Bidirectional Flow Export using IPFIX

draft-ietf-ipfix-biflow-00

http://www.ietf.org/internet-drafts/draft-ietf-ipfix-biflow-00.txt

Brian Trammell <bht@cert.org>

Elisa Boschi <elisa.boschi@hitachi-eu.com>

Thursday, November 9, 2006

IETF 67 - San Diego, California, USA

Motivation

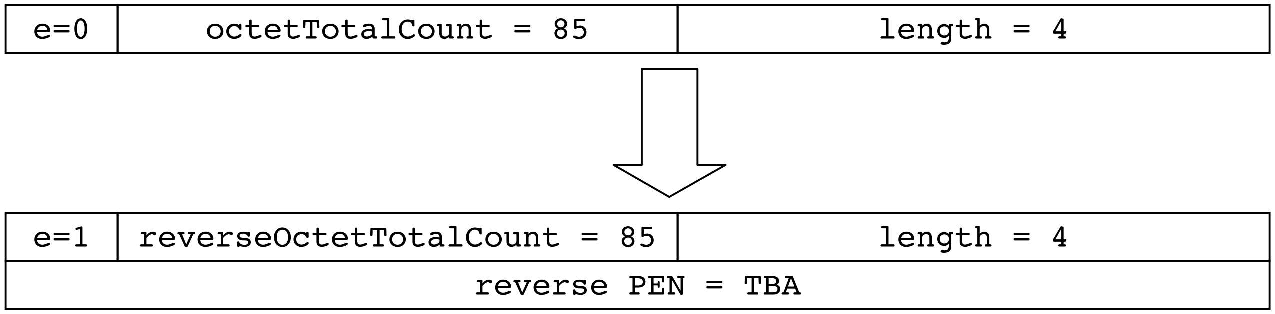
- Bidirectional flow information useful for a variety of use cases.
- Biflow matching becomes more efficient closer to the measurement interface, and often best addressed at the Metering Process itself.
- Need an efficient way to export this data using IPFIX.

Single Record Biflows

- Represent each bidirectional flow with a single record.
- Define “forward” direction as packets sent from the flow initiator.
- Define “reverse” direction as packets sent to the flow initiator.
- Assign direction to biflows using a variety of methods, according to application.
- Define new “reverse” information elements to represent values for reverse direction.

Reverse PEN

- Allocate an IANA private enterprise number (PEN) to the draft.



```
e=0 | octetTotalCount = 85        | length = 4

e=1 | reverseOctetTotalCount = 85 | length = 4
reverse PEN = TBA
```

- Information elements within this PEN IE number space correspond to the IETF number space, except that they apply to the reverse direction of a biflow.

Direction Assignment

- The largest remaining open issue: how to determine the "source" and the "destination" of a biflow.
- Previous revisions of this draft suggested direction be assigned according to Metering Process' best effort to determine the initiator (sender of the first packet) of the Biflow.
- This approach is not applicable in all cases.

Direction Assignment Methods (1)

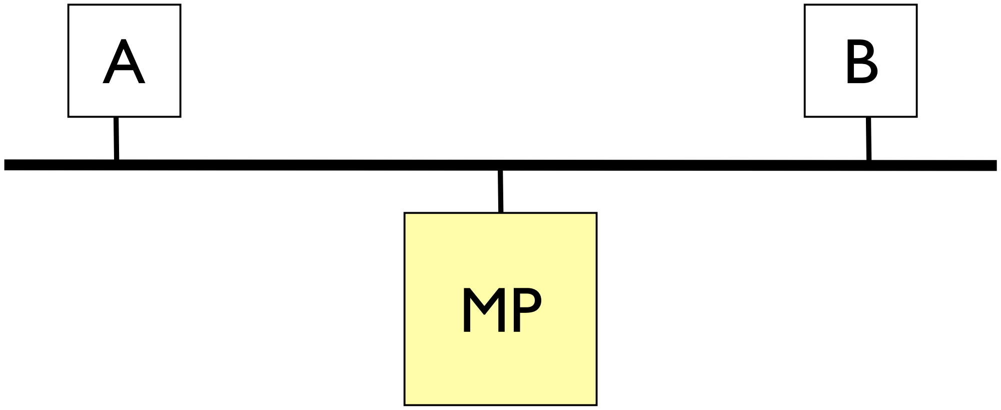
- By Initiator: “source” is source of packet initiating the communication (active open for TCP).
  - Assume the first packet seen is the first packet sent.
  - Validate through use of TCP flags, application protocol analysis (e.g. UDP DNS answer count), etc.
  - Requires synchronization of clocks among Metering Processes.
- By Interface/Address: “source” and “destination” assigned via membership in address set or side of a given interface.
  - Useful when defining a perimeter.
  - Does not require clock synchronization.
  - Not appropriate for applications where initiator is important.

Direction Assignment Methods (2)

- Random: “source” and “destination” assigned randomly.
  - The only additional information provided by biflow export is that two flows are related.
  - Places no restrictions on measurement system arrangement.
- Each of these are applicable to certain use cases, and will be selected by the draft as appropriate.

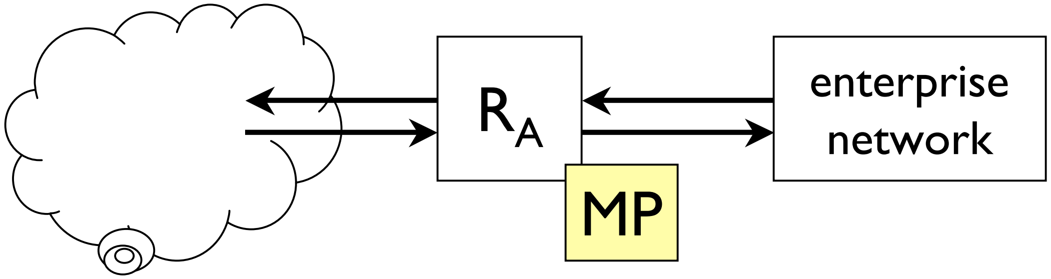
Local Network Metering

- Metering Process attached to a shared link layer (shared medium or switch span port)
- SHOULD assign direction by initiator.



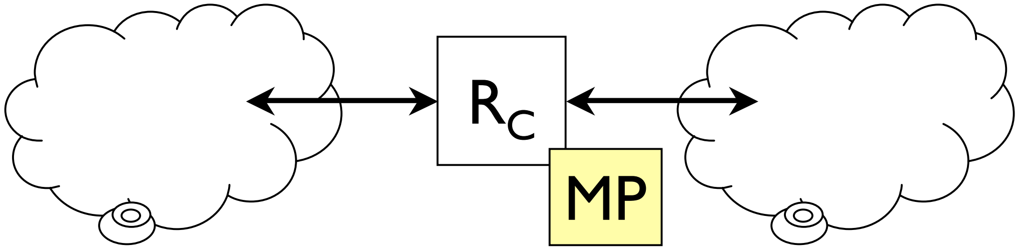
Perimeter Metering

- Attach Metering Process(es) to links at an enterprise/AS perimeter.
- SHOULD assign direction by perimeter
  - MAY assign by initiator if knowing the initiator is important AND clocks synchronized among MPs.



Metering within Transit AS

- Direction assignment by initiator difficult due to clock synchronization issues.
- Direction assignment by interface troublesome because addresses may move from one side to another of an MP during IGP/EGP updates.
- MAY assign direction randomly.



From Montréal to Prague

- ietf -00 (30 August 2006)
  - selected reverse PEN allocation policy
  - began to address direction selection
- ietf -01 (November 2006)
  - addresses remaining open issues with direction assignment as outlined herein.
  - will continue to incorporate WG comments.

Questions and Discussion