IPFIX Mediators

draft-kobayashi-ipfix-mediator-model-00.txt

(NTT) Atsushi KOBAYASHI

Keisuke ISHIBASHI

Tsuyoshi KONDOH

(Hitachi) Daisuke MATSUBARA

Introduction

- **After IETF69th, we have improved IPFIX Mediator draft.**

- **Mainly, this draft updates as follows.**
  - ☐ Describes arrangement of roles and functions for several nodes, such as IPFIX proxy, firewall and concentrator.
    - ■ This part is not enough to describe whole concept yet.
  - ☐ Defines internal components of IPFIX Mediator.
  - ☐ Adds IPFIX protocol considerations.
  - ☐ Refines solution scenario using IPFIX Mediator.

What is IPFIX Mediator ?

- **IPFIX Mediators have basically two types of mediation function.**
  - ☐ <u>IPFIX protocol Mediation</u>
    - Simply, it forwards input Flow Records.
    - IPFIX proxy, IPFIX distributor
  - ☐ <u>Flow Mediation</u>
    - Create renewed Flow Records from input Flow records
    - IPFIX Firewall, IPFIX concentrator

<u>IPFIX protocol mediation</u>

IPFIX → [CP] → [EP] → IPFIX

<u>Flow mediation</u>

IPFIX → [CP] → [MP] → [EP] → IPFIX
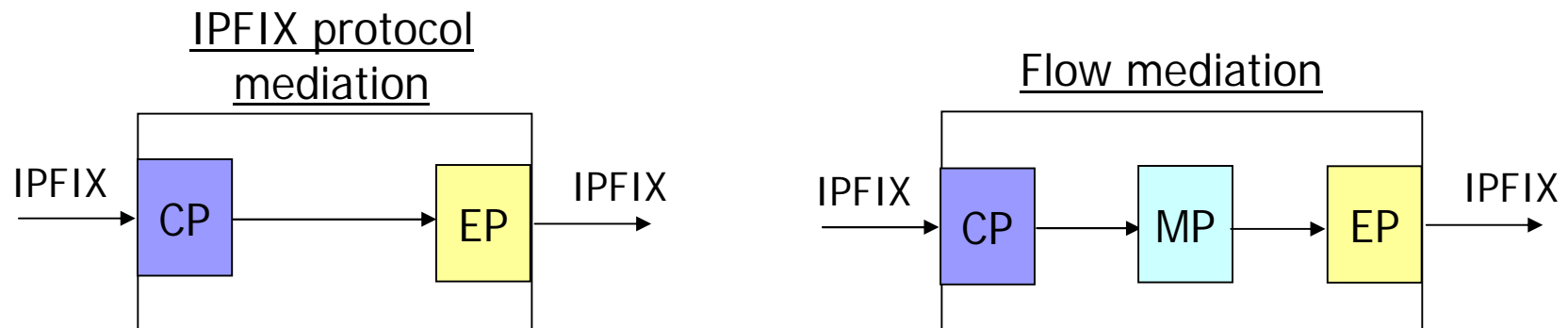
CP : Collecting Process
MP: Metering Process
EP: Exporting Process

What is IPFIX Mediator ? (cont'd)

- **IPFIX Mediators has basically two roles.**
  - ☐ <u>Acts as a guard to external domain instead of an original Exporter.</u>
    - ■ Try to guard a original exporter and networks.
    - ■ Prevents to reveal the network topology information, such as "exporterIPAddress" and "ipNextHopIPAddress".
    - ■ IPFIX proxy, IPFIX firewall
  - ☐ <u>Assists an original Exporter.</u>
    - ■ Complements the inability function of an original Exporter.
    - ■ Forwards Flow Record that the top collector required.
      - ☐ Distributes Flow records based on the Flow contents.
      - ☐ Aggregates Flow records.
      - ☐ Adds other fields into Flow records. For example, BGP Next-Hop, MPLS route distinguisher.
      - ☐ Anonymizes privacy field.
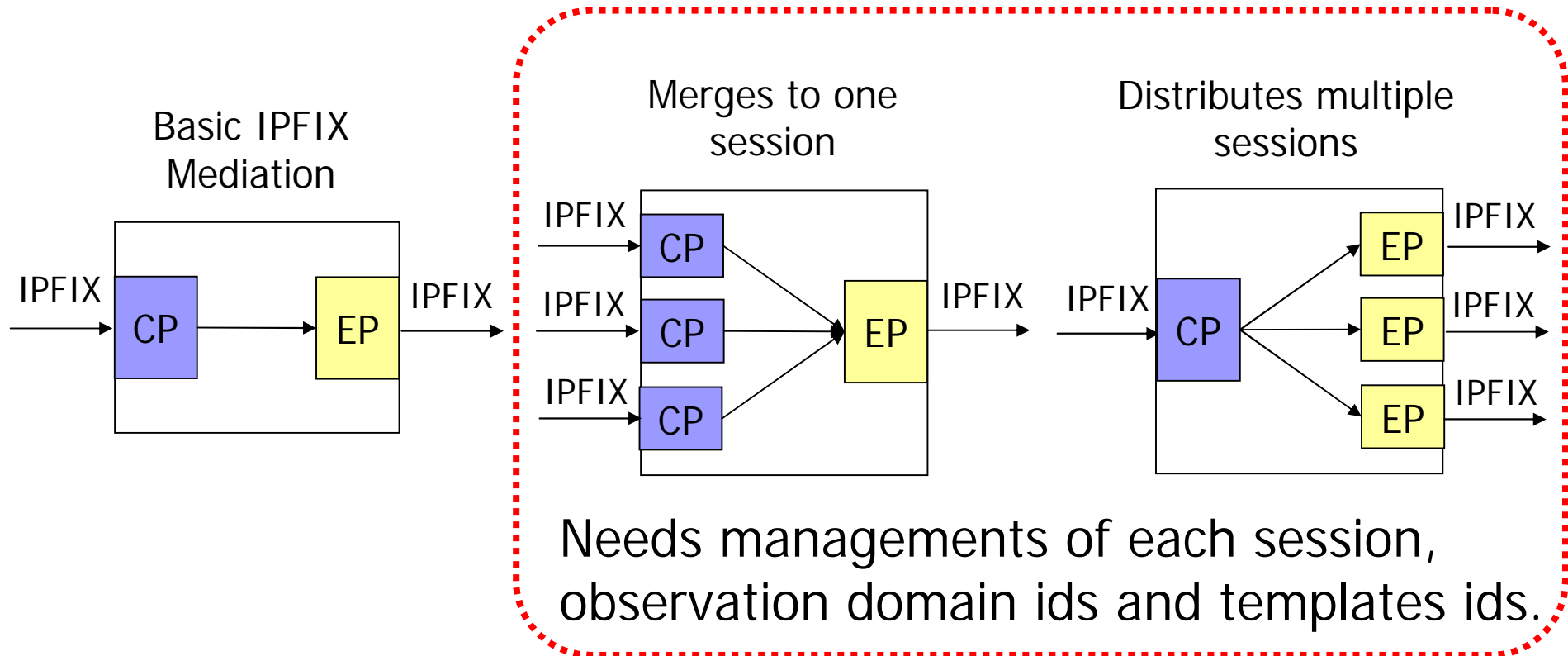   - ■ IPFIX concentrator, IPFIX distributor

What is IPFIX Mediator ? (cont'd)

- Total picture of IPFIX Mediator.
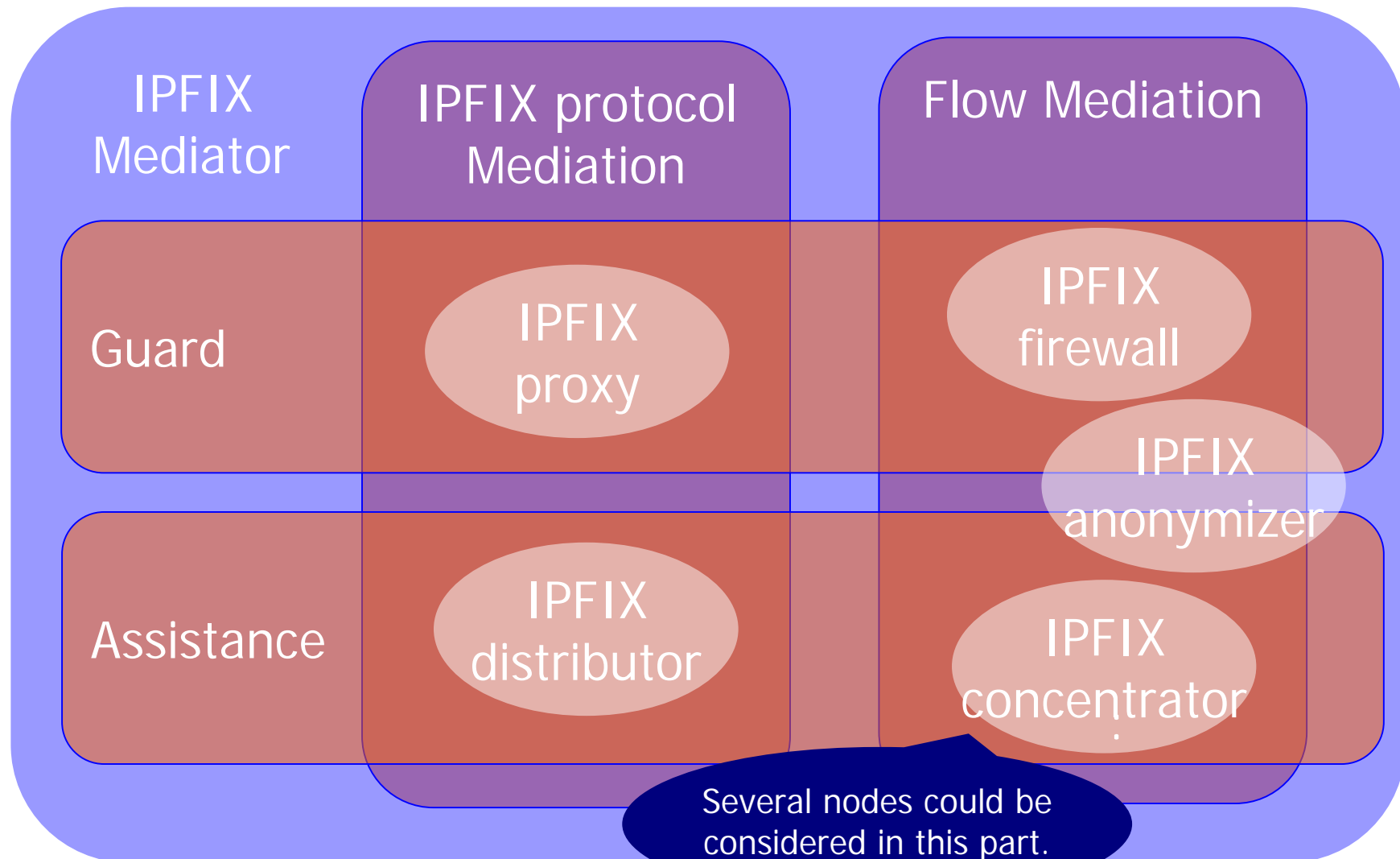
IPFIX Protocol Mediation

- IPFIX protocol mediation handles multiple collecting sessions and multiple exporting sessions.
  - □ Merges from multiple sessions to one session.
  - □ Distributes from one session to multiple sessions

Basic IPFIX Mediation

Merges to one session

Distributes multiple sessions

Needs managements of each session, observation domain ids and templates ids.

Flow Mediation

- **MP is consisted of following sub-processes.**
  - ☐ <u>Aggregation process</u> : creates aggregated Flow Records.
  - ☐ <u>Modification process</u> : deletes, adds some fields and modifies the value of some fields in the Flow Records.
    - ■ Anonymizes and hides the privacy or the topology information.
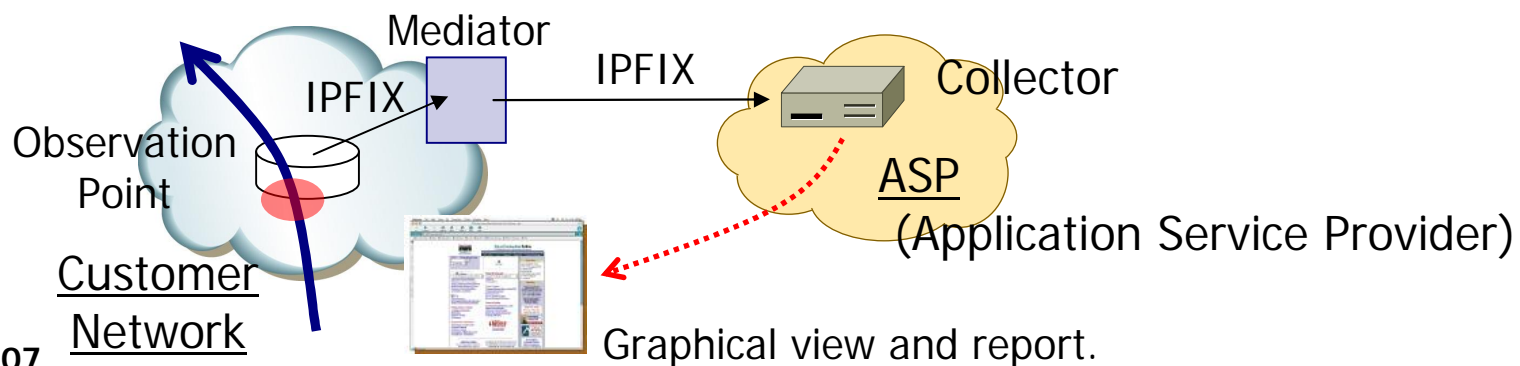 - ☐ <u>Selection process</u> : Filtering Flow Records based on Flow contents.
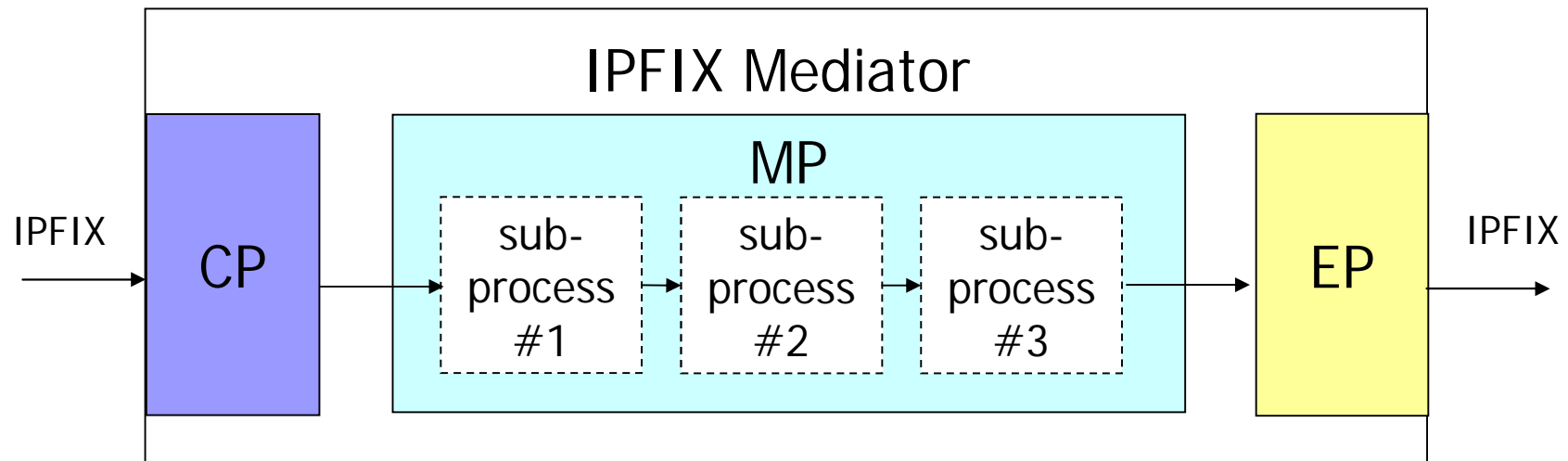
Any sequence and combination is configured by the user.

IPFIX Protocol Considerations

- **Export time issue**
  - ☐ Take care of delta time field, if it rewrites the export time.
- **Observation Domain ID management**
  - ☐ Generally, needs to be unique per IPFIX Mediator. Simply, it's zero.
  - ☐ Needs to manage collecting ODID and the exporting ODID, if it handles the multiple sessions.
- **Template ID management**
  - ☐ Generally, needs to be unique per the exporting ODID.
  - ☐ Needs to manage template id with ODID and session information.
- **Transport Session Management**
  - ☐ How to handle exporting sessions, if the collecting session resets.
- **Option Template Management**
  - ☐ Needs to rewrite the scope fields, if observation domain id and template id are rewritten.
- **Reporting of Exporter Information**
  - ☐ How to notify the original exporter information to the final collector.
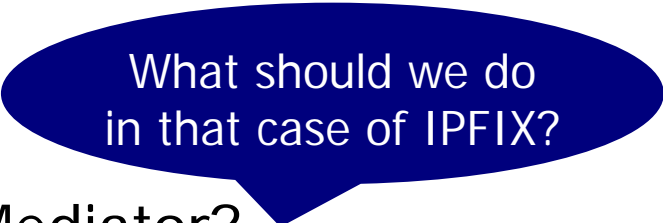
Solution Scenario using IPFIX Mediators

- **Large scale traffic monitoring system**
  - ☐ Thanks to mediators, the traffic collecting system consists of hierarchical architecture.

- **Assist an old router function.**
  - ☐ It adds the derived packet property field, such as BGP Next-hop and AS path information.

- **Exchange Flow Records between different domain.**
  - ☐ ASP provides the graphical view and reports of traffic data by sending monitored Flow Records to ASP.

Mediator

IPFIX

Observation Point

IPFIX

Collector

ASP
(Application Service Provider)

Customer Network

Graphical view and report.

Summary

- We present a taxonomy of IPFIX Mediator use-cases through two axes, types and roles.
- The concept of IPFIX Mediator has been described mainly.
  - □ IPFIX protocol considerations, and the definement of several nodes need discussion with IPFIX members.
- Implementation of IPFIX Mediator is ongoing.
- Discussion
  - □ Does it deserve the WG work item?
  - □ Do NW operators stand in need of Mediator?
    - Some collectors have a proxy function based on the NetFlow v.5.
    - Some collectors can cascade itself, whole system can consist of hierarchical architecture.

What should we do in that case of IPFIX?