Toward a Network Telemetry Framework

draft-song-ntf-02

Haoyu Song, Tianran Zhou, **Zhenbin Li** (Huawei)
Giuseppe Fioccola (Telecom Italia)
Zhenqiang Li (China Mobile)
Pedro Martinez-Julia (NICT)
Laurent Ciavaglia (Nokia)
Aijun Wang (China Telecom)

What’s new

- New co-authors: Giuseppe Fioccola (Telecom Italia), Zhenqiang Li (China Mobile), Pedro Martinez-Julia (NICT), Laurent Ciavaglia (Nokia) and Aijun Wang (China Telecom)
- Clearer definition and characteristics summary of network telemetry
    - Clear distinction between conventional OAM and telemetry
- New module for the framework: External data and event telemetry
- New content for Control Plane Telemetry: identify the requirements and challenges in details. BMP extensions are identified as NMP (Network monitoring Protocol)
- New content for Data Plane Telemetry:
    - Technique Classification: Active and Passive, In-Band and Out-of-Band, E2E and In-Network, Flow-Path-Node
    - New technology: IPFPM alternately mark for point-to-point and multipoint-to-multipoint

Challenges of Today's Networks

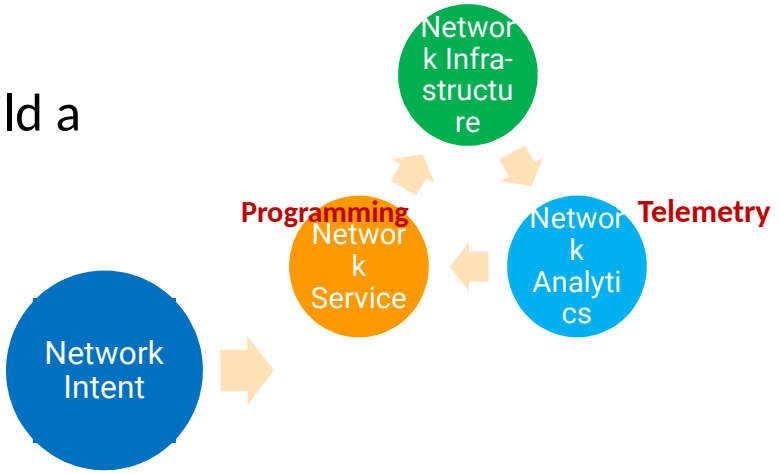
- Networks become more and more complex
  - Cloud, 5G, IoT, overlay, underlay, VPN, slicing, …
- Applications are sensitive to network performance
  - Bandwidth, latency, jitter, packet drop, network churn, …
- Network visibility is important for
  - Network OAM
  - Network Provision
  - Network Planning
  - Network Security
  - Network Troubleshooting
- Yet our old tools for network visibilities are outdated
  - Lack of application level visibility
  - Lack of automation tools

Challenges of the Future Networks

- Network management and service evolve to become intent-driven and automatic
  - Reduce human labor
  - Improve agility and performance
  - Optimize resource efficiency
- Network visibility through telemetry is pivotal to realize intent-driven autonomous networks
  - Telemetry can provide rich, reliable and real-time data, and build a close-loop network service management system.
  - Telemetry should be promoted as a first class

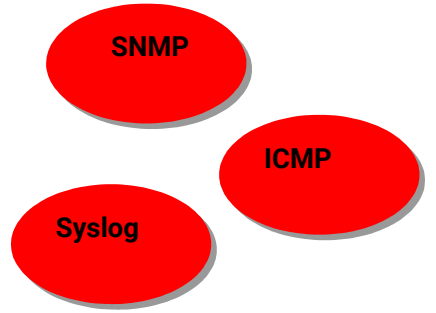
  citizen in network technologies and protocols
  - Telemetry work should be better unified,

  consolidated, and integrated to support the future networks



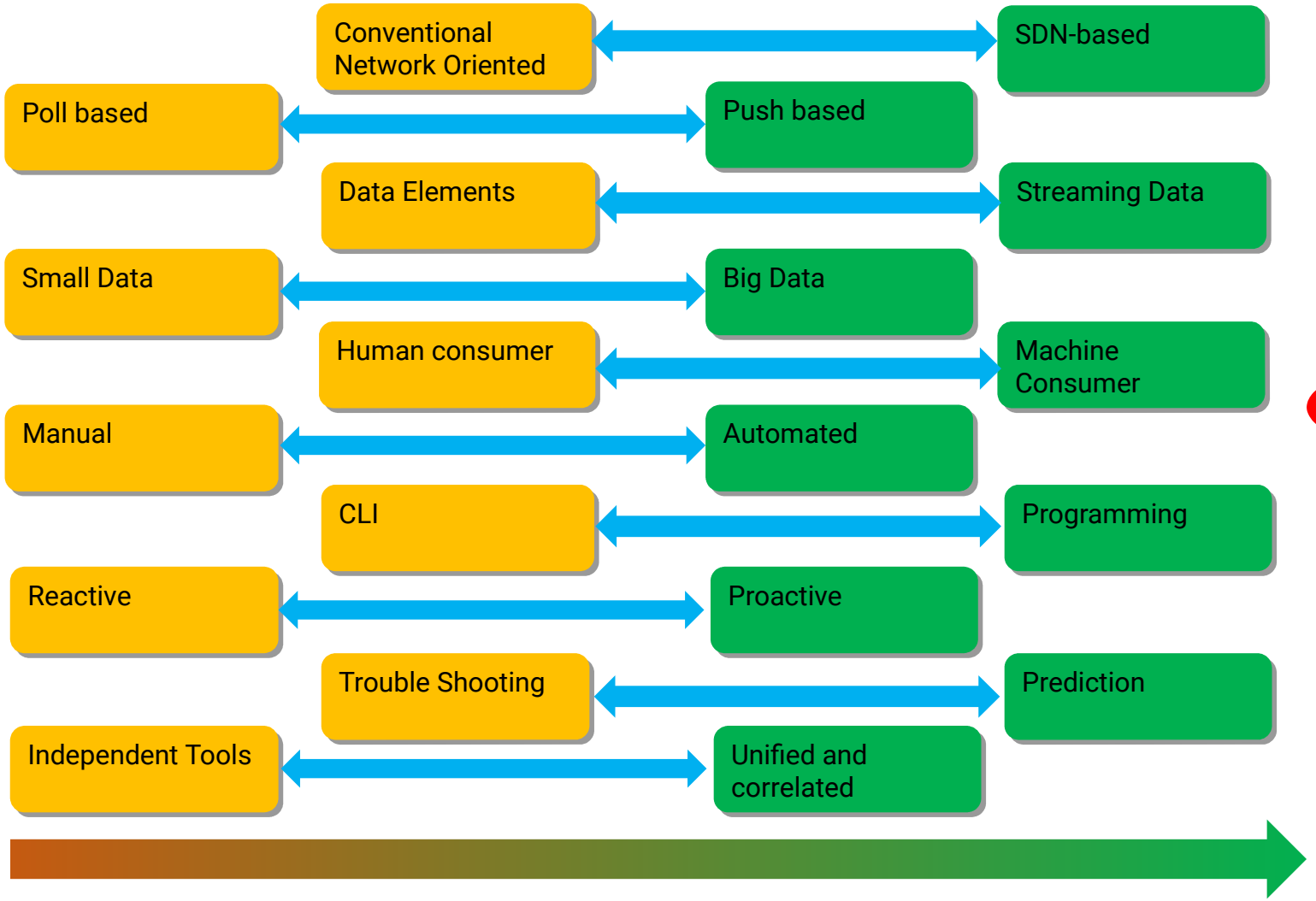
Current Solution: Network OAM

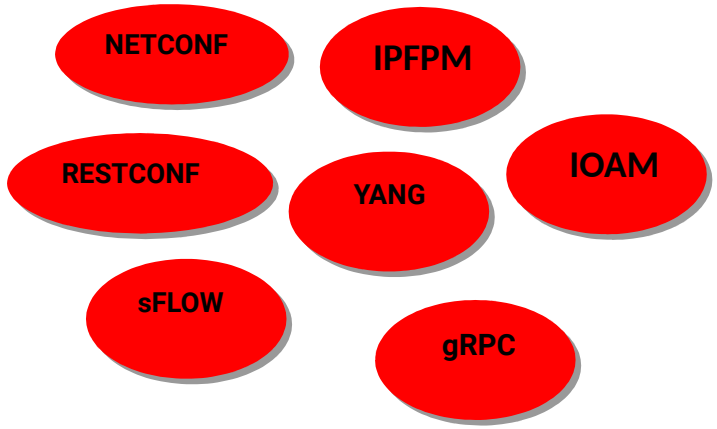
- Conventional OAM is inefficient and insufficient to sustain future autonomous networks
  - SNMP is based on low frequent polling and CLI
  - Lack of coverage, timeliness, and accuracy



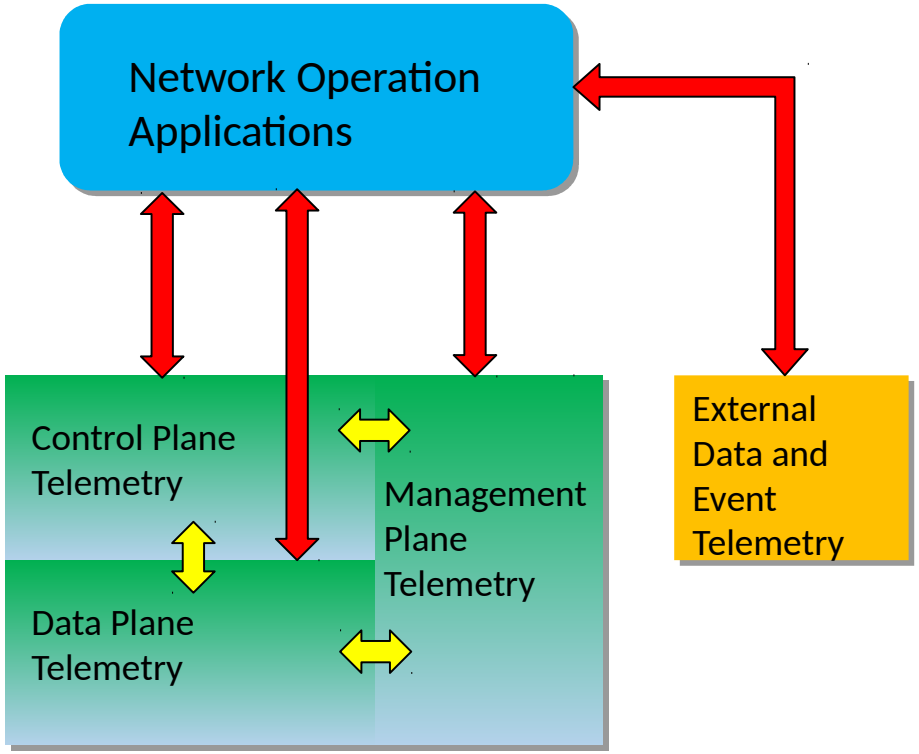
- Existing OAM mechanisms are disaggregated
  - Piecemeal vertical solutions are hard to be composed into a cohesive one
  - Repetitive and redundant work, lack of collaboration and consolidation
  - Designed as afterthought patches and on a case-by-case basis, lack of holistic and systematic view
- A new brood of technologies is expected
  - A framework is needed to normalize the concepts, terms, and technology/standard developments
  - Telemetry to replace OAM as the standard term to achieve network visibility

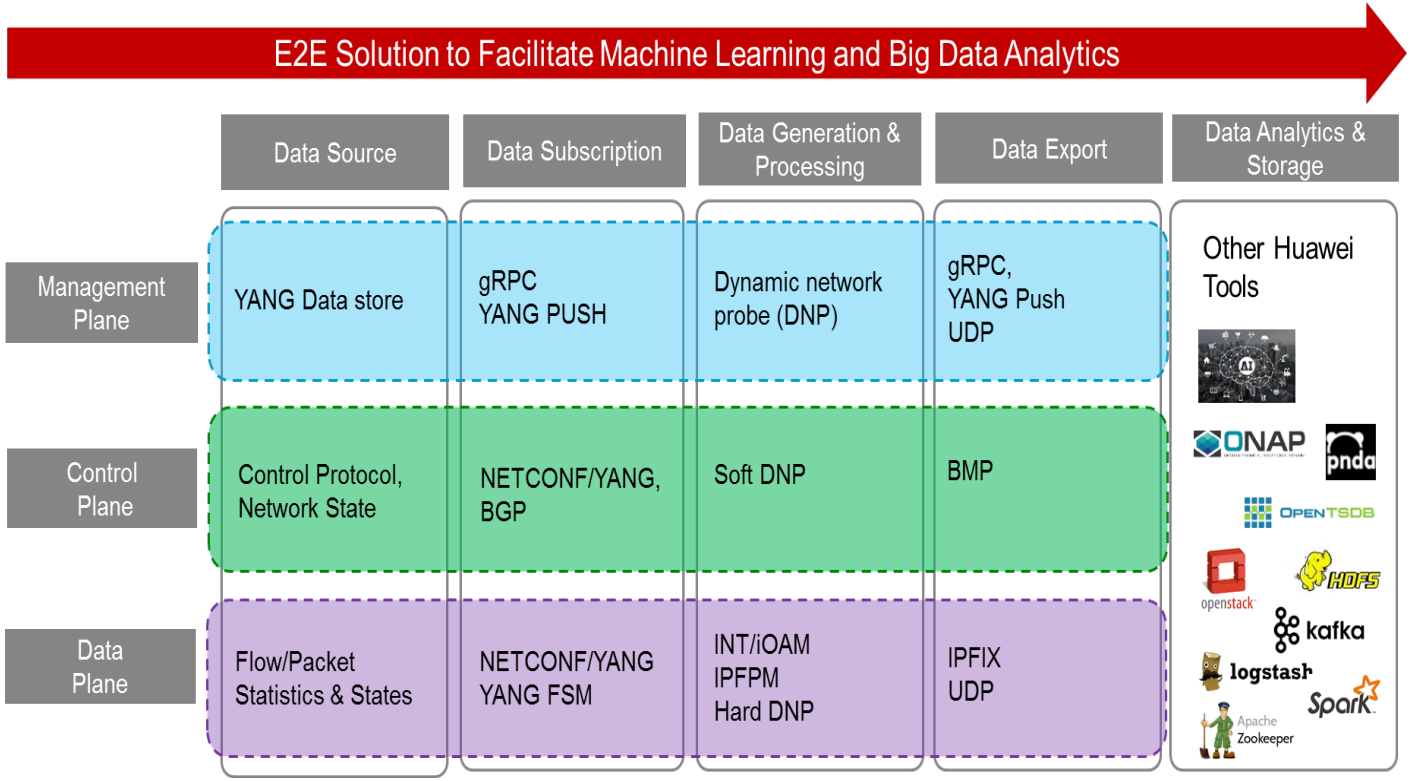
Conventional Network OAM vs. Network Telemetry





Network Telemetry Framework (NTF)





Challenges of Network Telemetry

- Dynamics
  - Continuous, real-time, and interactive
- Multiple sources
  - In device, in network, and out of network
  - Passive, active, and hybrid
- Performance impact
  - Bandwidth and latency
  - Data retention
  - Observer effect

Recap & Conclusion

- Promote the significance of telemetry work in IETF
  - Keep the big picture in mind (Intent-Driven Autonomous Network)
  - Make IETF the leading SDO in this area
- Formalize the telemetry-related terms and technology classification in IETF
  - Network measurement, troubleshooting, and monitoring are all data oriented and serve for the network visibility
  - Consolidate existing work
  - Guide future work

NMP: Network Monitoring Protocol

- Proposed by the draft draft-gu-network-monitoring-protocol-00.
- 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.
- Welcome to GROW and OPSAWG for more discussion.

Next Steps

- Solicit more comments and feedbacks.
- Refine the draft
- More cooperation