Network-wide Protocol Monitoring (NPM): Use Cases

draft-chen-npm-use-cases-00

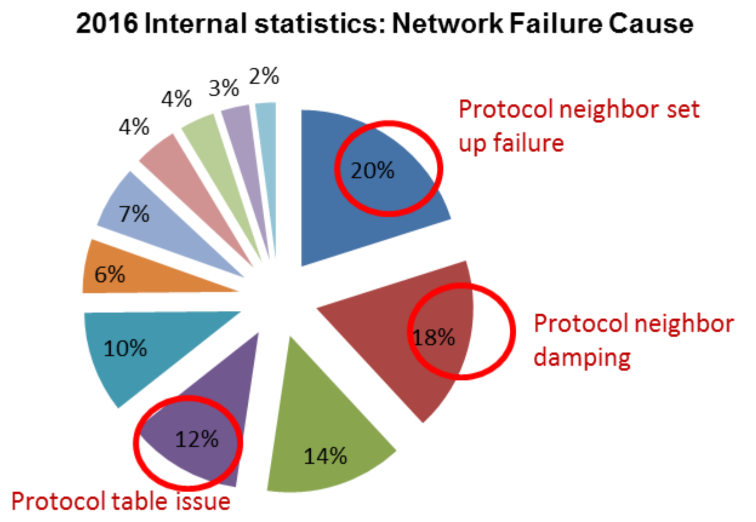
Huainan Chen (China Telecom)
Zhenqiang Li (China Mobile)
Feng Xu (Tencent)
Yunan Gu, Zhenbin Li (Huawei)

Mar. 24, 2019

Control Plane Telemetry

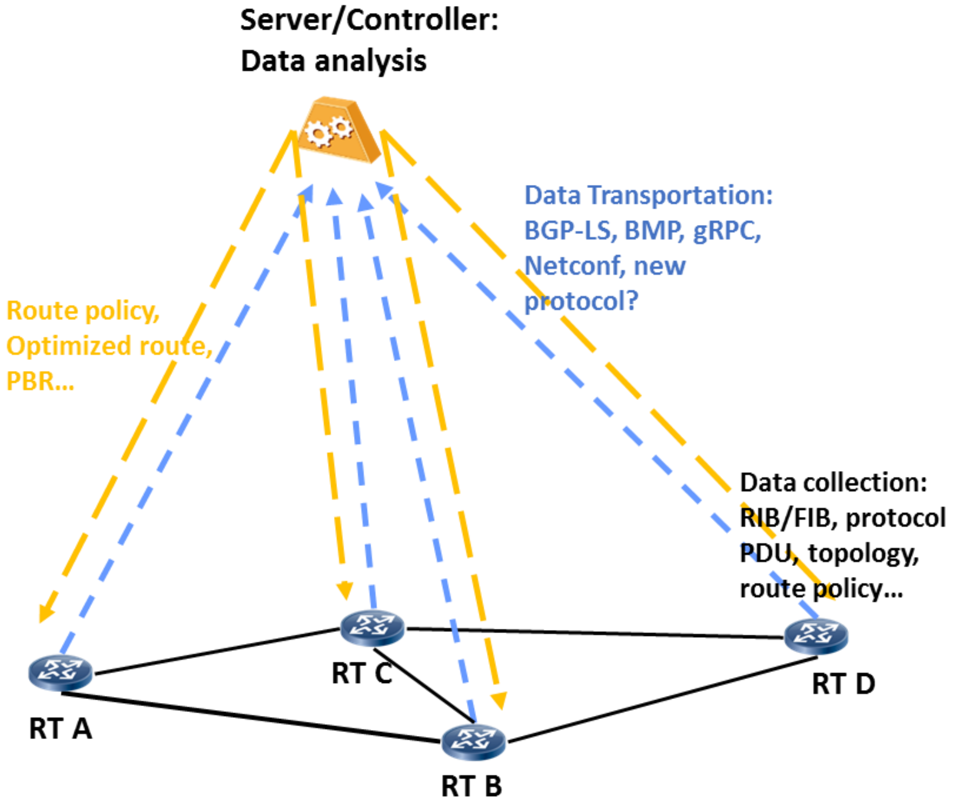
- Management/control/data plane telemetry
  - **Management plane telemetry:** network operational state retrieval and configuration management
  - **Control plane telemetry:** routing protocol monitoring and routing related data retrieval, e.g., topology, route policy, RIB…
  - **Data plane telemetry:** traffic performance measurement and traffic related data retrieval
- Role of control plane telemetry:
  - **Network troubleshooting**
    - 48% of the problems are based on protocol errors or misconfiguration impact both tracking of operational and provisioning
  - **Network planning**
    - No effective route policy/configuration validation approach, and lacks route-traffic correlation insight
    - Real time applications of 5G require real-time TE optimization, and accurate what-if simulation for network planning

Hawei Internal Statistics: control protocol failures take up about 48% of all network issues.



- Traditional troubleshooting methods
  - Time-consuming (hours)
  - Labor-consuming
  - Data acquisition difficult
  - Require OAM experience for operators
- Issues, like route flapping, hard to localize

Network-wide Protocol Monitoring (NPM) Framework



NPM Framework

```
     Data Source:
   Topology,protocol PDU,        NPM problem space:
   RIB,route policy,             suffcient data type coverage,
   statistics...                 sufficient device coverage
   +---------+----------+
             |
             v
+------------+-------------+
|     Data Generation:     |     NPM problem space:
|   data encapsulation,    |     data model definition,
|   data serialization,    |     data process efficiency
|   data subscription      |
+------------+-------------+
             |
             v
+------------+-------------+
|   Data Transportation:   |     NPM problem space:
|                          |     Transportation protocol
|   BMP, gRPC, Netconf,    |     selection,
|   BGP-LS, new protocol?  |     exportation efficiency
+------------+-------------+
             |
             v
+------------+-------------+
|      Data Analysis:      |
| Protocol troubleshooting,|     NPM problem space:
|    Policy validation,    |     data synchronization,
|  Traffic optimization,   |     data parse efficiency
|    What-if simulation    |
+--------------------------+
```

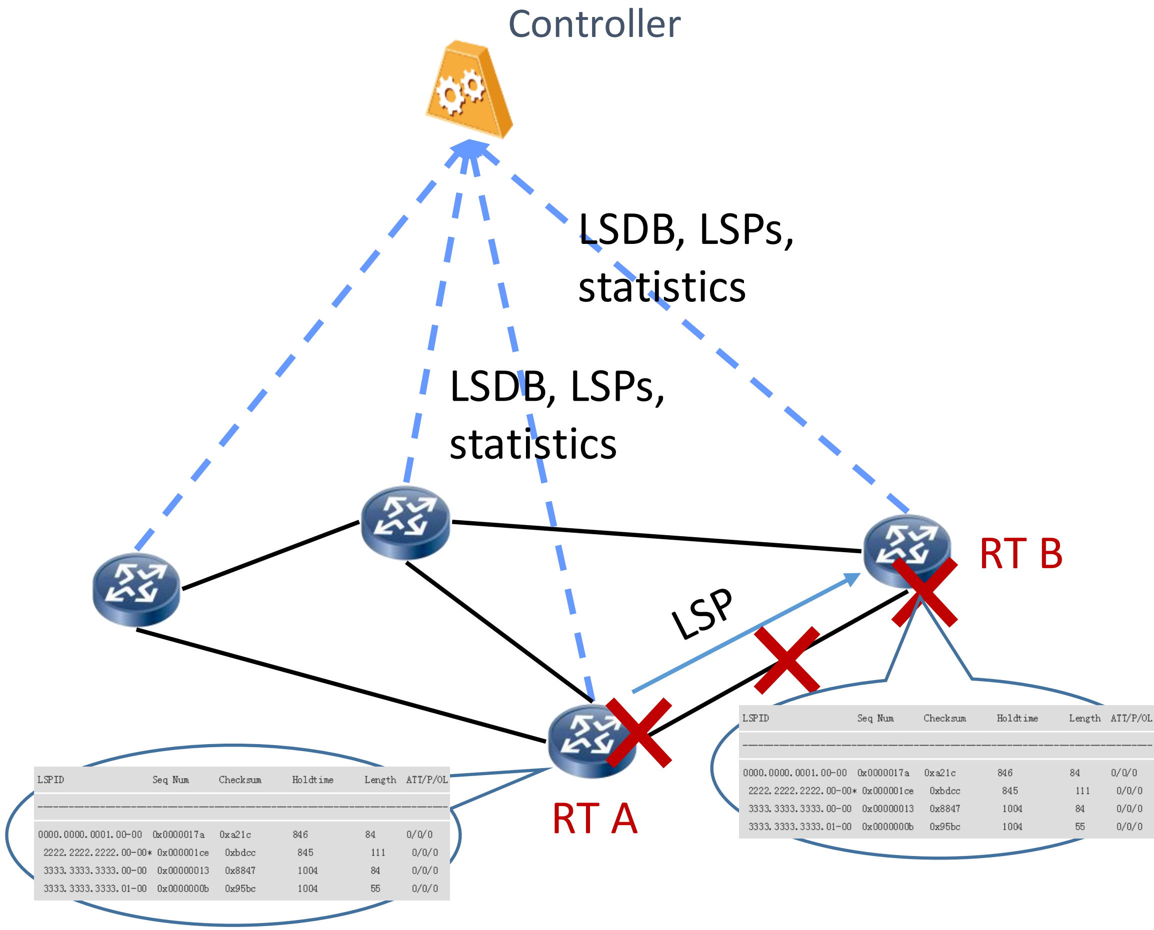
Use case 1: ISIS Route Flapping

- Typical cause 1:
  - System ID conflict
- Typical cause 2:
  - IS-IS neighborship flapping: caused by interface flapping, BFD flapping, CPU high…
- Typical Case 3:
  - Route policy misconfiguration (e.g., multi-protocol import)
- Typical Case 4:
  - Abnormal LSP purges

Causes	Conventional troubleshooting	Improvements with NPM
System ID conflict	• Manual check one by one	• Takes seconds • Alert in advance
IS-IS neighborship flapping	• Log in devices one by one • Manual check: protocol PDUs, configurations, statistics, RIB • Complex CLI checks	• Automatic/semi-automatic troubleshooting • Saves time
Route policy misconfiguration	• Currently lack tracking of how route policy impact route change	• Correlated route attribute and responsible policy record for root cause analysis
Abnormal LSP purges	• POI (RFC 6232) provides the flapping source but no root cause analysis	• Analysis of PDUs for root cause detection

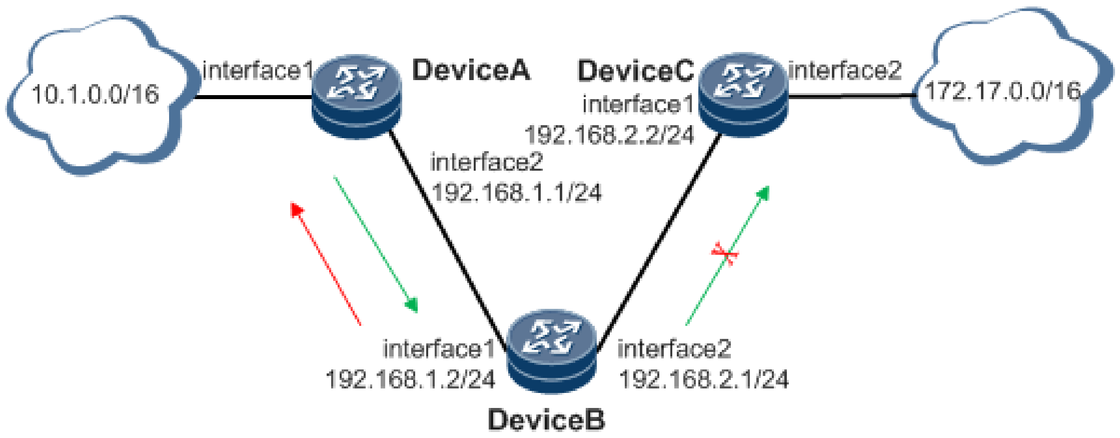
Use case 2: LSDB Synchronization Failure

- Cause 1: LSP not correctly advertised
  - It can be due to incorrect route export policy, or too many prefixes being advertised which exceeds the LSP/MTU threshold, and so on at Router A.
- Cause 2: LSP transmission error
  - IS-IS adjacency failure, .e.g., link down/BFD down/authentication failure.
- Cause 3: LSP correctly received but incorrectly processed
  - The problem that happens at Router B can be faulty route import policy, or Router B being in Overload mode, or the hardware/software bugs.



Use case 3: Route Loop

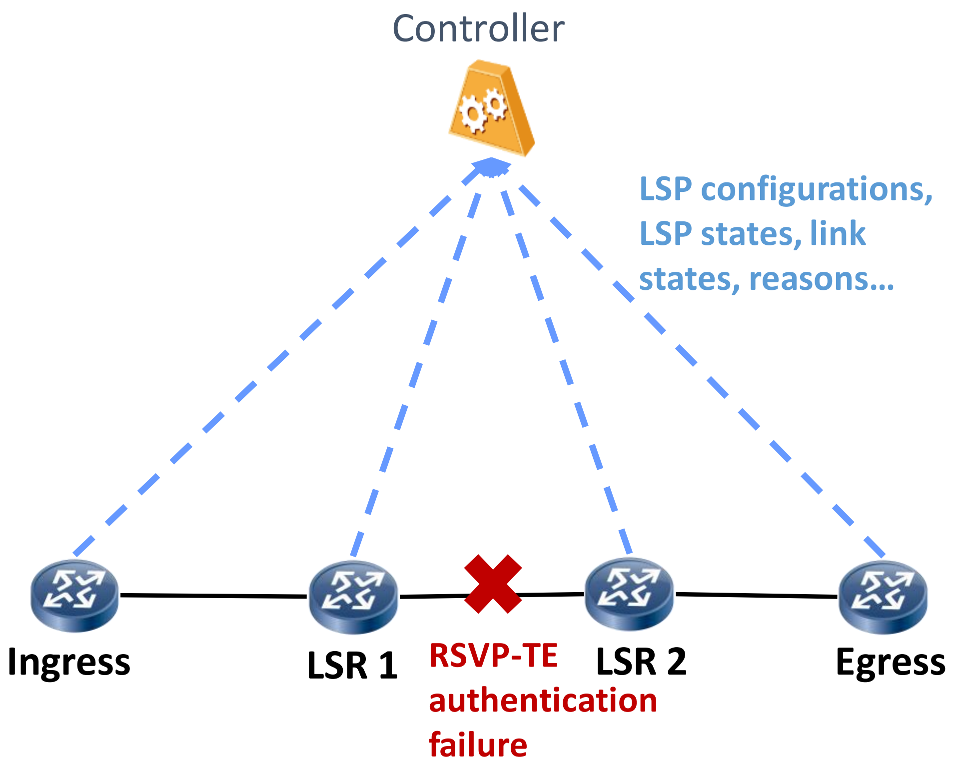
- Conventional loop detection
  - Only post-event detection: TTL anomaly report or packet loss complain
  - Requires network-wide device-by-device check
- Improved with NPM:
  - Real-time and in-advance loop detection
  - Root cause analysis: correlated route change and policy record



Prefix	Route event	Route policy	Time stamp	Next hop	Cost
172.17.0.0 /16	1	ISIS: Route-policy r1 : permit/permit : cost 100	xx:xx:xx	192.168.2.2/24	100
	2	RM: Route-policy r2 : permit/deny : next-hop	xx:xx:xx	192.168.1.1/24	100
	3	RM: Route-policy r3 : permit/deny : cost 200	xx:xx:xx	192.168.1.1/24	200

Use case 4: Tunnel Set Up Failure

- Root causes:
  - Configuration error, path computation error, link failure
- Gaps
  - Data not carried by RSVP-TE messages (PathErr/ResvErr, etc.)
    - IP address conflict
    - LSP establishment time out at head end node
    - RSVP-TE authentication failure
- Possible improvement with NPM:
  - Collection of LSP configurations, LSP states, link states and other reasons from devices along the LSP



Use case 5: Route Policy Validation

- Existing route policy validation:
  - Lacks the vision of how policy impacts the route attributes
- Route policy pre-check simulation:
  - Simulation based on device configurations: not 100% on-going network mirroring
- Possible improvements with NPM
  - Real-time track of how policy changes route attributes
  - Control plane snapshots as the simulation input: topology, protocol neighbor state, RIB… to improve the simulation accuracy

General Requirements from above use cases

1. A "tunnel" for the control plane data export:
   - Performance guarantee for: data modeling, encapsulation, serialization, exportation, transportation performance
2. Adequate protocol data collection:
   - The data type coverage:
     - Protocol PDUs (LSP, LSA, Hello, Open, Update…)
     - Network-wide RIBs
     - Route policies
     - Correlated policy and route attributes…
   - The network coverage:
     - Refers to the devices providing such information (network-wide)