# Flow Aware Packet Sampling


**Ram Krishnan/David Meyer – Brocade Communications**

**Ning So – Tata Communications**

# INTRODUCTION

- Current Issues
  - Uniform packet sampling in networking devices
  - Sample long-lived/short-lived, large/small flows equally
  - Large percentage of samples is large flows (aka top-talkers)
  - Small flows -- typical cause of security threats like Denial of Service (DOS) attacks, Scanning attacks etc.
  - Small percentage of the bandwidth and a large percentage of the flow space
- Flow Aware Packet Sampling Solution
  - Automatically detect the top-talkers inline & real-time in networking devices
  - Sample only the small flows
  - Security threat detection more effective with minimal sampling overhead

Terminology:
-- Large flow(s): long-lived large flow(s)
-- Small flow(s): long-lived small flow(s) and short-lived small/large flow(s)

# SOLUTION DETAILS (1)

- Large Flow Recognition
  - Flow identification - all layer 2/3/4 formats supported by IPFIX
  - Define observation interval and observe the bandwidth of the flow over that interval
  - A flow that exceeds a certain minimum bandwidth threshold over that observation interval would be considered a large flow
  - Suggested technique for automatic recognition
  - Algorithm based on counting bloom filters
- Large Flow Classification
  - Recognized large flows can be broadly classified into 2 categories as detailed below.
  - Well behaved (steady rate) large flows, e.g. video streams
  - Bursty (fluctuating rate) large flows e.g. Peer-to-Peer traffic

# SOLUTION DETAILS (2)

- Recognized large flows can be sampled at low rate if desired
- Export large flows to a central entity, for e.g. Netflow Collector, using IPFIX protocol
- Top-talker reporting or further analysis

- Small Flow Processing
  - Sample small flows (excluding the large flows) at a normal rate using PSAMP protocol.
  - Examine small flows for determining security threats like DOS attacks (for e.g. SYN floods), Scanning attacks etc.

# NEXT STEPS

- Adopt as a work item in IPFIX working group – Informational RFC
  - Operator Interest
  - Vendor Interest

# ADDITIONAL WORK ITEMS

- Programmable parameters in switches and routers for automatic recognition of large flows
  - Option 1: Open APIs like REST API
  - Option 2: Data models like YANG
- Address gaps in IPFIX protocol
  - Option 1: Explicit protocol specification e.g. VXLAN, NVGRE
  - Option 2:
  - Virtualization/abstraction layer to central management entity
  - Flexible protocol type, packet offset/byte model interface to switches/routers