Strawman proposal on Network Telemetry and Analysis

draft-wu-network-telemetry-00

Qin Wu(bill.wu@huawei.com)

John Strassner(john.sc.strassner@huawei.com)

Objective and Motivation

- Objective:
  - Propose a network measurement and analysis architecture
    - Collect data from various data sources using different transport protocol and data format.
    - Provide consistent data representation and interpretation.
    - Provide better network visibility

- Motivation:
  - Billions of devices connecting to the internet and VPN imposes a great impact on the network
    - Prove network innocence become important
  - Network management protocol is not sufficient for data collection
  - Machine readable vs human readable format for big data collection
  - Extraction value from big data collection from network environment and IoT application.
    - Define a Network KQI to measure network performance and health and prove network innocence
    - Using Network KQI/KPI to predict network incidents and diagnose the network

What is the network Telemetry

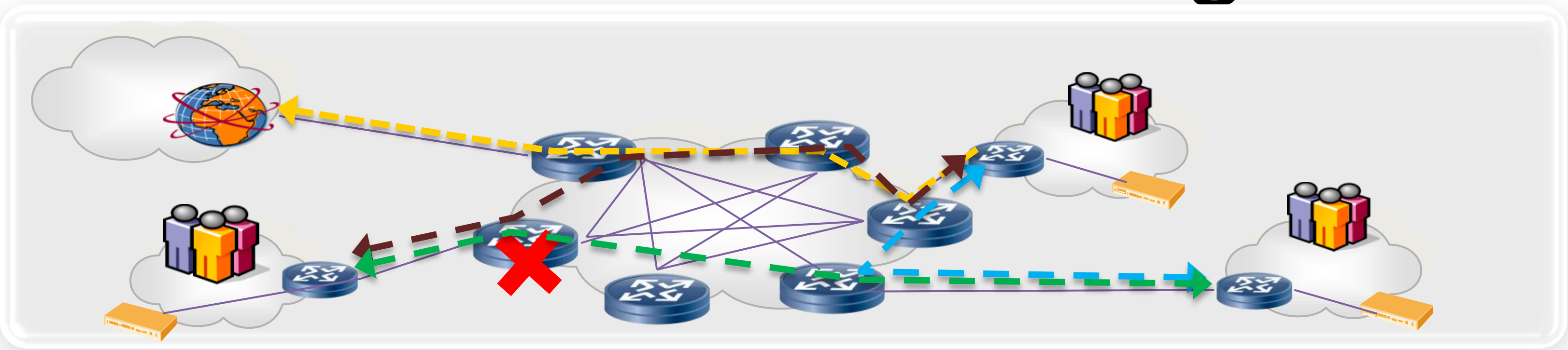
- Network Telemetry is to define methodology for data distribution and processing
  - What kind of data is collected? Configuration data, operational data, Log data, etc.
  - Where the data is generated? Where the data is stored?
  - Who distribute the data?
  - What communication protocol is used for data distribution? gRPC, HTTP2.0
  - What data format is used to encode data? XML, protobuf?
  - How data is pre-processed? Serialization, aggregation, normalization,filtering

Why Network Telemetry and Analysis

- Event correlation,
- Anomaly detection,
- Performance monitoring,
- Service Assurance
- Metric calculation,
- Trend analysis,
- and other related processes.

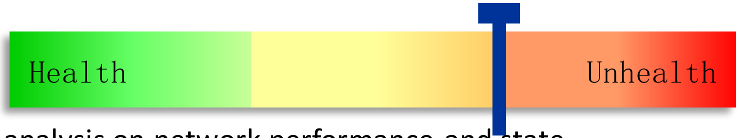
Fault localization and Diagnosis

Network running state



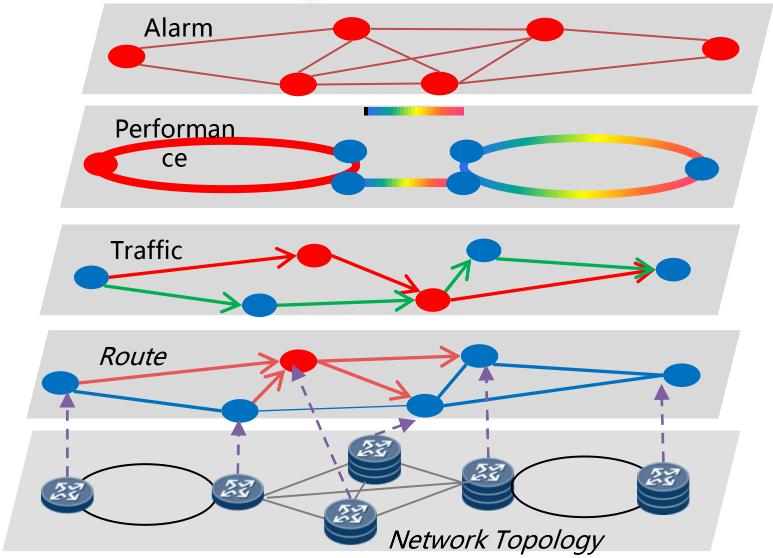
1 Assess network performance and running state, rate network quality in terms of score

Network Health Index： **20**



2 data Correlation analysis on network performance and state，quickly locate fault and identify root cause in case of network incident.

Network Fault Diagnosis



Quickly locate network fault with alarm and event information

Locate anomaly device in the topology based on Path KPI value change using KPI statistics learning algorithm

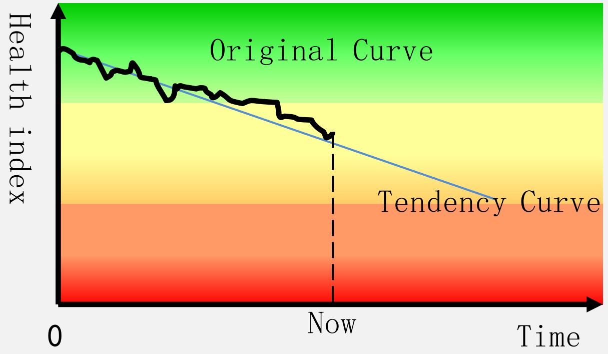
Locate anomaly traffic and device based on statistics learning traffic model

Locate Anomaly device based on route behavior and interaction assessment model

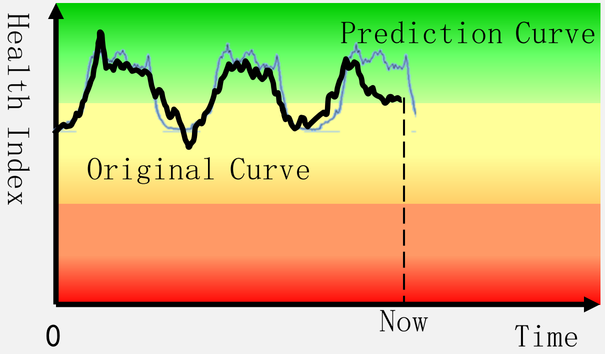
Topology model with layering and service classification and provide basic infrastructure for network fault diagnosis

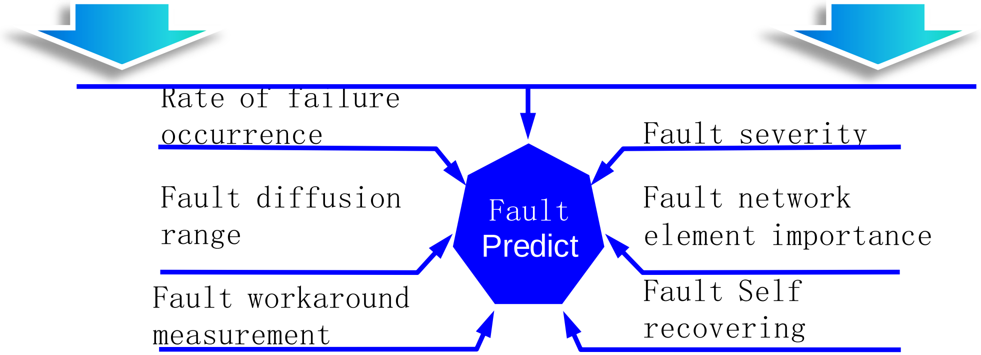
Network Fault Predictability

Case A: performance monitoring, Check if measured results exceed threshold value set based on network health index histogram and whether network running state get worse



Case B: anomaly detection Compare the measured data curve with network health index reference curve, measure network anomaly using algorithm that directly calculate offset between two curves





Rate of failure occurrence

Fault diffusion range

Fault workaround measurement

Fault Predict

Fault severity

Fault network element importance

Fault Self recovering

Objective: quickly identify faults and anticipant incidents, take measure to bypass recognized problem and recover from network failure, prevent service interruption, Network damage/ deterioration

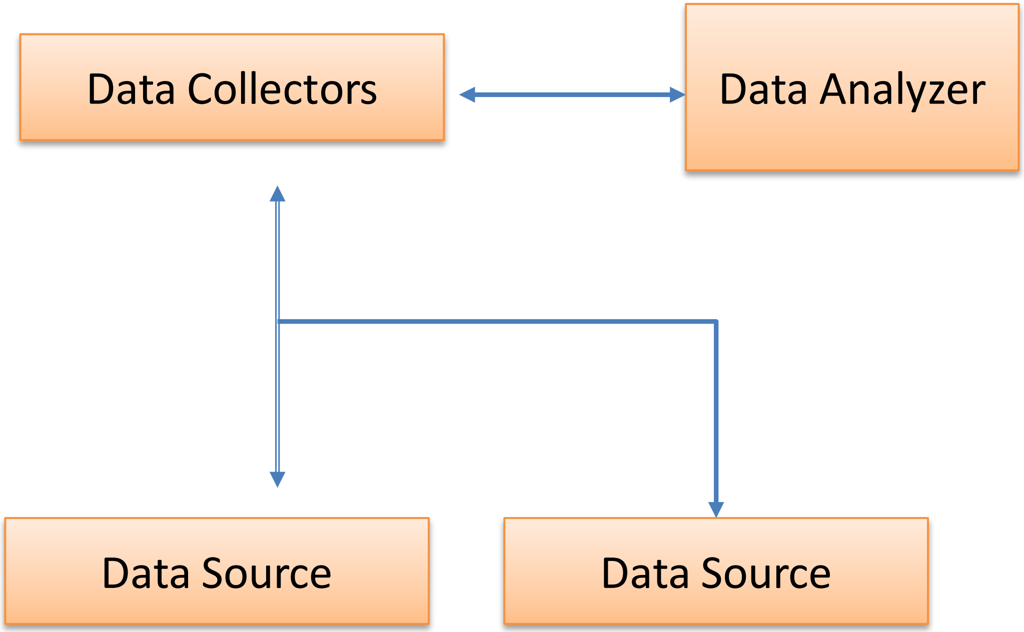
Data Source Classification

Data Source Category	**Information**
Network Data	Usage Records Performance Monitoring Data Fault Monitoring Data Real Time Traffic Data Real Time Statistics Data Network Configuration Data Provision Data
Application Data derived from interfaces, channels, software, etc.	Traffic Analysis Web, Search, SMS, Email, Social Media Data, Mobile Apps
Subscriber Data	Profile Data Network Registry Operation Data Billing Data

Measured data Characteristics

Characteristics	Description
Structured data or unstructured data	Structure data
Variety of the data	Measurement data can be any of network performance data, network logging data, network warning and defects data, network statistics and state data, and network resource operation data (e.g., operations on RIBs and FIBs[RFC4984]).
High proportion data	1. Most measurement data are monitor state data rather than configuration data. 2. However, on occasion, network configuration data may also be included (e.g., to establish context for the measurement data). 3. the required frequency of access to monitoring state data is extremely high.
Velocity of the data	data requires real time delivery with high throughput, multi-channel data collection mechanisms.

Basic Network Telemetry and Analysis Architecture



Core Functional Components

Data Source: can be any type of network device or IoT device that generates data.

Examples include

a. the management system that accesses IGP/BGP routing information,
b. network inventory,
c. topology,
d. and resource data,
e. other types of information that provides data to be measured
a. and/or contextual information to better understand the network telemetry data.

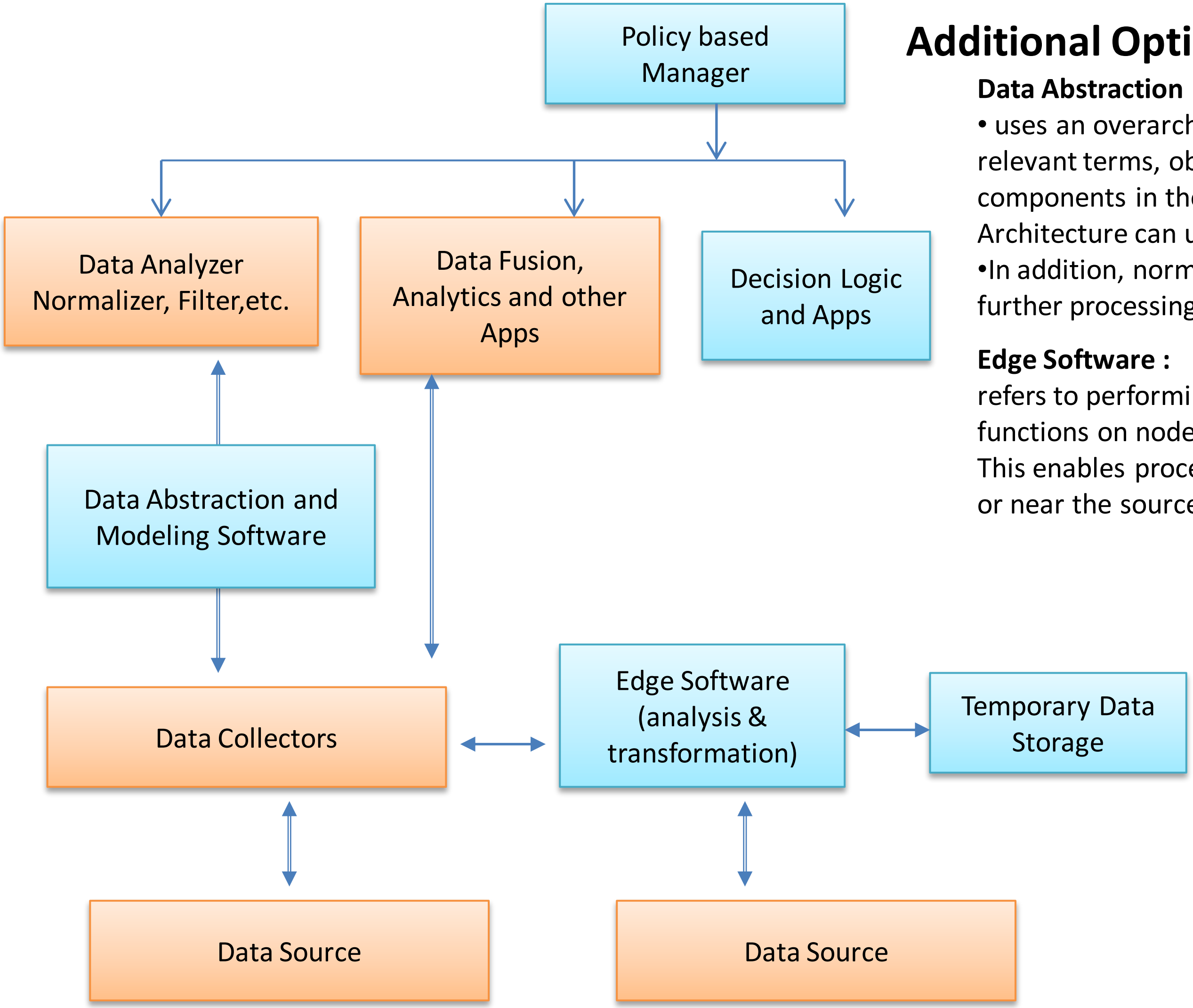
Data Collector: may be a part of a control and/ or management system (e.g., NMS/OSS, SDN Controller, or OAM system) and/or a dedicated set of entities.

- It gathers data from various Data Sources,
- and performs processing tasks to feed raw and/or processed data to the Data Analyzer.

Data Analyzer: processes data from various data collectors to provide actionable insight.

This ranges from generating simple statistical metrics to inferring problems to recommending solutions to said problems.

Advance Network Telemetry and Analysis Architecture



Policy based Manager
Data Analyzer Normalizer, Filter,etc.
Data Fusion, Analytics and other Apps
Decision Logic and Apps
Data Abstraction and Modeling Software
Data Collectors
Edge Software (analysis & transformation)
Temporary Data Storage
Data Source
Data Source

Additional Optional Functional Components

Data Abstraction and Modeling Software:

• uses an overarching information model to define relevant terms, objects, and values that all components in the Network Telemetry Architecture can use.

•In addition, normalize data and filter data for further processing and analytics.

Edge Software :

refers to performing compute, storage, and/or networking functions on nodes at the edges of a network. This enables processing of data to occur at or near the source of the data.

Policy-based Manager:

• use of a set of policies that govern the behavior of the system.

•managing different aspects of the Network Telemetry Architecture in a distributed and extensible manner

•Examples include defining rules that determine what data to collect when, where, and how,

•as well as defining rules that, given a specific context, determine how to process collected data.

Issues with Network Telemetry and Analytics

- Data Fetching Efficiency
- Inefficiency of existing transport metrics
- Measurement data format consistency issue
- Data Correlation issues
- Data Synchronization Issue

Data Fetching Efficiency

- The existing Network management protocol is not dedicated and also not sufficient for data collection.
  - NETCONF more network configuration, only retrieve operational data
  - SYSLOG can only retrieve Log and Event data

- SNMP relies on Periodic fetching. Periodic fetching of data is not an adequate solution for many types of applications
    - E.g., Applications that require frequent update to the stored data
    - adds significant load on participating networks, devices, and applications

- We increasingly rely on RPC-style interactions [RFC5531] to fetch data on demand by application. However most of applications are interested in update of the data or change to the data.

- Human readable language and format prevail, however it it lacks efficiency on the wire

Inefficiency of existing network performance metrics

- These transport-specific metrics are defined for specific technologies. For example, network performance parameters in Y.1540 are only designed for IP networks, and do not apply to connection- oriented networks, such as an MPLS-TP network.

- Not all the metrics are end-to-end performance metrics at the network level. For example, the TE performance metric defined in ISIS-TE [RFC5305] is only defined for per link usage.

- These transport specific metrics are all single objective metrics; there are no transport specific metrics defined as multi-objective metrics. For example, IP transfer Delay (IPTD) is a single-objective metric and cannot be used to measure similar and important performance behaviors such as IP packet Delay Variation[Y1541]).

- Different services have different performance requirements. It is hard to measure network quality to satisfy all possible services requirement using a single metric.

- Transport-specific metrics are not applied to the whole network, but to a specific flow passing through the network corresponding to matched QoS classes.

- If there are multiple paths from source to destination in the IP network, then transport-specific metrics change with the path selected and it may be also hard to know which path the packet will traverse.

Measurement data format consistency issue

- different commands, having different syntax and semantics characteristics that use different protocols, may have to be issued to retrieve the same type of data from different devices.
- The data format is typically vendor- and device-specific
- The Data Analyzer may need to ingest data in a specific format that is not supported by the Data Collectors that service it

Data Correlation issues

- Useful trend analysis and anomaly detection depend on proper correlation of the data collected from the different Data Sources.
  - Correlated fault data with network topology information at different layer or different network segment can help network diagnosis

- Data can only be meaningful if they are correlated in time and space.
  - Predict trend more up to correlation data with time information.
  - Correlate different type data from different data source with time or space can provide better network visibility
  - But such correlation is still a challenging issue.

Data Synchronization Issue

- When retrieving data from Data Sources or Data Collectors, synchronization the same type of data between data source and data collector or between data collector and data analyzer is a complicated thing.
  - Arrange src and dst synchronized, especially when multiple source feed one data collector, or multiple data collector feed one data analyzer
  - Aggregate data from different data source and synchronize the data to the data analyzer is also not easy task.

Next step

- Any Comments and Feedback on this draft?
- Anyone interested in this topic or issues raised?
- Any piece fits into the scope of T2TRG?