

Standardization Activities (IPFIX, PSAMP)

Tanja Zseby

IP Flow Information Export (IPFIX)

Goal: Find or develop a protocol for exporting IP traffic flow information from routers and probes

- Metering to be integrated in general purpose IP routers and other devices (probes, middleboxes)
- Target Applications: Accounting, Traffic Engineering, QoS monitoring, Intrusion detection
- Status:
 - Requirements done (RFC3917)
 - NetFlow 9 (RFC3954) selected as basis for protocol development
 - Protocol specification nearly finished
 - Architecture, Data Model in progress

Packet Sampling (PSAMP)

Goal: Configuration and reporting of sampling schemes on routers and probes

- Define standardized way to express sampling schemes for configuration and to inform application
- MIB for sampling configuration
- Export protocol (relations to IPFIX)
- Status:
 - Framework close to last call
 - Description of Methods close to last call
 - Information Model, MIB in progress
 - Export Protocol: Based on IPFIX

Current Documents

• IPFIX Requirements (Co-author)

- Authors: J. Quittek (NEC Europe Ltd.), T. Zseby (FOKUS), B. Claise (Cisco Systems), S. Zander (Swinburne University)
- Latest Version: RFC3917, October 2004
- Status: now RFC3917

• IPFIX Applicability Statement (Editor)

- Authors: Tanja Zseby, FhG FOKUS, Elisa Boschi (Hitachi/FOKUS), Reinaldo Penno, Nortel Networks, Nevil Brownlee, CAIDA, Benoit Claise, Cisco Systems
- Latest Version: draft-ietf-ipfix-as-03.txt, October 2004
- Status: include input from last IETF, more examples needed

• IPFIX for Export of Per-Packet Information (Editor)

- Authors: Guido Pohl (FOKUS), Lutz Mark (FOKUS), Elisa Boschi (Hitachi/FOKUS)
- Latest Version: draft-pohl-perpktinfo-00.txt , October 2004
- Status: presented at last IETF, separate document or in IPFIX or PSAMP protocol ?

• PSAMP Sampling and Filtering Techniques for IP Packet Selection (Editor)

- Authors: Tanja Zseby (FhG Fokus), Maurizio Molina (DANTE), Fredric Raspall (NEC Europe Ltd.), Nick Duffield (AT&T Labs), Saverio Niccolini (NEC Europe Ltd.)
- Latest Version: draft-ietf-sample-tech-05.txt, October 2004
- Status: all issues solved, next version goes to last call

IPFIX Requirements (now RFC 3917)

- Requirements for the IPFIX protocol
- Investigated target applications
 - Usage-based Accounting
 - QoS Monitoring
 - Attack/Intrusion Detection
 - Traffic Engineering
 - Traffic Profiling
- ➔ Table with mandatory/optional features for future IPFIX protocol
- ➔ Evaluation of candidates was based on this

IPFIX Applicability

- Show how (target) applications can use IPFIX
 - How can IPFIX be deployed in concrete scenarios
 - When are which optional features useful
 - What else can be done with IPFIX (IP *Flexible* Information Export ?)
 - What not to do with IPFIX
- Describe relations and potential interfaces to other frameworks/ working groups
 - What is the relation between IPFIX and other WGs/frameworks (PSAMP , IPPM, AAA, RTFM, RMON)
 - How would IPFIX fit into existing frameworks (potential integration/interfaces) e.g. Connections to AAA

IPFIX Export of Per-Packet Information

- Proposal to use IPFIX to export per packet information (e.g. packet IDs)
 - Required e.g. for passive measurement (e.g. one-way delay, jitter...)
- Per-packet information export can be done:
 - Using one flow record (“one-packet flow”)
 - Using two different records (flow and packet properties)
- Draft proposes to separate flow from packet information
- Packet maintain references (indices) to the flow they belong to
- ➔ Solution reduces overhead and requires less storage capacity

PSAMP Packet Selection

- Description of Filtering and Sampling Methods
 - What information needs to be provided to describe the method
 - Basis for Information Model
 - Configuration of methods
 - Reporting of technique in use to collector

Filtering: A filter is a Selector that selects a packet ***deterministically*** based on the ***packet content***, or its treatment, or functions of these occurring in the selection state. Examples include match Filtering, and Hash-based Selection.

Sampling: A Selector that is not a filter is called a Sampling operation. This reflects the intuitive notion that if the selection of a packet cannot be determined from its content alone, there must be some type of Sampling taking place.

Schemes and Parameters

Selection Scheme	Deterministic Selection	Content-dependent	Category
Systematic Count-based	X	—	Sampling
Systematic Time-based	X	-	Sampling
Random n-out-of-N	-	-	Sampling
Random Uniform probabilistic	-	-	Sampling
Random Non-uniform probabil.	-	(X)	Sampling
Random Non-uniform flow-state	-	(X)	Sampling
Field match filter	X	X	Filter
Hash Function	X	X	Filter
Router state filter	X	(X)	Filter

Thank you for your attention !