Extending IP Flow-Based Network Monitoring with Location Information

draft-irtf-nmrg-location-ipfix-03

Olivier Festor, Abdelkader Lahmadi,
Rick Hofstede, Aiko Pras

IM 2015- NMRG Meeting

Ottawa, Canada, 2015

Status

- Status:
  - Presented in IETF 83, IETF 87, IETF 90
  - Presented in several NMRG meetings for discussion and feedback
  - Latest version: http://tools.ietf.org/html/draft-irtf-nmrg-location-ipfix-03
- Changes since IETF 90:
  - More use cases
  - Applicability of associating IP Flows with metering processes location
  - Implementation guidelines: metering process and collector sides

Motivation and scope

- Aggregated view of network traffic
  - IPFIX, NetFlow
  - But, only over time
- Monitoring network traffic usage in space
  - How much network traffic is generated in a specific location?
- Coupling space and time to understand network usage
  - Associate IP Flows to the location of their observation point

Use cases

- Mobile traffic
  - Exporter location can be of interest
  - Where often do users interact with their phones?
  - How many applications does a user run in a specific location?
- Virtualized environments
  - Virtual machines change location during migration and replication
  - What are the current locations of flows processed by VMs ?

Location information

- Geographic location
  - Numerical data format
  - Point: latitude, Longitude and altitude
  - Circle: point with uncertainty (radius)
- Civic location
  - Textual information
  - Location in buildings: postal address, approximated information (living room, office 123 building 2, …)

Applicability

- Management applications require knowing the location of the device
  - Space, time and volume of traffic
- Per location usage-based accounting
- Traffic profiling: traffic distribution in a specific location
- Security applications: detect unusual location-related communication patterns

Enabling location extensions

- Extend metering processes
  - Selection of a localisation method (GPS, network, …): accuracy, saving battery life, configuration parameter
  - Build a data record with location information using appropriate template
- Location information for each IP flow
  - Single location: first observed packet or last observed packet
  - Multiple locations: a sample of locations, starting location and ending location

Flow expiration

- Several expiration conditions
  - No observed packets, resource constraints
  - Regular expiration for long-running flows
  - Section 5.1.1 of [RFC5470]
- Location or distance based expiration
  - The device changes its location
  - Long-running flows: expire them every upon a configured distance value in meters
  - Unavailability of location information

Collecting Process's Side

- Metering process should transmit the set of location specific templates

- Unavailability of location information
  - Stop resending location templates

Information Elements

- **geospatialLocationLat**: coordinate information value of the latitude
- **geospatialLocationLng**: coordinate information value of the longitude
- **geospatialLocationRadius**: radius value of location using a circular area (known certainty)
- **CivicLocationValue**: civic address
- **deviceId**: identifier of the physical device acting as IPFIX exporter

IPFIX template: geographic location

- Point record: there is no known uncertainty

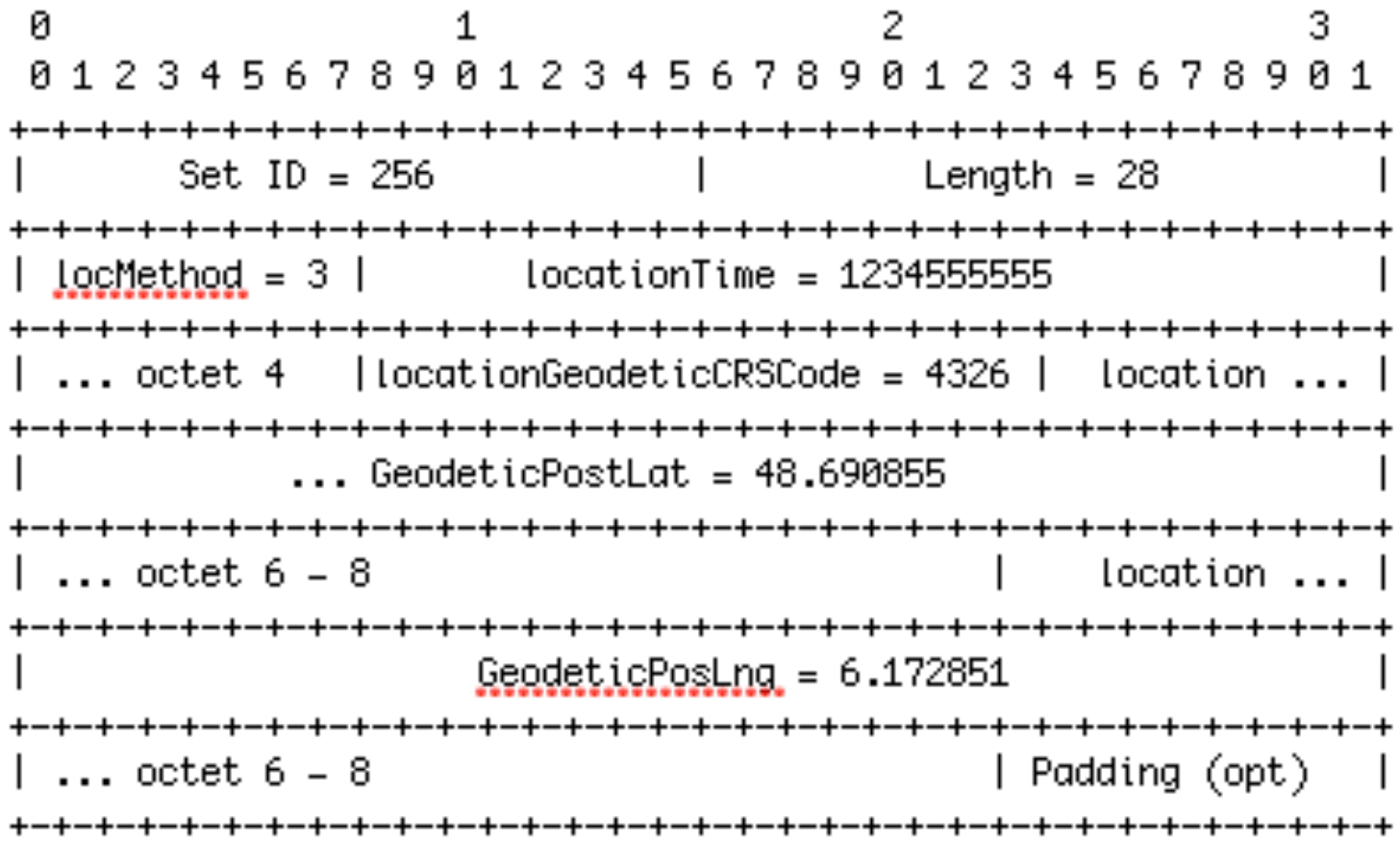

Figure 2: Data record of a geodetic 2D point location

Proof of Concept: Android devices

Start time	Src IP Addr:Port	Pkts	Bytes	Latitude	Longtitude
20:19:21.852	173.194.40.113:443	9	2730	48.690855	6.172851
20:21:42.307	91.202.200.229:80	13	9137	48.690855	6.172851
20:22:38.084	73.194.40.113:80	8	1799	48.690855	6.172851
…					
21:17:13.498	173.194.45.80:443	12	2830	48.713145	6.17526
21:17:13.498	10.21.20.232:49233	15	2301	48.713145	6.17526
21:17:16.919	10.21.20.232:15572	1	72	48.744506	6.154815

Conclusion

- Associate location of the metering process to IP Flows
  - Geographic location information in the Internet is growing
  - Cars, mobile devices, Virtual machines, Sensors
- Interesting use cases
  - Location aware network traffic usage
  - Verification of flows processing locations
  - Measurement applications
- Security considerations
  - IPFIX/NetFlow messages carrying location information should be signed and encrypted