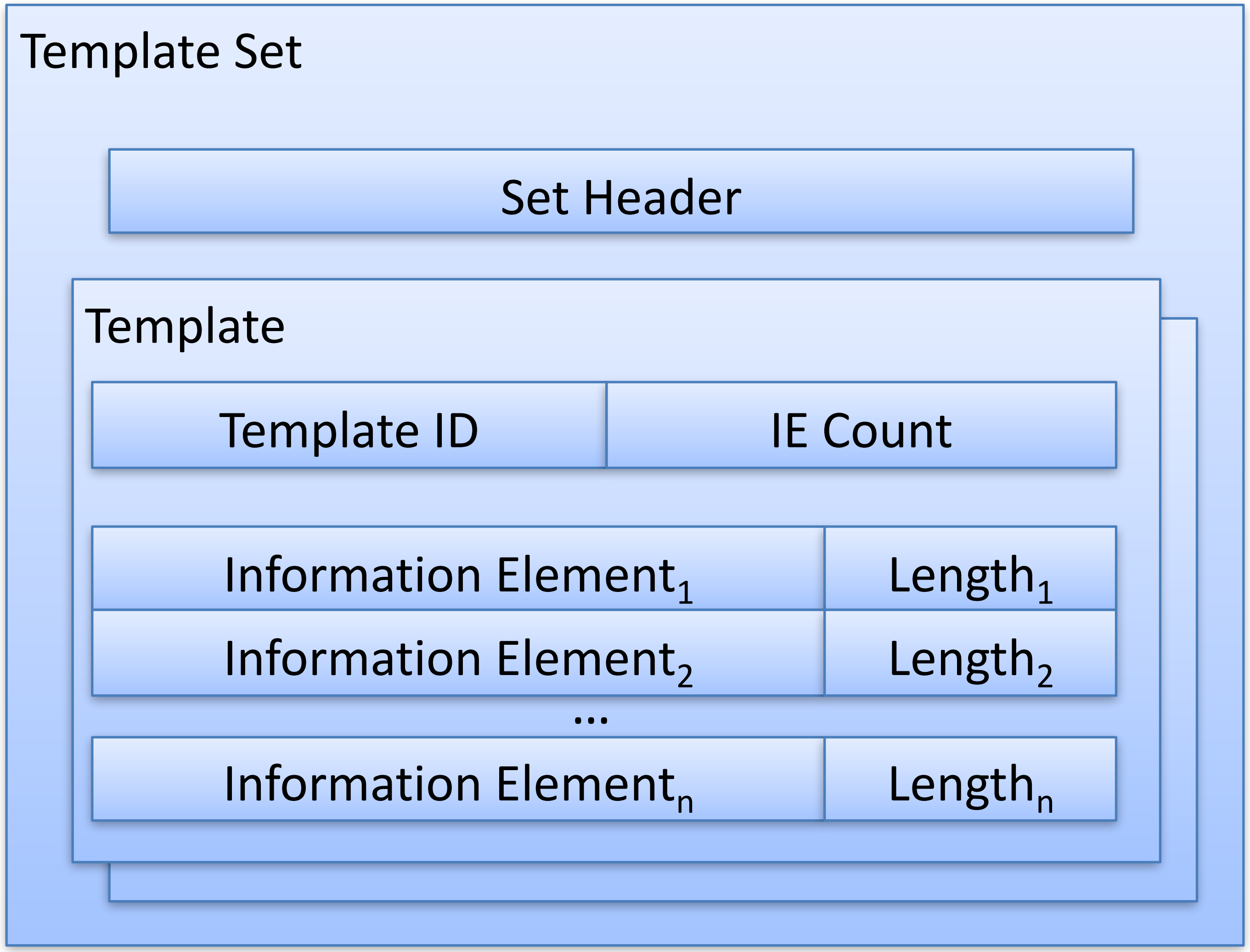
Version Number (10)
Length
Export Time in seconds
Sequence Number
(dropped message detection)
Observation Domain ID
(Template context)

Set ID
(defines a Set’s type (e.g. Template Set);
links Data Sets to Templates)
Length

Templates and Information Elements

- A **Template** describes the structure of **Data Records** within a Data Set.
- Templates identified by **Template ID**…
- …which corresponds to **Set ID** in the Set Header of the Data Set.
- Templates are composed of {*Information Element (IE), length*} pairs.
- IEs provide field type information for Templates.
    - If a Template defines a table, the IEs name the columns

Template Structure



Template Set

Set Header

Template

Template ID | IE Count

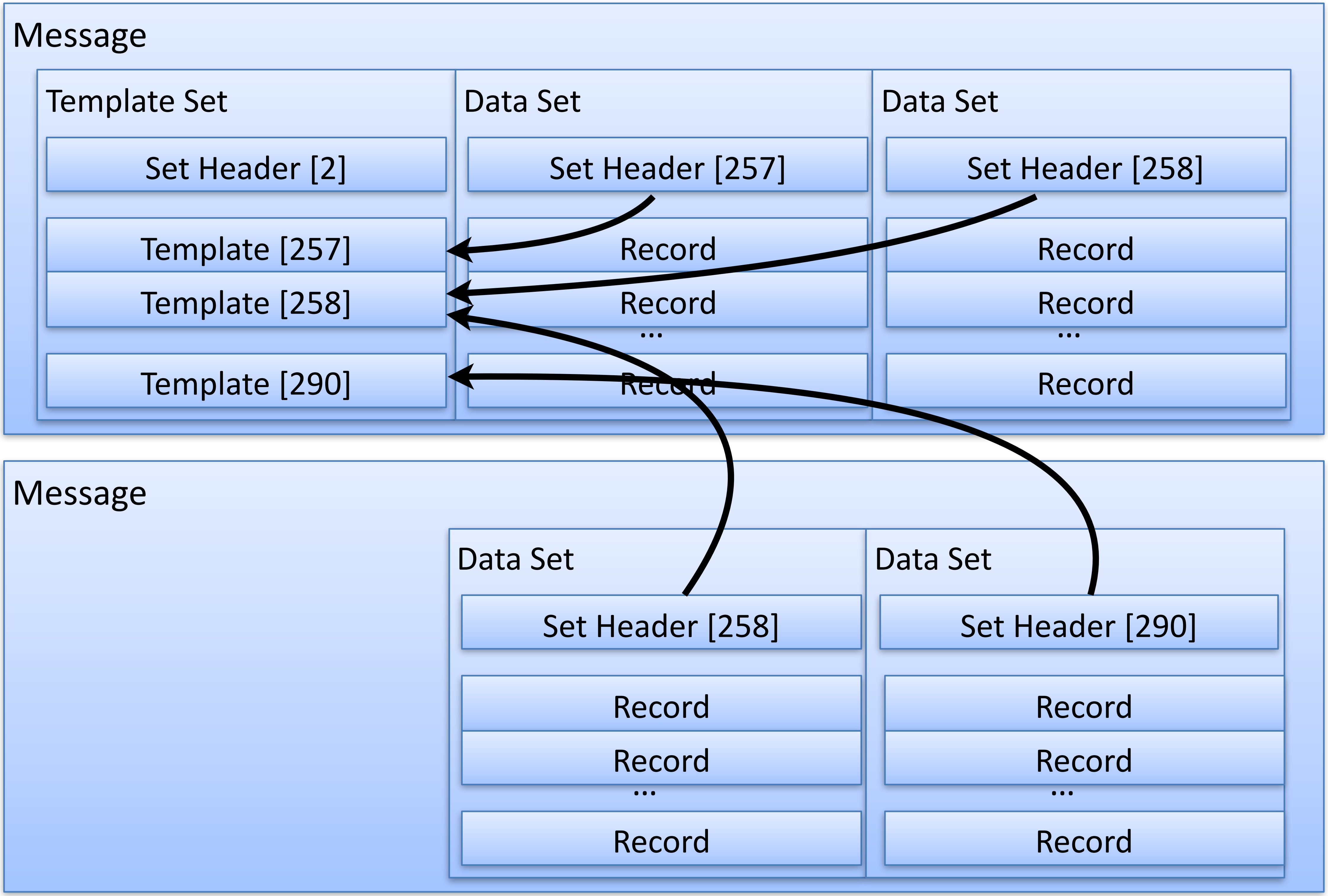
Information Element$_1$ | Length$_1$

Information Element$_2$ | Length$_2$

…

Information Element$_n$ | Length$_n$

Templates and Data Sets



Message

Template Set

Set Header [2]

Template [257]

Template [258]

Template [290]

Data Set

Set Header [257]

Record

Record

…

Record

Data Set

Set Header [258]

Record

Record

…

Record

Message

Data Set

Set Header [258]

Record

Record

…

Record

Data Set

Set Header [290]

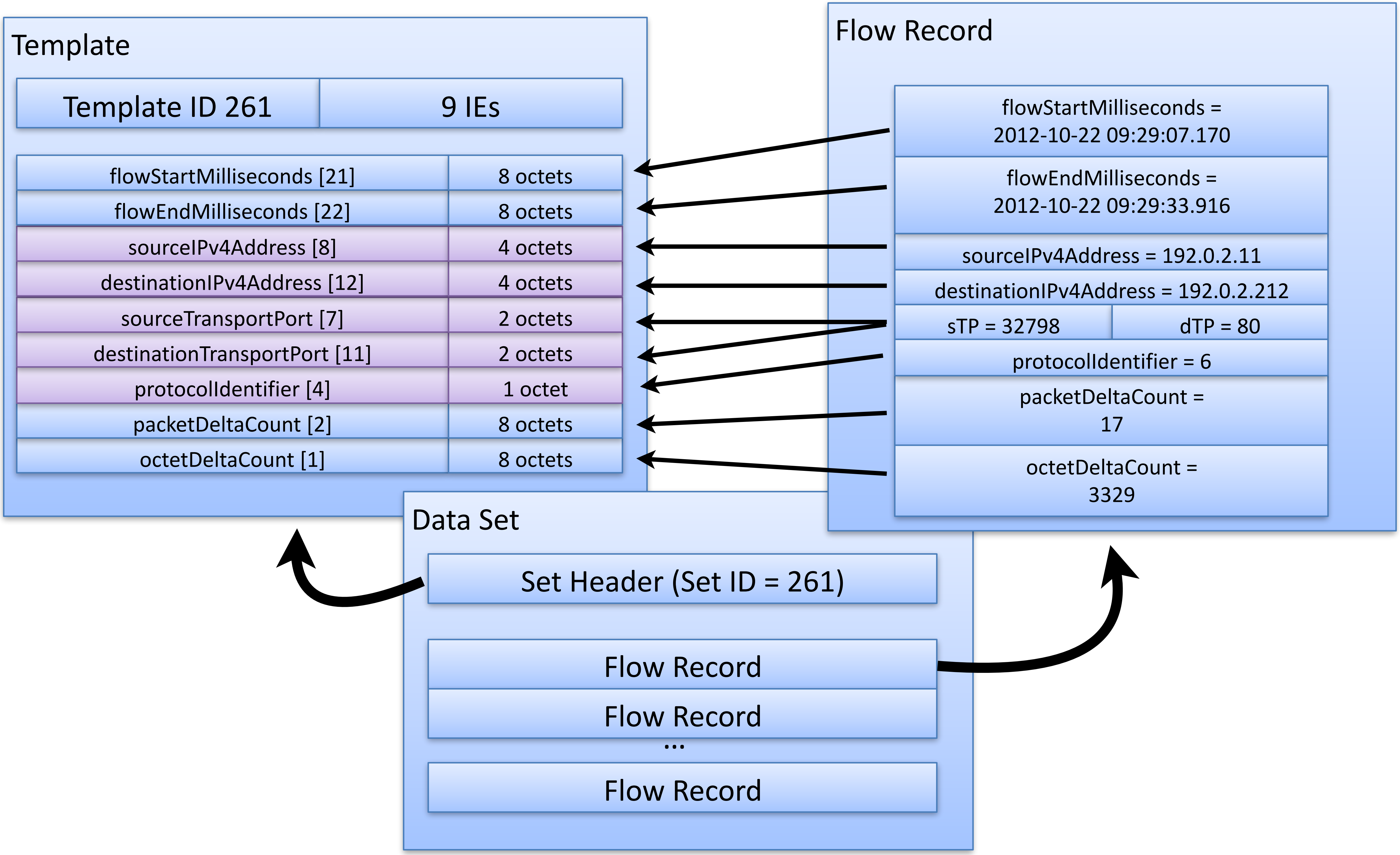
Record

Record

…

Record

A Simple Flow Record



Template

Template ID 261	9 IEs
flowStartMilliseconds [21]	8 octets
flowEndMilliseconds [22]	8 octets
sourceIPv4Address [8]	4 octets
destinationIPv4Address [12]	4 octets
sourceTransportPort [7]	2 octets
destinationTransportPort [11]	2 octets
protocolIdentifier [4]	1 octet
packetDeltaCount [2]	8 octets
octetDeltaCount [1]	8 octets

Flow Record

flowStartMilliseconds = 2012-10-22 09:29:07.170

flowEndMilliseconds = 2012-10-22 09:29:33.916

sourceIPv4Address = 192.0.2.11

destinationIPv4Address = 192.0.2.212

sTP = 32798

dTP = 80

protocolIdentifier = 6

packetDeltaCount = 17

octetDeltaCount = 3329

Data Set

Set Header (Set ID = 261)

Flow Record

Flow Record

…

Flow Record

Information Model

- Information Model (www.iana.org/assignments/ipfix): 400+ elements covering nearly all common flow collection use cases:
- “traditional 5 tuple”:
  sourceIPv4Address, destinationTransportPort, etc.
- Packet treatment:
  ipNextHopIPv4Address, bgpDestinationAsNumber, etc.
- Timestamps to nanosecond resolution:
  flowStartSeconds, flowEndMilliseconds, observationTimeMicroseconds, etc.
- IPv4, IPv6, ICMP, UDP, TCP header fields:
  ipTTL, icmpTypeIPv6, tcpSequenceNumber, etc.
- Sub-IP header fields:
  sourceMacAddress, wlanSSID, mplsTopLabelStackSection, etc.
- Various counters:
  packetDeltaCount, octetTotalSumOfSquares, tcpSynTotalCount, etc.
- Flow metadata information:
  ingressInterface, egressInterface, flowDirection, ingressVRFID, selectorID, etc…

Information Model Extension

- Information elements may also be scoped to an SMI **Private Enterprise Number**
  - Commercially sensitive Information Elements
  - Pre-standardization activities
  - Experimentation
- Used extensively in QoF (https://github.com/britram/qof/wiki/Information-elements)
- Registry of standard Information Elements (http://www.iana.org/assignments/ipfix) can be extended following the guidelines in RFC 7013.

Information Element Length

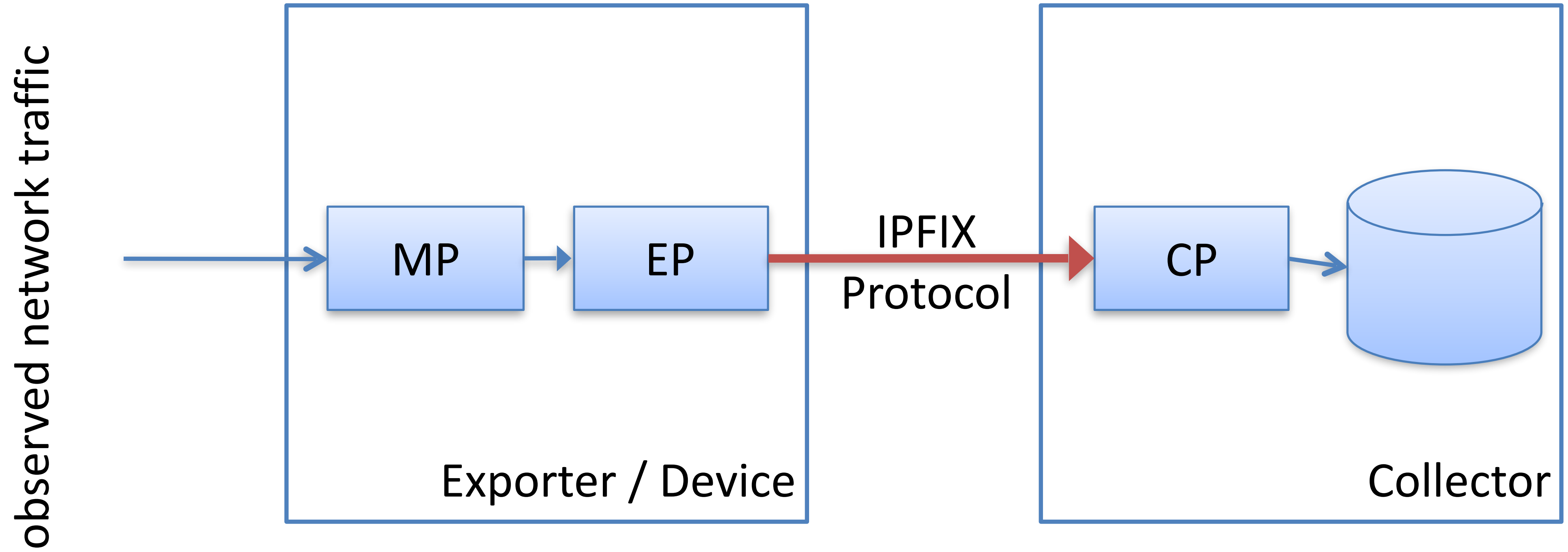
- Each Information Element has a **native length** associated with its data type:
    - IPv6 addresses are 16 octets, IPv4 addresses are 4 octets, and so on.
- **Reduced-length encoding** can be used to increase export efficiency.
    - e.g., a Template for use with packet and octet count that will never overflow 232 can be encoded in 4 octets, instead of the native 8.
    - e.g., interface numbers: many devices can get away with 1 byte.
- **Variable-length encoding** can be used to efficiently export variable length data.
    - One-byte length-prefix up to 254 bytes (i.e., Pascal-style string)
    - Three-byte length prefix up to 65515 bytes
    - e.g. wlanSSID, which is a string.

Options

- **Options Templates** are a special type of Template used to define records (Options) bound to a specified scope.
    - A scope can define an entity in the real world or the IPFIX Architecture or Protocol (e.g., an Exporting Process, a Template), or a property of some set of flows.
- While Flow Records describe Flows, Options Records describe things **other than Flows**:
    - information about the collection infrastructure,
    - metadata about flows or a set of flows, or
    - common properties of a set of flows.

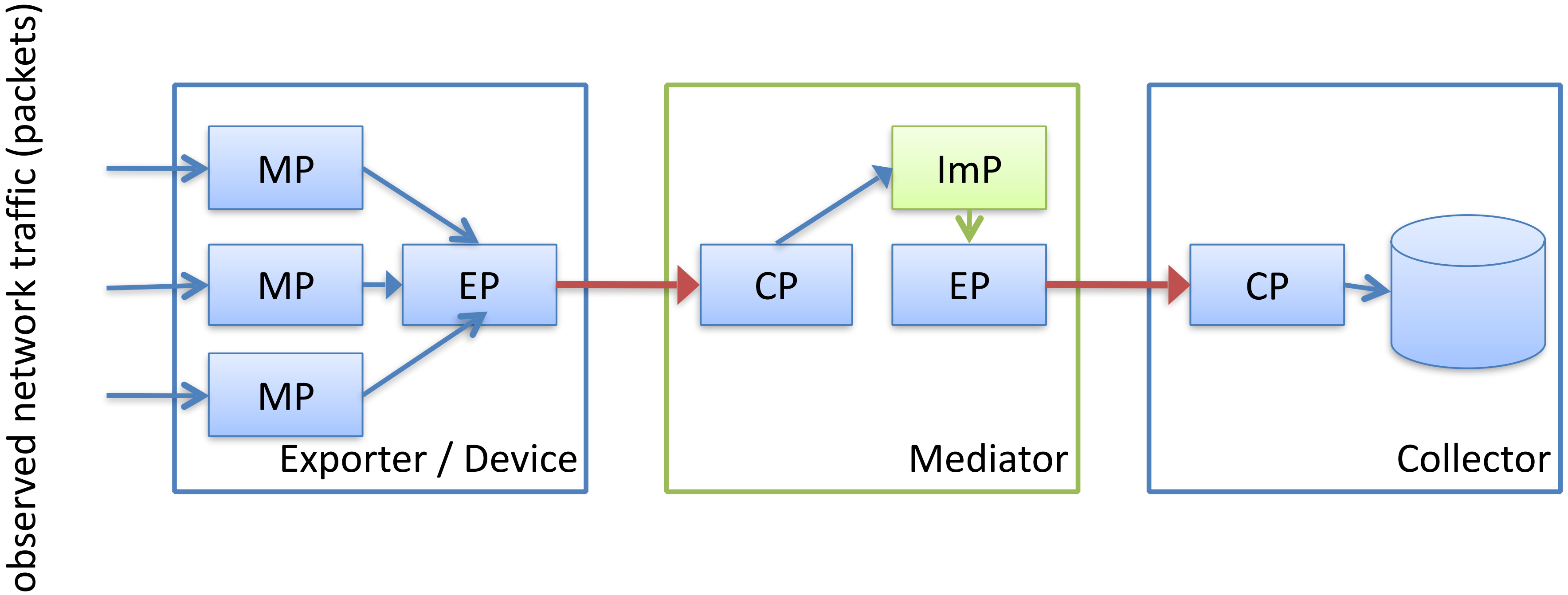
Architecture

- IPFIX transports data records generated by a **Metering Process** (MP) in Messages over SCTP, TCP, UDP from an **Exporting Process** (EP) to a **Collecting Process** (CP).
- IPFIX Messages can also be collected in files (RFC 5655) for storage or transport.



IPFIX Mediators

- Mediators collect, transform, and re-export IPFIX Message streams.
- Framework in RFC 6183, protocol considerations in RFC 7119.
- Intermediate Processes (ImP) transform data:
  - Anonymization (RFC 6235), Aggregation (RFC 7015)
  - Filtering, proxying, mux/demux, protocol translation, etc.



Transport Protocols

- SCTP
  - Mandatory to implement
  - Provides partial reliability, multiple streams
  - Some issues with implementation
- TCP
  - Intended for transport of IPFIX across the Internet
  - or implementations on devices which do not support SCTP where security (via TLS) is important.
- UDP
  - No reliability or congestion awareness
  - Intended for deployment only on devices without SCTP support, and
  - only on dedicated networks within a single administrative domain
  - i.e., as a migration path for replacement of legacy collection infrastructures.

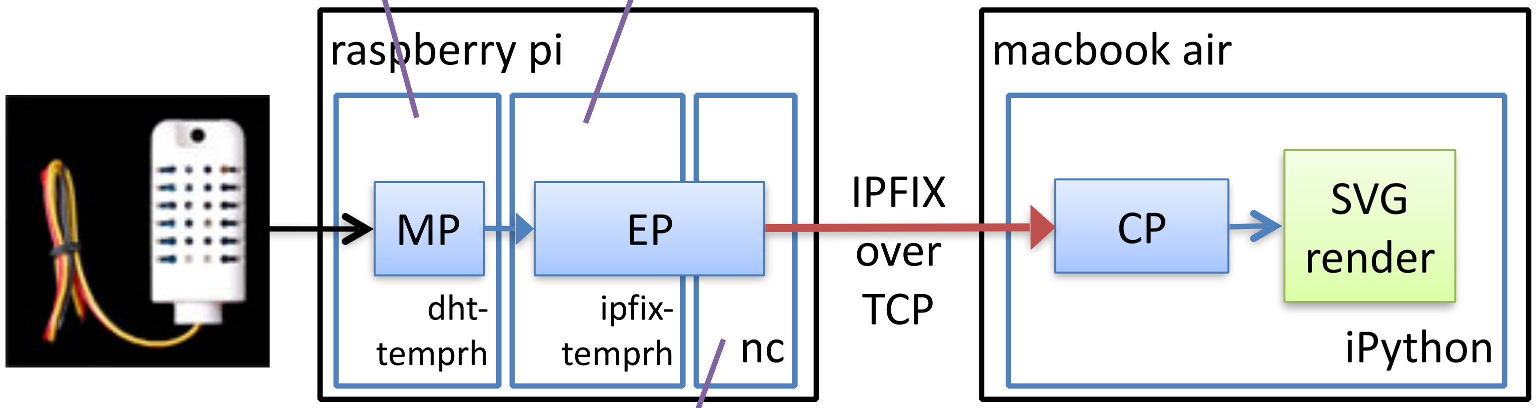
Lab:
IPFIX Data Structures and Applications

```
ipfix-tutorial/notebooks/
Introducing IPFIX.ipynb
```

Design: RH/Temp Exporter

dht-temprh:
periodically print
temp/rh to stdout

ipfix-temprh:
translate temp/rh to IPFIX
with static template



raspberry pi

MP

dht-temprh

EP

ipfix-temprh

nc

IPFIX
over
TCP

macbook air

CP

SVG render

iPython

AM2302
Temp/RH
Sensor

nc: send IPFIX
message stream
via TCP