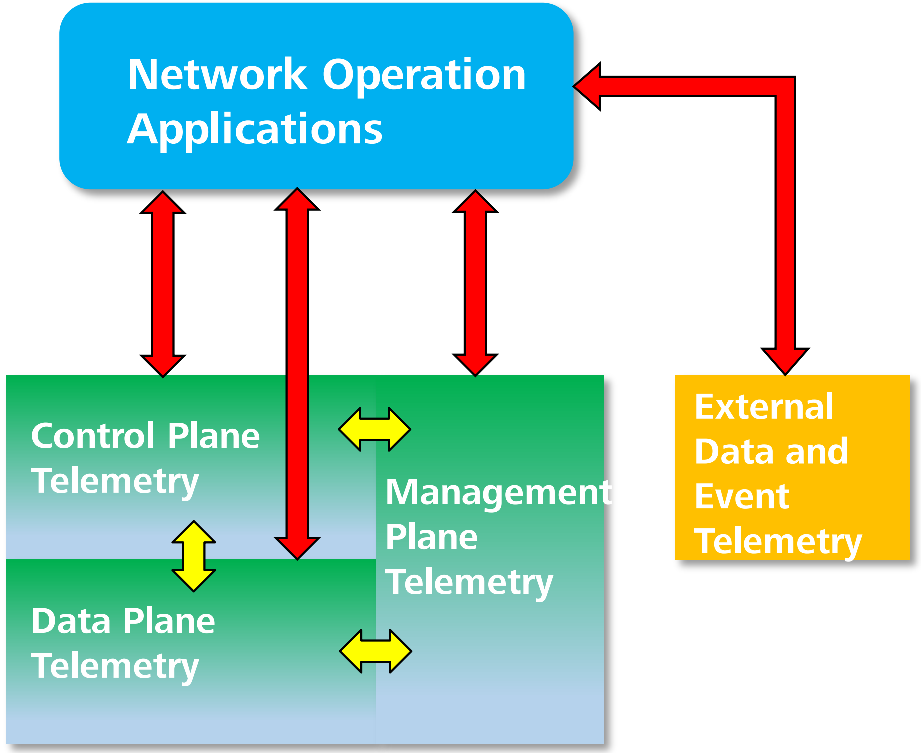
Network Monitoring Protocol (NMP)

draft-gu-network-monitoring-protocol-00

Yunan Gu, Shunwan Zhuang, **Zhenbin (Robin) Li**

2018-07-18

Network Telemetry Framework (NTF)


Network Operation Applications
Control Plane Telemetry
Management Plane Telemetry
Data Plane Telemetry
External Data and Event Telemetry

E2E Solution to Facilitate Machine Learning and Big Data Analytics

	Data Source	Data Subscription	Data Generation & Processing	Data Export	Data Analytics & Storage
Management Plane	YANG Data store	gRPC YANG PUSH	Dynamic network probe (DNP)	gRPC, YANG Push UDP	Other Huawei Tools ONAP pnda OPENTSDB openstack HDFS kafka logstash Spark Apache Zookeeper
Control Plane	Control Protocol, Network State	NETCONF/YANG, BGP	Soft DNP	BMP **NMP**	
Data Plane	Flow/Packet Statistics & States	NETCONF/YANG YANG FSM	INT/iOAM IPFPM Hard DNP	IPFIX UDP	

Motivation & Introduction

- The control plane monitoring, i.e., monitoring the running status of control protocols, enables the evolution towards automated network OAM.
- Network monitoring protocol (NMP) is proposed to collect the protocol running status data, e.g., protocol PDUs and protocol statistics, and export the collected data to the NMP monitoring station for analysis, which facilitates the network troubleshooting.
- The monitored protocols include IGP (ISIS/OSPF) and other control protocols. NMP for ISIS (IMP) are specifically defined in this draft to showcase the necessity of NMP.

Use Cases

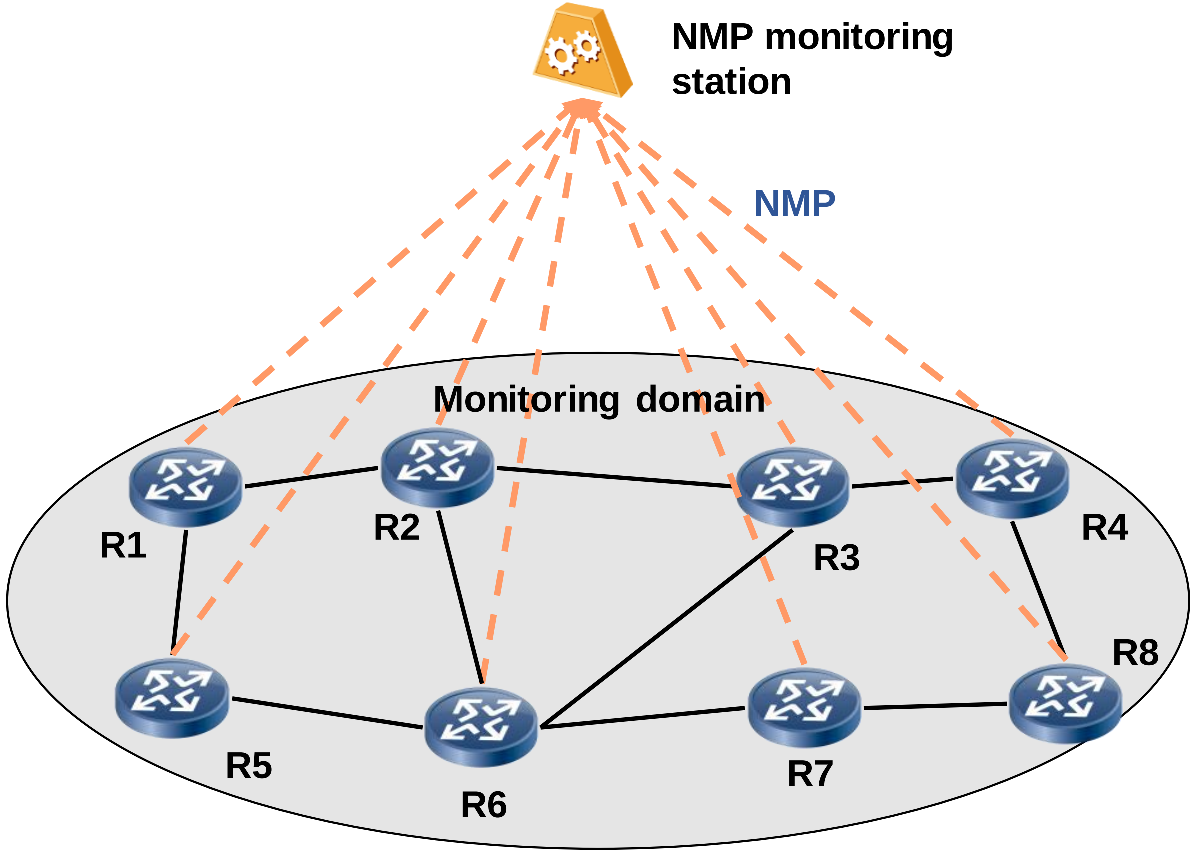
- Network OAM issues:
  - ISIS neighbor down
  - LSP synchronization failure
  - Forwarding plane disconnection
  - Route flapping…
- Existing troubleshooting methods
  - Time-consuming
  - Labor-consuming
  - Data acquisition difficult
  - Typical issues, like route flapping, hard to localize
- Evolving towards autonomous Network OAM

Data Export Options: BMP or NMP?

- Option 1: Proposing new BMP message types
  - New BMP message types for other protocol monitoring
  - Reusing BMP framework, less implementation cost
  - Unified monitoring standard for routing protocols (BGP, ISIS, OSPF)
- Option 2: Proposing a new network monitoring protocol (NMP)
  - Independent framework, more flexible and customized for IGP

NMP for ISIS (IMP)

- NMP session
  - TCP connection between IS (NMP client) and monitoring station (NMP server)
- Message types
  - Type = 0: Initiation
    - Common header + Router Capability TLV
  - Type = 1: Adjacency Status Change Notification
    - Common Header + Per Adjacency Header + Reason TLV
  - Type = 2: Statistic Report
    - Common Header + Per Adjacency Header + Statistic TLV
  - Type = 3: ISIS PDU Monitoring
    - Common Header + Per Adjacency Header + ISIS PDU
  - Type = 4: Termination Message
    - Common Header + Termination Info TLV



NMP for ISIS (IMP)

NMP common header

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+---------------+
|    Version    |
+---------------------------------------------------------------+
|                        Message Length                         |
+---------------------------------------------------------------+
|   Msg. Type   |
+---------------+
```

NMP per adjacency header

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+---------------------------------------------------------------+
|          Reserved           |CT|      Neighbor System ID      |
+---------------------------------------------------------------+
|                      Neighbor System ID                       |
+---------------------------------------------------------------+
|       Neighbor Area ID         |                              |
+---------------------------------------------------------------+
|                     Timestamp (seconds)                       |
+---------------------------------------------------------------+
|                   Timestamp (microseconds)                    |
+---------------------------------------------------------------+
```

Router Capability TLV

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-------------------------------+-------------------------------+
|        Router Cap.Type        |      Router Cap. Length       |
+-------------------------------+-------------------------------+
+                 Router Cap. Value (variable)                  +
~                                                               ~
+---------------------------------------------------------------+
```

Reason TLV

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-------------------------------+-------------------------------+
|   Reserved  |S|  Reason Type  |         Reason Length         |
+-------------------------------+-------------------------------+
+                   Reason Value (variable)                     +
~                                                               ~
+---------------------------------------------------------------+
```

Statistic TLV

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+---------------------------------------------------------------+
|  Reserved   |T| Statistic Type|        Statistic Length       |
+---------------------------------------------------------------+
|                       Statistic  Value                        |
+---------------------------------------------------------------+
```

Termination Info TLV

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-------------------------------+-------------------------------+
|     Termination Info Type     |    Termination Info Length    |
+-------------------------------+-------------------------------+
+              Termination Info Value (variable)                +
~                                                               ~
+---------------------------------------------------------------+
```

Summary of Comments in Mailing List

- Thanks to Acee, Randy Bush, Jeff, Einar, Robert, Wilton, Robert Raszuk, Tim and Greg Skinner for your valuable comments on NMP:
  - Special thanks to Randy Bush for sharing the network OAM develop history for reference.
  - Special thanks to Acee/Jeff/Greg for comments on the motivation of NMP and the comparison with the existing NETCONF/gRPC/YANG works.
  - Special thanks to Tim Evens/Robert Raszuk for raising the BGP-LS-based method for IGP monitoring, especially Tim's detailed design work of BGP-LS for each usecase proposed in our draft.
  - Special thanks to Greg for providing the refinement suggestion on our draft.
- Summary of comments:
  - Why not gRPC/YANG? (Refer to next slide)
  - Why not BGP-LS? (Refer to next slide)
  - History for reference: forget history dooms to repeat it (Definitely we will take the history into account. In fact we are involved in much work of gRPC/Nectconf/YANG and the experience triggered us for complimentary solution combining with the existing work to solve the network OAM issues better.)
  - Draft refinement: should -> SHOULD; Terminology (We will refine the draft accordingly for better quality.)

Why not gRPC/YANG?

- Control plane telemetry (CPT):
  - Definition: monitoring of network protocol running status, e.g., protocol PDUs, protocol statistics and peer stastus
- Why not gRPC/YANG for CPT:
  - CPT and MPT (management plane telemetry) differences
  - CP and MP monitoring decoupling
    - Unified CP information collection using NMP
  - Protocol PDU analysis required for troubleshooting
    - Protocol PDUs are already in binary format, and are transmission-ready
    - Extra work of modeling PDUs as YANG
    - Modeling process slows down data export in cases of massive PDU update
    - Possibility of losing date integrity (retain its original form in case of PDU corruption) during YANG modeling

	Management Plane Telemetry (MPT)	Control Plane Telemetry (CPT)
Data contents	**Device viewpoint: CPU, memory, interface…**	**Protocol viewpoint: Protocol PDU, PDU statistics**
Data interaction	**Status data retrieval and configuration manipulation**	**Unidirectional data retrieval (avoid influencing protocol running)**
Time sensitivity	**Not very time-sensitive**	**Time-sensitive**
Data update frequency	**Not continuously changing with time**	**Continuously changing with time**
Data export	**Netconf, gRPC**	**BMP, NMP**
Data modeling	**YANG Model**	**Header + TLV**
Encoding	**Xml (text-based), protocol buffer (binary)**	**PDU (binary)**

Why not BGP-LS?

- The intention of BGP-LS:
  - Initially proposed for carrying link state information using BGP
  - Currently used for applications like topology visualization
  - Not a “monitoring” protocol
- Network troubleshooting requirements:
  - Requiring more than just link state, e.g., peer down event notification with reasons, Hello PDU, and PDU statistics
  - Requiring information from more than one single device, but per-device feed
  - Technically worktable for BGP-LS to carry non-link-state information, but it deviates from its intention
- Other shortcomings of BGP-LS
  - Dependency on ISIS/OSPF extension
  - Extra non-routing information flooding with ISIS/OSPF (e.g., peer down reason)
  - Extra data flooding leads to extra network bandwidth consumption

Conclusions

- There exists difference between CPT and MPT.
    - CPT is more fit for network troubleshooting, requiring the analysis of protocol PDUs.
    - CPT and MPT margins may overlap.
- The usecases proposed in the draft are to justify the necessity of NMP.
    - They do not exclude the possibility of other methods.
    - According to our NTF work the different telemetry work should be combined for the better solutions.
- Just like the debates between management and control for SDN over the past years, lessons learned:
    - Combine CPT, MPT and even more methods for better solutions.
    - Different solution options for the same issue w.r.t. considerations such as performance, cost, standardization, customer preference, etc.
    - Requirements and running code to justify the necessity finally.

Next Steps

- Close the existing comments.
- Solicit more comments, feedback, and more use cases
- Detailed analysis of different methods for advantages and disadvantages
    - gRPC/YANG, NETCONF/YANG
    - BGP-LS
    - Joint solution with existing methods