LISP-(IN)FIX

In-Network Analysis of Flow Information Export
IETF 111 LISP Working Group
Sharon Barkai
IPFIX Netflow Sflow FlowLogs..

- Very successful network sampling protocols widely deployed in switches, routers, and OS network stacks
- In given time-slots, or volume-slots, information regarding packets sharing a number of properties (flows), is sent from an exporter to a collector
IPFIX Aggregation

- In principle exporters can send IPFIX records to multiple collectors and collectors can receive records from multiple exporters.

- The protocol also pushes records from exporters to collectors every time-period without the need to request them individually.

- In practice the architecture is hierarchical (manager-agents) or typical ops in nature, geared for long-term collection and behavior analysis, plus manual debug.
LISP Relevance

• LISP Based aggregation vs administrative aggregation opens up new possibilities to address new challenges

• The focus of the draft is less on IPFIX statistics sampling of methodologies or sampling directive syntax ..

• Focus is on emerging a CFN like (Compute First Networking Or Contextual Functional Networking) .. architecture for realizing new possibilities in addressing new challenges

What is CFN?

• Collaboration between Huawei, BT, and Cambridge University

• Looking at the intersection of use cases, node and network technology for compute-first networking, i.e., in-network computing
  • Investigate driving use cases for CFN, leading to requirements for node and network technologies
  • Develop key networking and node technologies
  • Provide demonstration of key benefits in selected use case
## Whats New

<table>
<thead>
<tr>
<th>New Challenges</th>
<th>New Capabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Patterns</strong></td>
<td>There are new AI technologies which are able to detect exceptions to (normalized) patterns or detect known (normalized) attack patterns in split seconds using GPUs once were trained appropriately over time</td>
</tr>
<tr>
<td>Networks under constant siege, penetrations occur through application layer traps, in non significant end-points, start lateral movement internally across the network to prepare for a deeper wider attack</td>
<td></td>
</tr>
<tr>
<td><strong>Virtualization</strong></td>
<td>Flow level separation is also very advanced, the same mechanisms used to steer/route traffic logically differently can be used to steer samples differently in (v)switches and eBPF like programable interfaces</td>
</tr>
<tr>
<td>Traffic is virtualized mixed-mangled on any given layer3 sampled interface, traffic from different logical subnets appear anywhere, traffic from different clusters share the same interface for utilization</td>
<td></td>
</tr>
<tr>
<td><strong>Distribution</strong></td>
<td>Distributed edge and cloud-native computing has advanced, it is not needed to concentrate information in-order to separate signal and emerge global consistent (analysis) logic when problems are naturally distributed</td>
</tr>
<tr>
<td>Enterprise and Service provider edge traffic, and datacenter spine-leaf east-west traffic may be so massive that even flow record sampling concentration can not be centralized for analysis</td>
<td></td>
</tr>
</tbody>
</table>
Flow Sampling - Flow Mapping

Using LISP (IN)FIX

• Any exporter can algorithmically (5-tuple-mask) send flow samples to a logical (EID) designated collector-analyzer for any given application-group

• Neither sampling traffic nor AI computation is concentrated, all sampling traffic uses the sampling overlay network to bring samples to designated (logical) crunching point

• Exceptions (cond. stat. Interpolation + normalized pattern matching) can be detected and acted upon within the sampling (sub-sec) period, in a distributed manner
LISP-(IN)FIX Industry Value

- Transition from Ops to In-Network IPFIX aggregation
- Generates distributed realtime tangent AI probes
- New network probes which support advanced capabilities are very hard to insert to some environments which already have IPFIX:
  - Intense low-latency east-west spines and high-volume network cores melt probes
  - Highly regulated (severely attacked) lengthy certified industries such as hospitals, power-grids, energy, gov
- Over 100 installations to date are based on mediation collectors for out-of-box nfx training
- LISP net-native aggregation can mainstream this
Informational RFC

Per Flow Collector
- Subscribe (signal-free) to exceptions
- Setup LISP-INFIX XTR for SampNet

Per Flow Exporter
- Setup 5-Tuple-Mask to EID
- Setup LISP-INFIX XTR for SampNet
LISP-Nexagon

Geolocation Services Mobility Network
IETF 111 LISP Working Group
Sharon Barkai
Need for LISP-NEXAGON

- LISP-Nexagon defines the use of lisp in realizing mobility Geolocation Services

- Geolocation Services are all mobility edge service delivered in a GeoSpatial Context

- Geospatial Context abstracts locations
  
  ✓ Map data: roads, signs..
  
  ✓ Events: hazards, free-parking, hard-breaks..
  
  ✓ Upload Queues`; for on move (LL) vehicles
  
  ✓ Push Feeds: for subscribed vehicles
  
  ✓ Lqedgeres: who, where, what, when
  
  ✓ References: images, localization
LISP Addresses Key-Issues

• Context-Switching: avoiding slow frequent chatty resolutions over mobile and floods of updates to cached resolutions upon changes to compute-network conditions

• Service-Continuity: supporting-maintaining connectionless point-to-point and point-to-multi-point sessions between vehicles and mobility services over mobile while:
  ▶ modems switch carriers for best receptions
  ▶ services dynamically reallocated-recovered

• Geo-Privacy: decouple clearly the RTR layer from the Geolocation Services Layer
Thank You

Backup
Mobility Geolocation Cycles

Edge Data Processing
Curate, Filter, Localize data, Track data subscribers, Reduce, Filter, Cache Store & Forward, Flatten-Curve

Bridge BW/Latency Gaps:
Tbps v2e vs Gbps e2c
Sub-sec vs Multi-sec

Data Production
Publish data v2e (unsolicited)
Fetch data v2e (ledgered)

Data Consumption
Pull data e2v (unsolicited)
Push data e2v (subscribed)

1. c2e cloud to edge
2. e2c edge to cloud
3. v2e vehicle to edge
4. e2v edge to vehicle
1. SID: Service ID (HID-EID)
2. VID: Vehicle ID (EID)
3. LID: Location ID (HID)