Network Artificial Intelligence (NAI)

draft-zheng-opsawg-network-ai-usecases

draft-li-rtgwg-network-ai-arch

Yi Zheng, China Unicom
Zhenbin Li, Jinhui Zhang, Xu Shiping, Dhruv Dhody, Huawei

Introduction

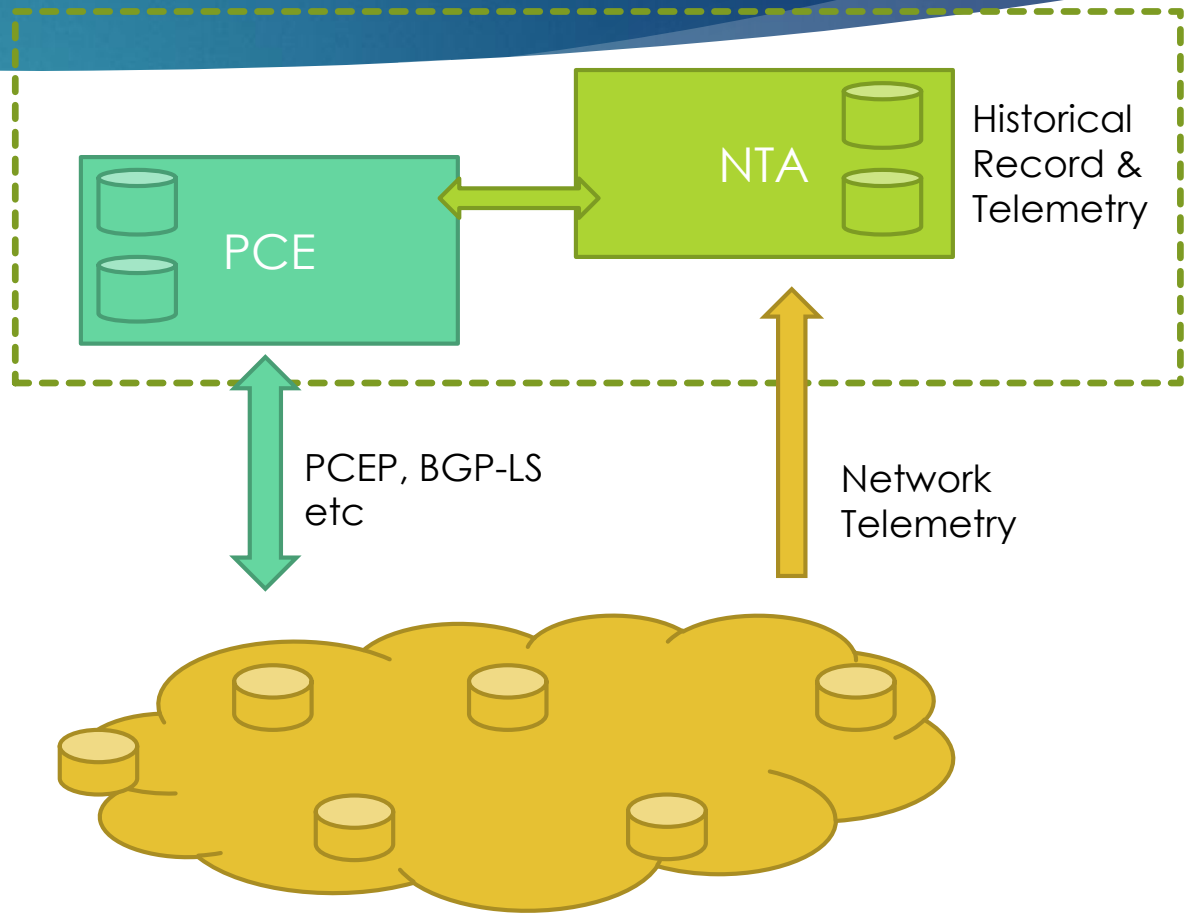
- Explore how Artificial Intelligence (AI) and Machine Learning (ML) can be applied to the network use-cases.
- As networks get more and more dynamic & complex, there are new challenges to network management and optimization
  - Can NAI help?
- What role does a central controller / SDN can play?
  - Use Intelligence to drive the controller and implement the recommendations and decisions made by the AI.
- This use-case document discusses how the Network Artificial Intelligence (NAI) is able to applied in various possible use-cases.

Key Functions

- Build a Network Telemetry Analytics (NTA) engine, usually collocated with a central controller.
- E2E deployment may involve multiple NTA engines coordinating with each other similar to the controllers.

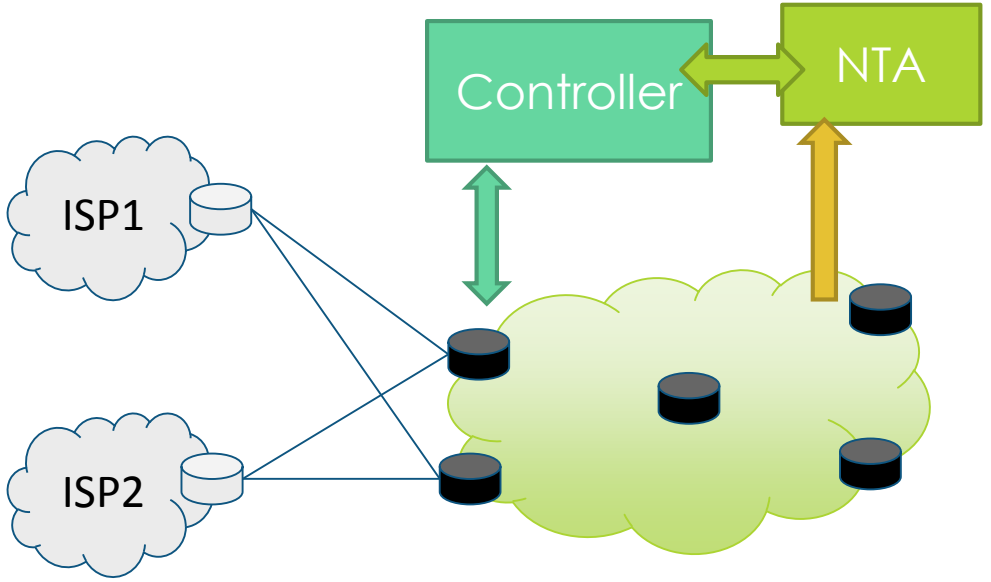
Enhance Path Computation and Traffic Engineering

- PCE has access to TEDB + LSP-DB
- Adding history records of the changes in LSP-DB and TEDB for analytics
- Adding Network Telemetry as well as real-time analytics of traffic monitoring, statistics etc.
  - PCE reroute/re-optimize using the historical trend and predications from NAI
  - PCE could handle the changes in bandwidth utilization and other performance monitoring data for predicted traffic congestion avoidance.
- Build intelligent context
  - What is the LSP/Path used for?



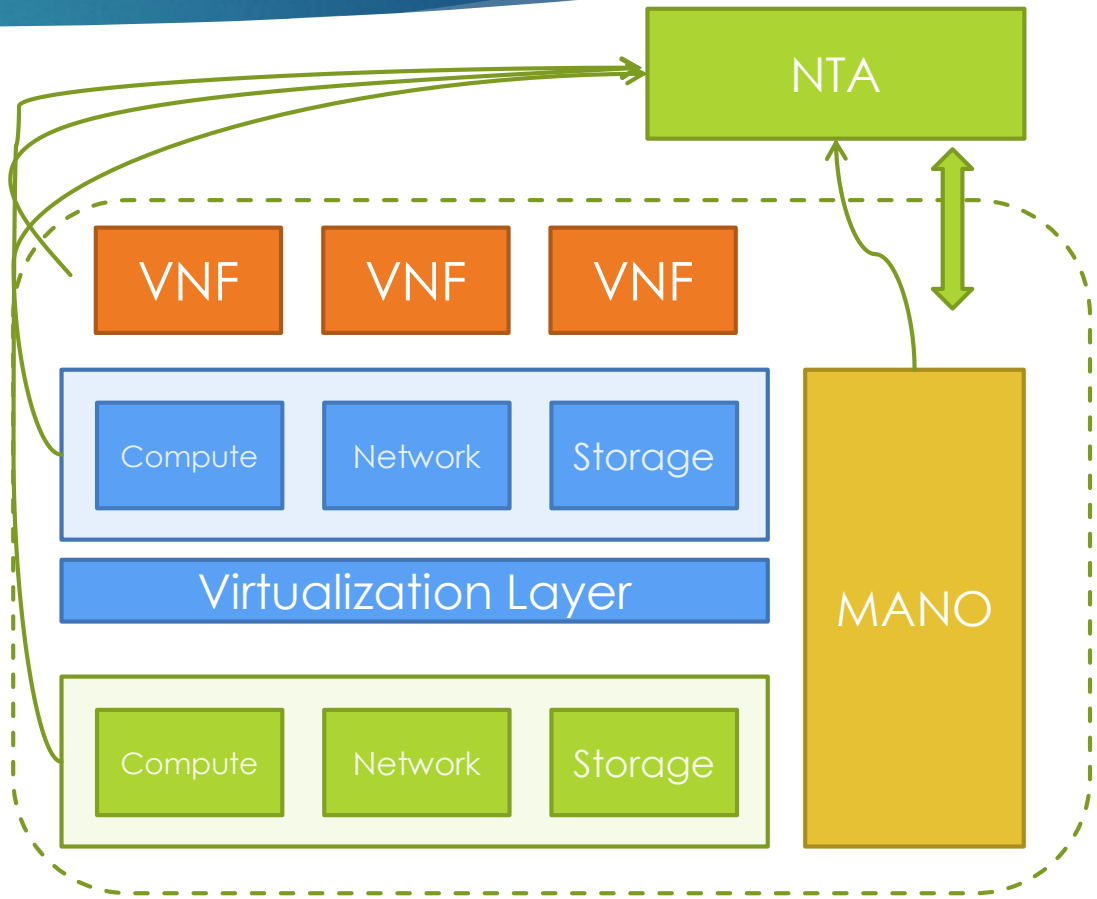
Route Monitoring and Analytics

- BMP can be used to monitor the BGP peer.
- The controller can monitor the BGP status and routing information of the routers using BMP.
- Historical records of changes can be maintained in the NTA for analytics
- Telemetry information can be added.
- Possible use-cases
  - BGP Route Leaks
  - BGP Hijacks -
  - Traffic Analytics and intelligent Traffic Engineering
- Intelligent detection via anomaly detection!



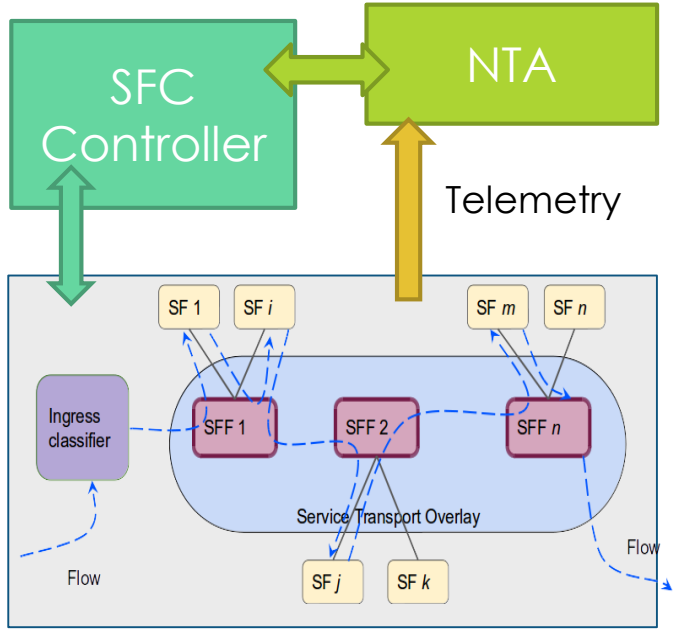
Multilayer Fault Detection in NFV

- Telemetry data from all layers
  - CPU performance, memory usage, interface bandwidth and other KPI indicators can be monitored.
  - At the same time resource occupancy and the life cycle of NVF software process can also be monitored.
- Historical records – correlate and categorize.
- Through the NAI, the relevant statistical data in multiple levels can be analyzed and the models can be setup to locate the root cause for the possible fault in the multi-layer environment.
- Intelligent Health Diagnostic



Smart SFC

- Network Telemetry - delay, jitter, packet loss from the network
- Service telemetry - CPU/memory usage utilizations from the SFs
- Via sFLOW/gRPC protocol and stored as historical records
- The analytics component in NTA can build models to predict the impact on various Service Function Paths due to network events, traffic and state of the SFPs and instruct the SFC controller to take necessary actions
- The SFC controller can calculate new paths/reroute the SFC path to avoid congested Ports/SFFs or overloaded SFs



Architectural Considerations

- Placement of NTA
  - Collocated with Controller
  - Integrated with controller
- Handling of multi-domain controllers
  - Analytics closer to the source is better!
  - Hierarchy (like ACTN…)
- Building Blocks
  - Telemetry Collector (Data Collector)
  - Data Movement
  - Analytics – real time or batch
  - ML Models
  - Visualization
  - Closed Loop Interactions

Next Steps

- Are these the right set of use-case to explore AI/ML in the networks?
  - Do you have other use-cases?
  - Is it useful to document them and discuss?
  - Please suggest and collaborate!
- What are the architectural considerations, that should be considered?
  - Are there any protocol considerations?
- Build prototypes, reuse various possible open-source.
  - Hopefully in a future Hackathon!

Thank You!