Challenges of Evolution towards Autonomous Network

Chang Yue
Chief Architect of Network Product Line

HUAWEI

The motivation of autonomous network

58% Experience issues driven by complaints

Pulled by customer requests

75B Connected devices by 2025

Network complexities beyond human capabilities

System architecture innovation to solve structural problems

OPEX ⇧ > Revenue ⇧

Last decade

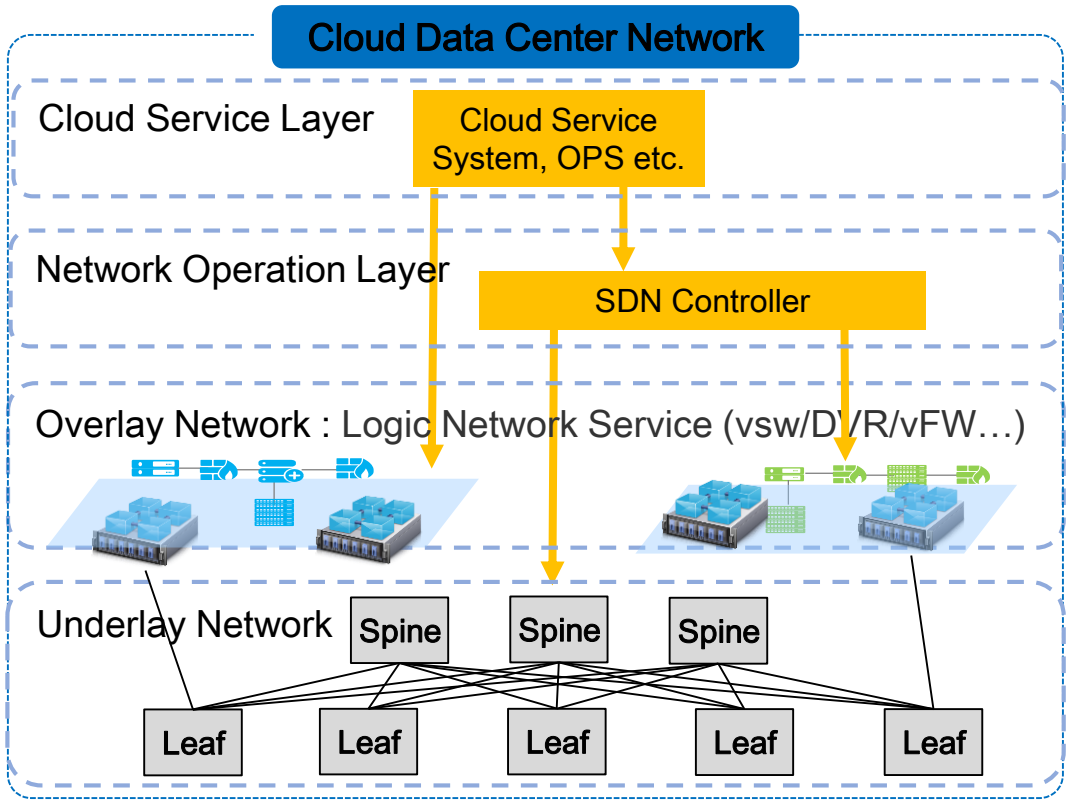
Pushed by structural problems

3 *OTT players* **vs** **300+** *Telcos*

Efficiency to maintain 10,000 devices

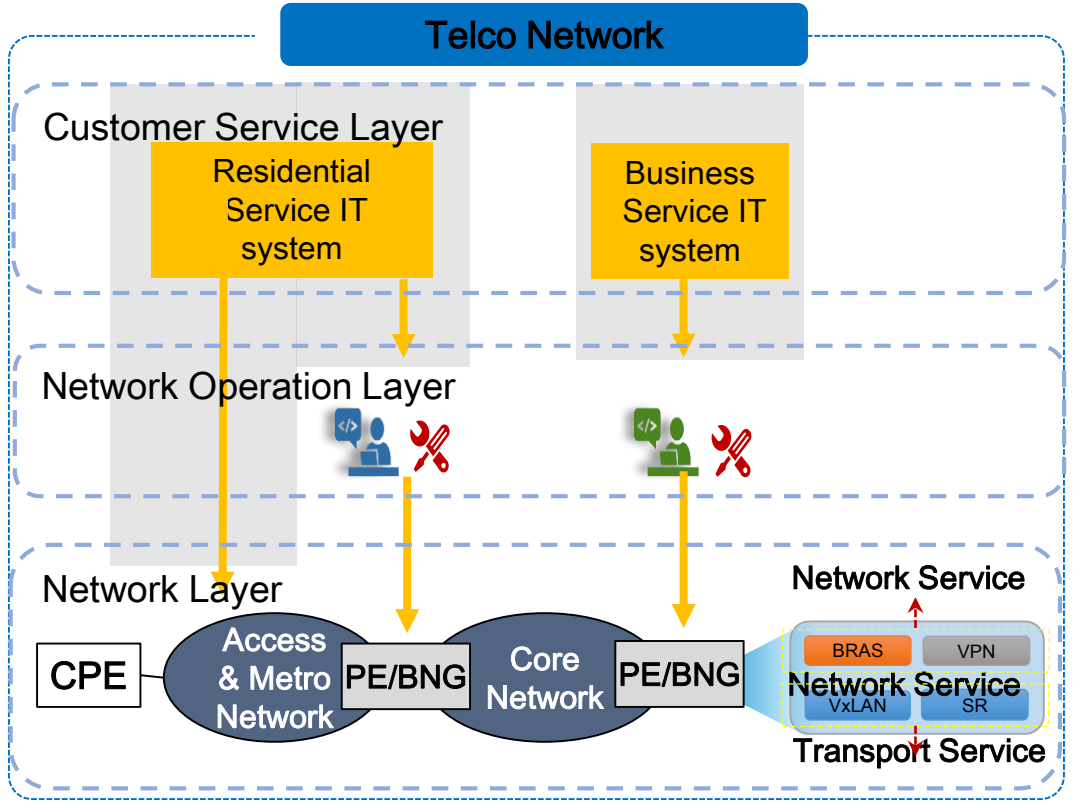
Key gaps and differences between OTT and CT

~ 3000 devices / person in Hyper-scale DC
~ 4 hours OTT New Service Provisioning
CAPEX 10%↑ Traffic Double Growth



VS

~ 100 Devices / person in Telco-S network
~ 28 weeks Private Line Service Provisioning
CAPEX 60%↑ Traffic Double Growth



Decoupling of network transport & service in hardware and software individually

Spine/Leaf Arch, elastic scale out, any to any non-blocking

Simplified protocols, reduce O&M experience requirements

Clear boundary of Network operation and Service system, Automatic service

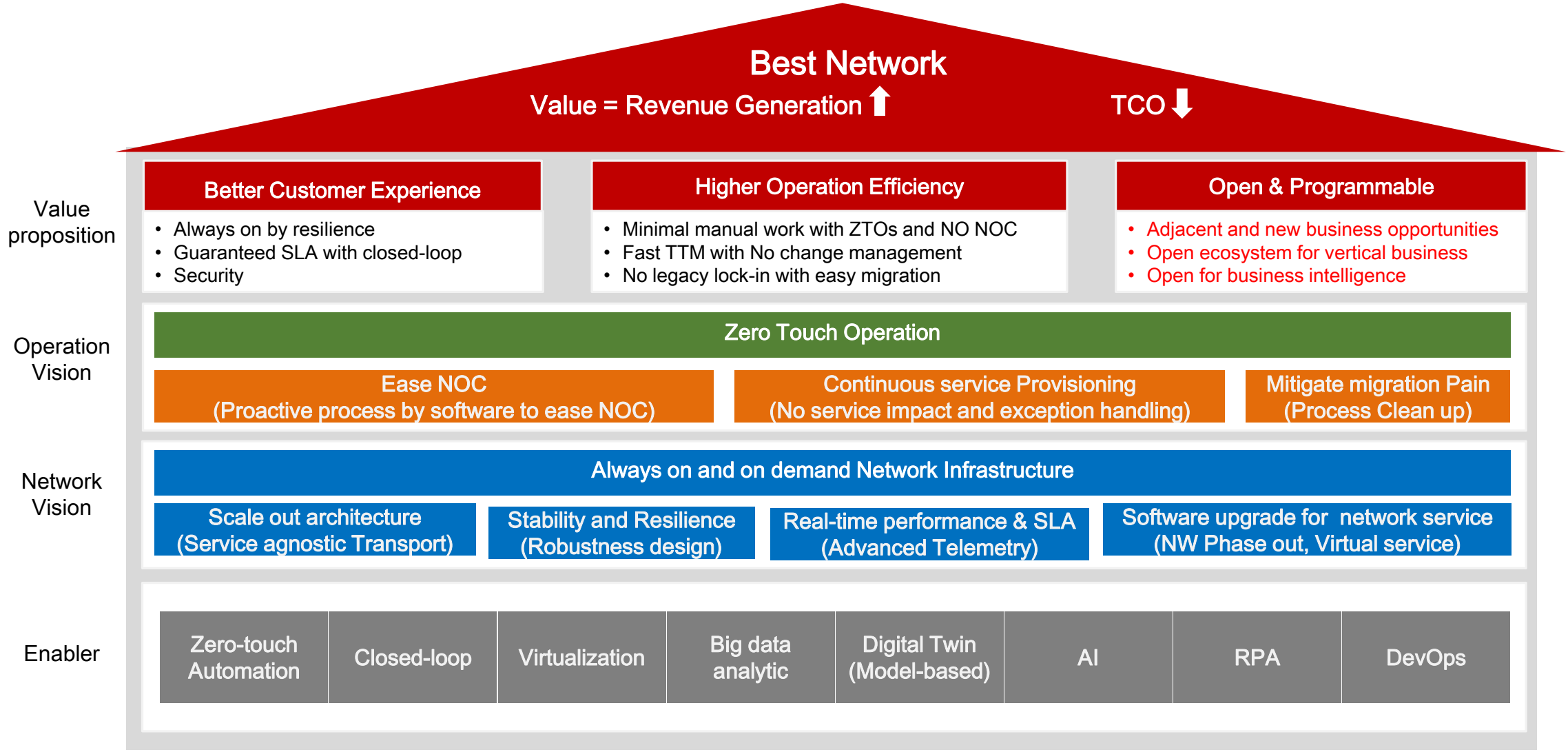
Coupling network transport & service into dedicated HW, difficult to scale up independently

Aggregation network with bandwidth convergence

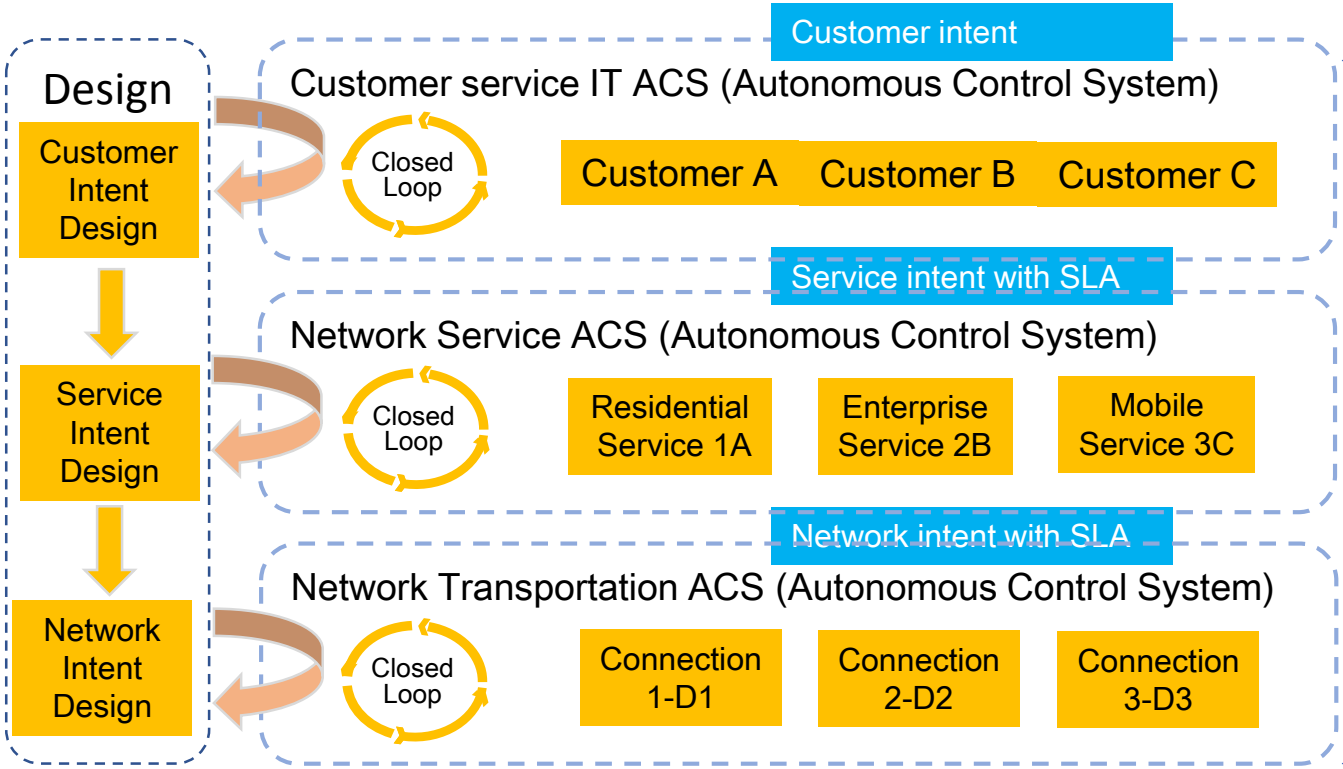
30+ protocols, high experience requirement

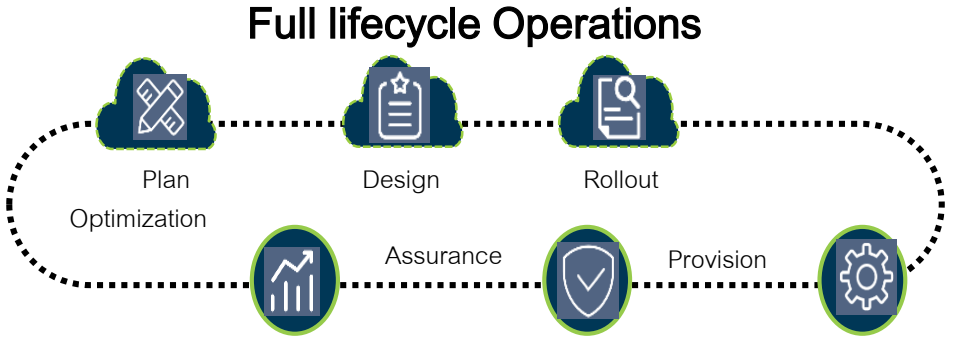
Unclear boundary of network operation and service IT system, Low efficiency by

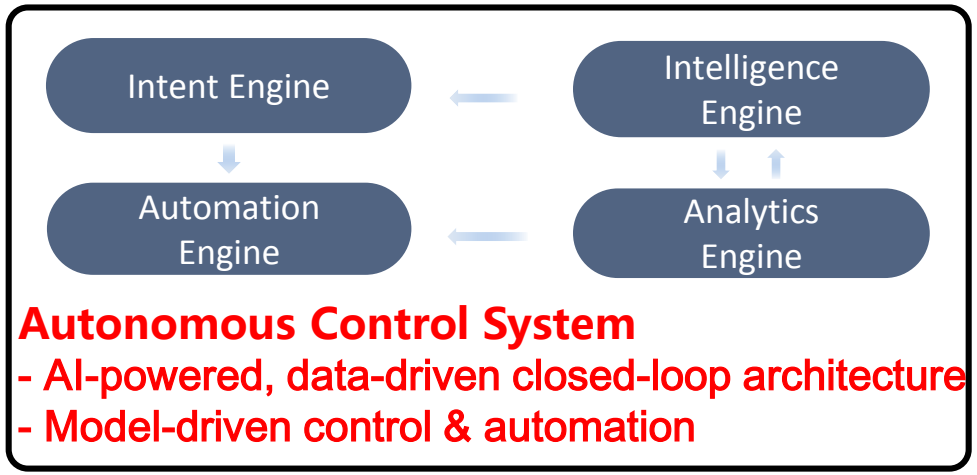
Vision and goal of the autonomous network

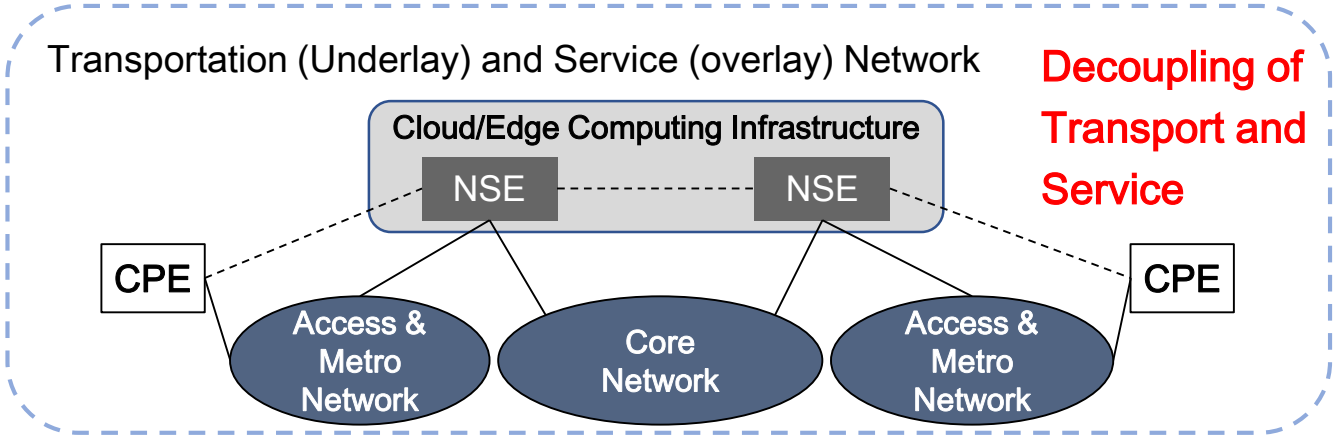


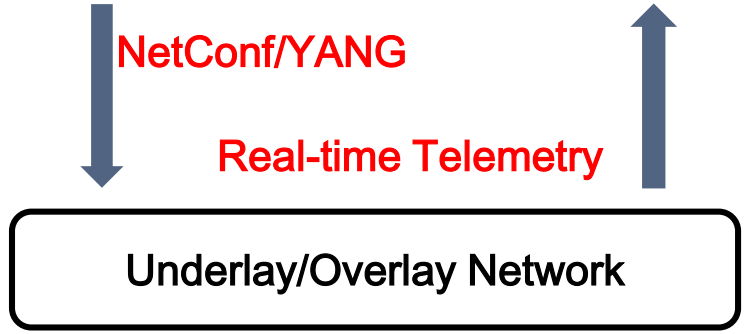
Autonomous Network Reference Architecture



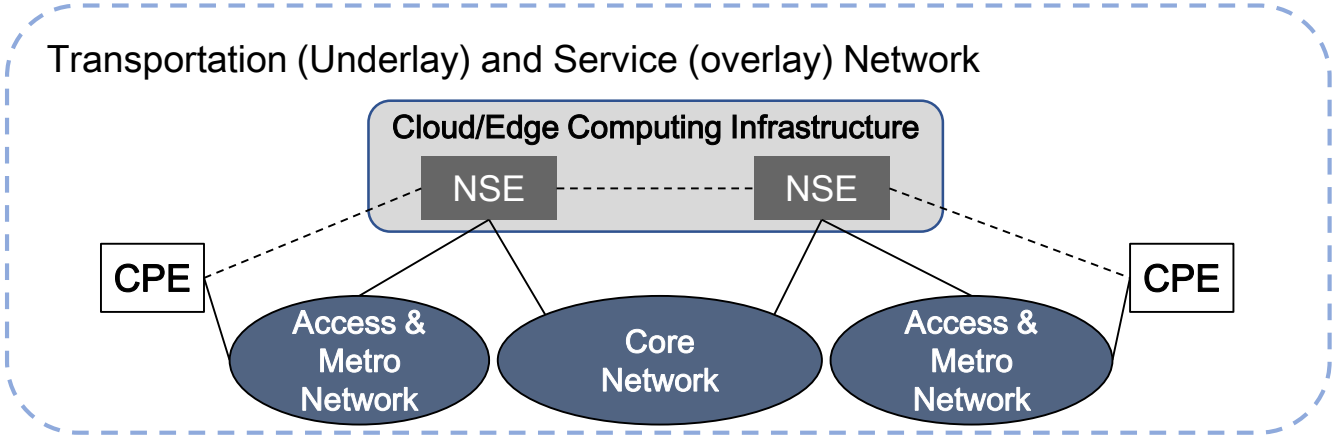








Principles for decoupling of network service and transportation



Network service and transportation technology are agnostic mutually and can be replaced independently;

Various transportation with different technology can be chosen for specific service

Multiple kinds of service can be supported by a specific transportation technology

Key design challenges for network transport layer

① **Decoupled from service**

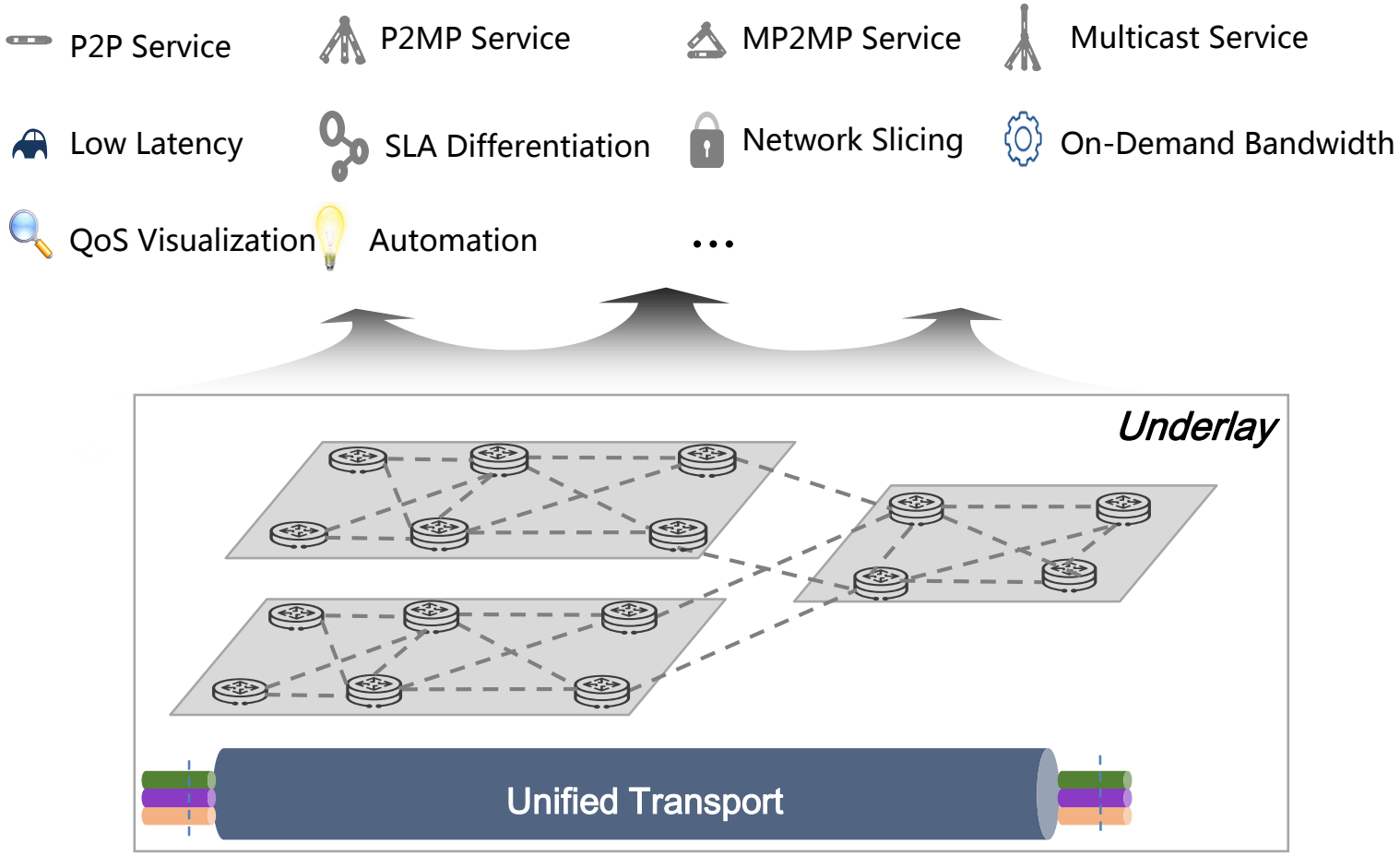
② **Simplified protocols system** to make it easy for O&M, and more robust network

③ **High utilization** by routing with service SLA as input

④ **High Availability,** to recover underlay path quickly at failure, without awareness by overlay, lower the protection requirement of overlay

⑤ **Automatic O&M**, based on machine analysis ans inference, lower the bar for O&M personnel requirement

⑥ **Open programmability**, provide P2P & P2MP service to overlay, with open SLA capability etc

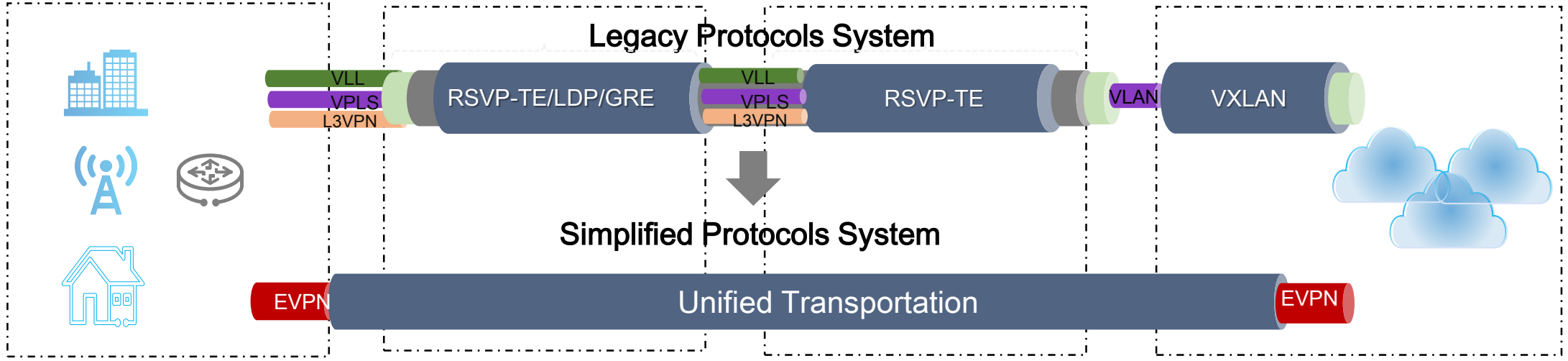


How to guarantee the capacity growth and resource utilization with reasonable cost?

How to visibility and guarantee SLA of service?

How to achieve always-on underlay?

Simplify the network transportation protocol with SR



10+ Protocols -> 2 Protocols

RSVP-TE/LDP/GRE/Vxlan/L2TPv3/E-line/E-tree… → SR/EVPN

Multi-domain -> Seamless

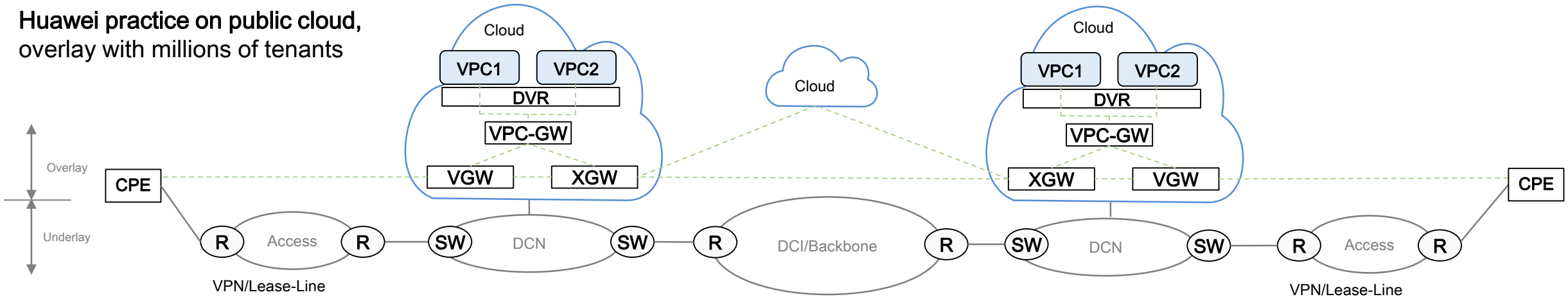
ACCESS-METRO-CORE-DC → ACCESS-DC

Seamless	1 hop	Simplified	All Scenarios
service automation + optimization of path	from access to application	native IP forwarding + path control	backhaul , leased private line, home access, cloud…

Use case of Cloud based overlay virtualized network

1. Deploy VNFs for overlay network, including XGW, VGW, etc. Separate services and transportation network
2. XGW connects tenant VPCs cross-region through VXLAN tunnel on overlay layer, DCI Physical backbone network only provide IP connectivity and do not concern the tenant information.
3. VGW work as the unified VPN Access point of massive tenant sites via lease Line/MPL S VPN and IPSEC VPN etc.
4. VGW connect to XGW, vRouter through VXLAN. The DCN only provide IP connectivity and do not concern the tenant information.
5. XGW, VGW and other VNF support scale-out

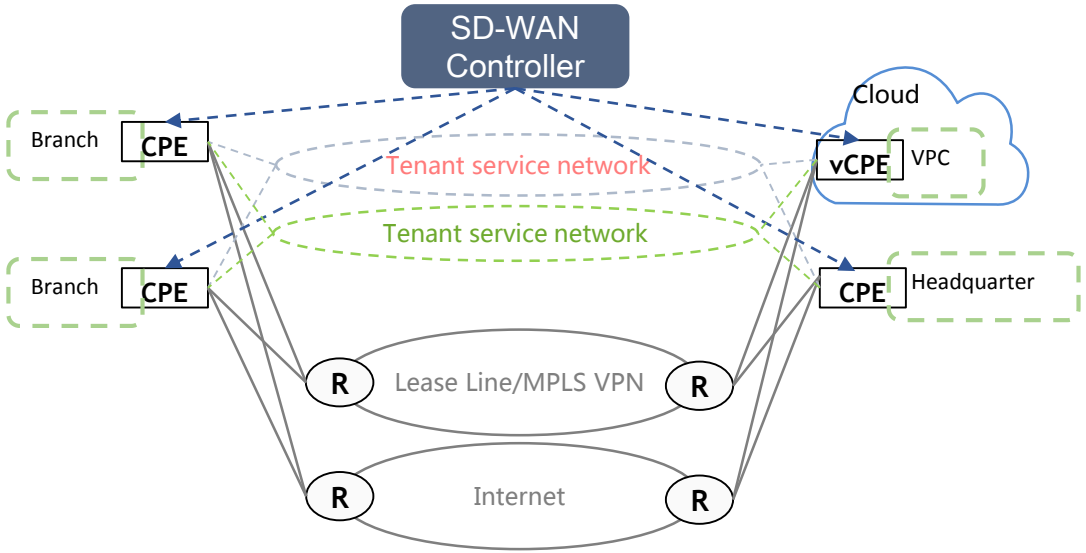
Huawei practice on public cloud,
overlay with millions of tenants

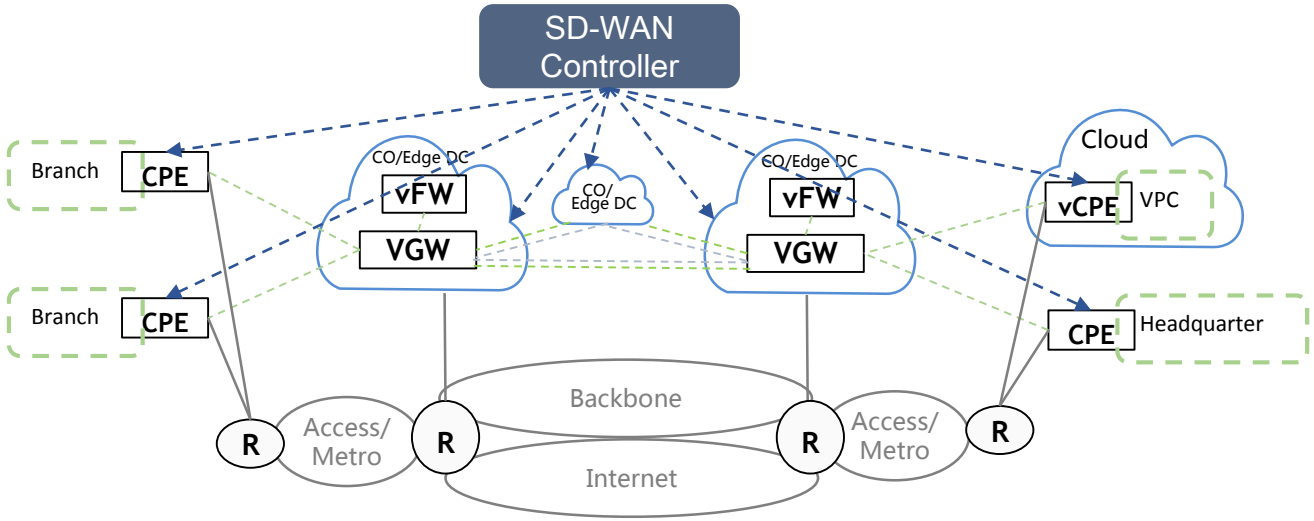


Key Targets:
- One point access for global network
- Service provisioning in minutes and routing convergence in seconds

Use case of SD-WAN, overlay service network for enterprise

Challenges for SD-WAN:
- ✓ Very big scale: massive tenants and CPE
- ✓ Smart routing: based on service level, policy, by tunnels
- ✓ Complex security environment: efficient security mechanism required
- ✓ Efficient protocols; light-weight , to support routing, path steering, policy and security
- ✓ Complex network environment: multiple IP address and dynamic IP address with CPE, NAT traversal, multi-layer NAT…





All SD-WAN vendors/providers are develop their proprietary protocols or extension to meet requirements, such as BGP extension to distribute tunnel and policy and to implement secret key negotiation. The explosion of SD-WAN solutions makes the interoperation very hard. Meanwhile, the security of each solution is not guaranteed.
Suggest IETF to standardize technology for SD-WAN, including protocols and security;

Open network capability based on YANG model to enable automation

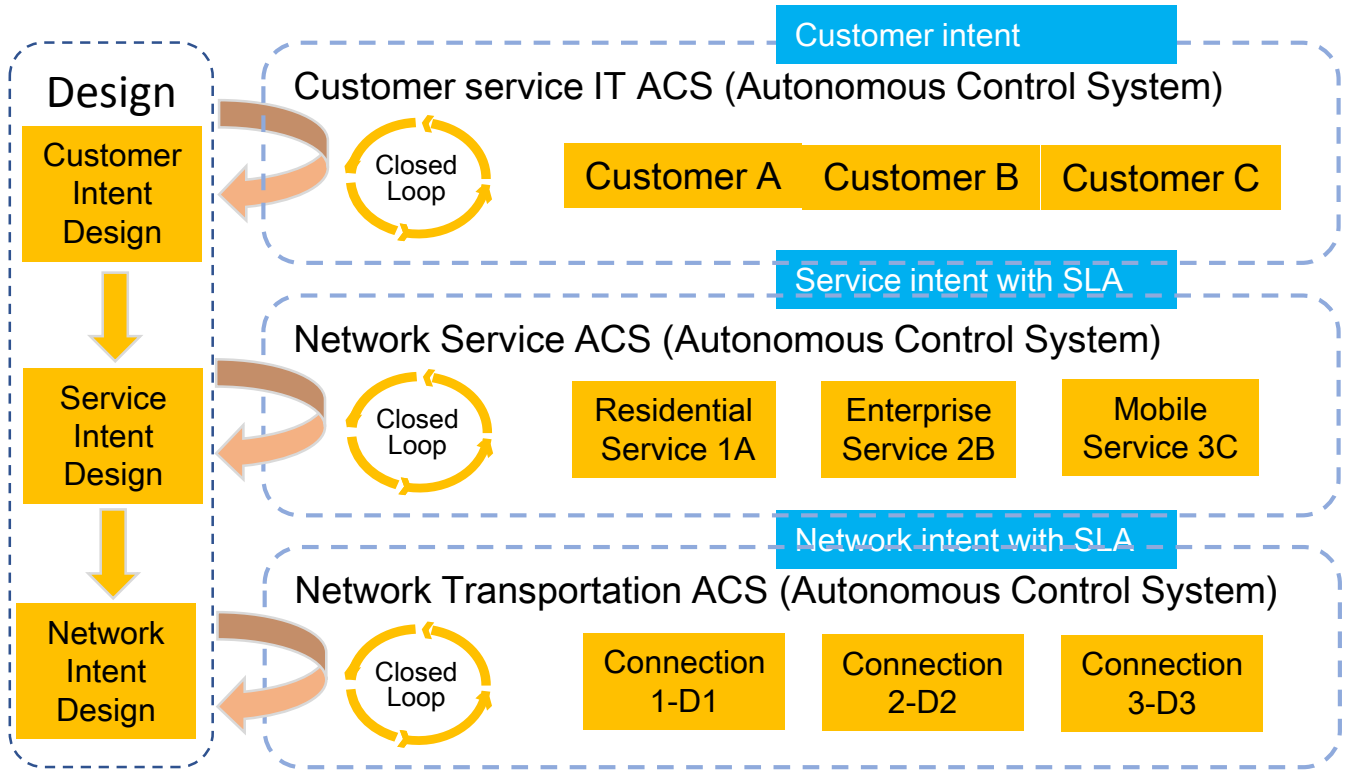
- ✓ Network automation is a network-wide mechanism, which involves various network element, software component, platform from various vendors. Capability openness is key for network automation.
- ✓ Traditional management protocols, such as CLI, is not optimized for software processing and difficult for operating programmatically. Transaction-based tools, optimal to software, good at validating results, are needed to fill the gap.
- ✓ YANG data Model driven management is the most practical and widely adopted approach. Decouple Service Model from Resource Model provide agile service creation, delivery and maintenance

Network Service YANG Model

- Independent of technology and operator, vendor
- Specify by operator on service intent(i.e.,what customer wants), but not how to implement it, using business-friendly concept
- Model Driven Service API, e.g., IETF L3SM model

Network YANG Model

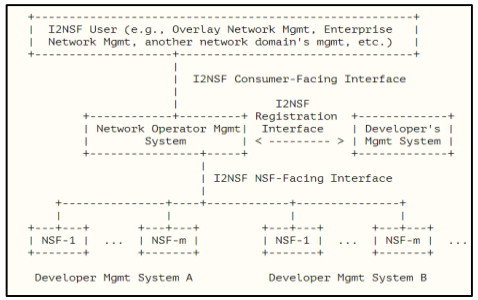
- Specify how to realize the service
- Vendor Neutral vs Vendor specific
- Provide Network visibility and support trouble shooting and diagnostic
- Expose resource to customer
- Allocate resource and tune resource distribution.



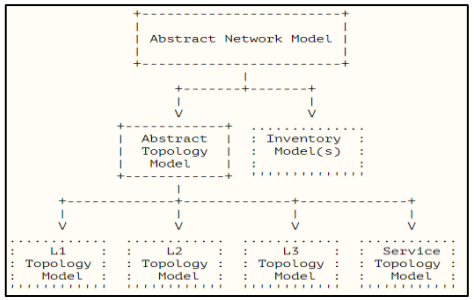
Expediting the standard process of YANG model

IETF has already developed plenty of YANG model standards, thank you!

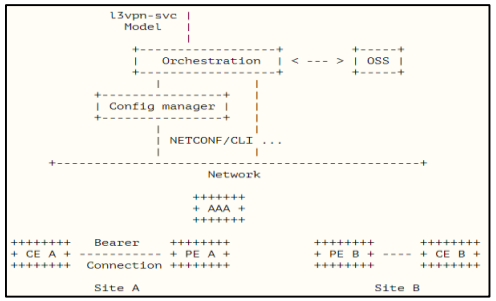
Service Models



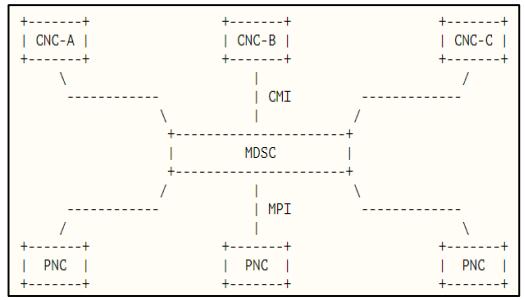
I2NSF



I2RS Topology



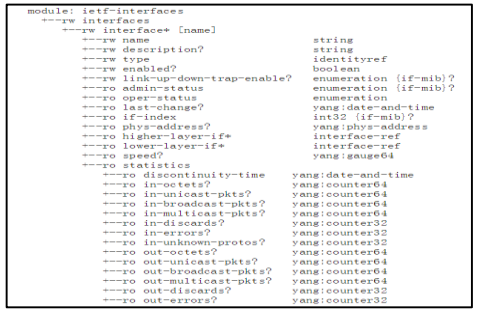
L3SM/L2SM



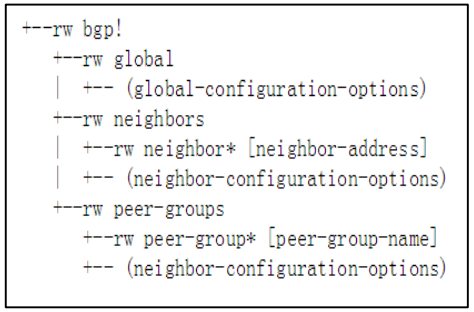
ACTN

...

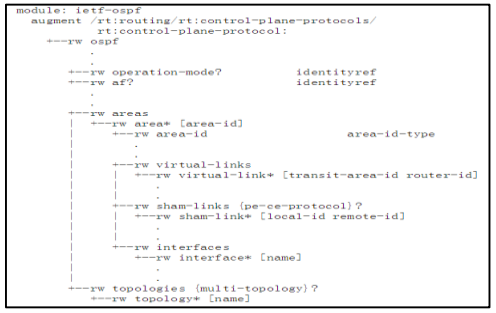
Protocols Models



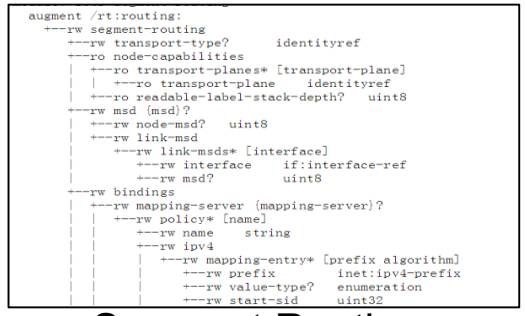
Interface



BGP



OSPF

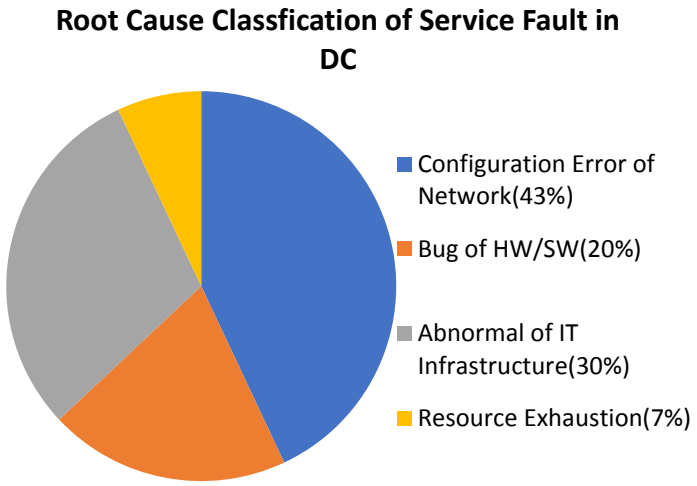


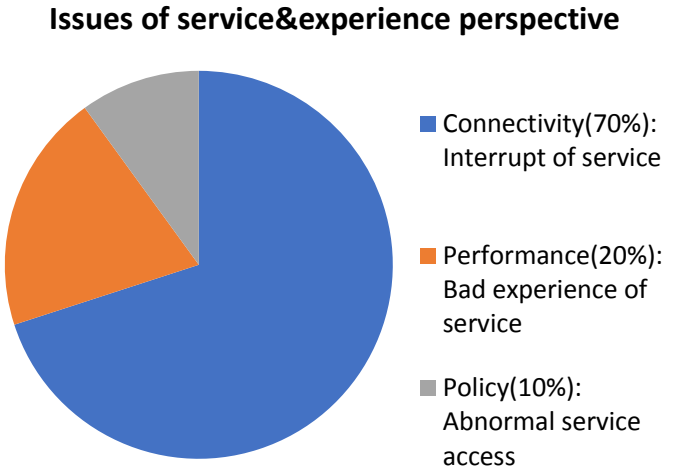
Segment Routing

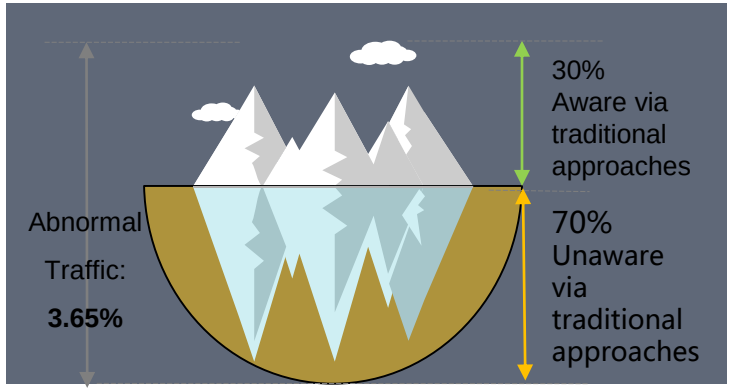
...

- The industry wants the YANG models now, while many IETF YANG model work are still in WG drafts or even individual drafts phase. Suggest to expedite the process. A simplified standard model is still better than none.
- There are many YANG model standardization work across various standards organizations. Overlapping may happen, suggest IETF to participate more industry coordination, even lead the effort.
- The industry does not know IETF model well! Suggest IETF to advertise its YANG model, especially service YANG model, to the industry.

Challenge for analytics and intelligence of autonomous network



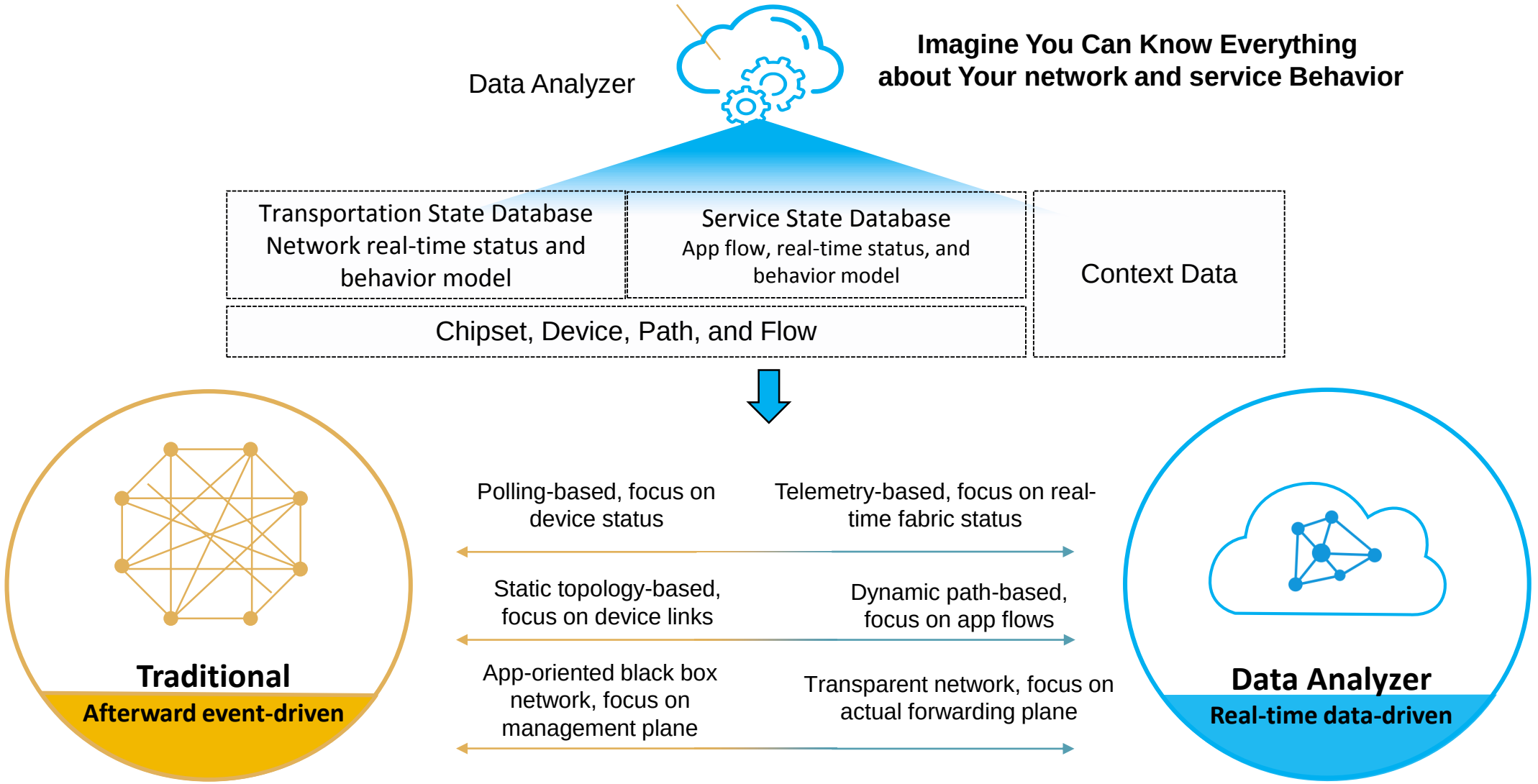




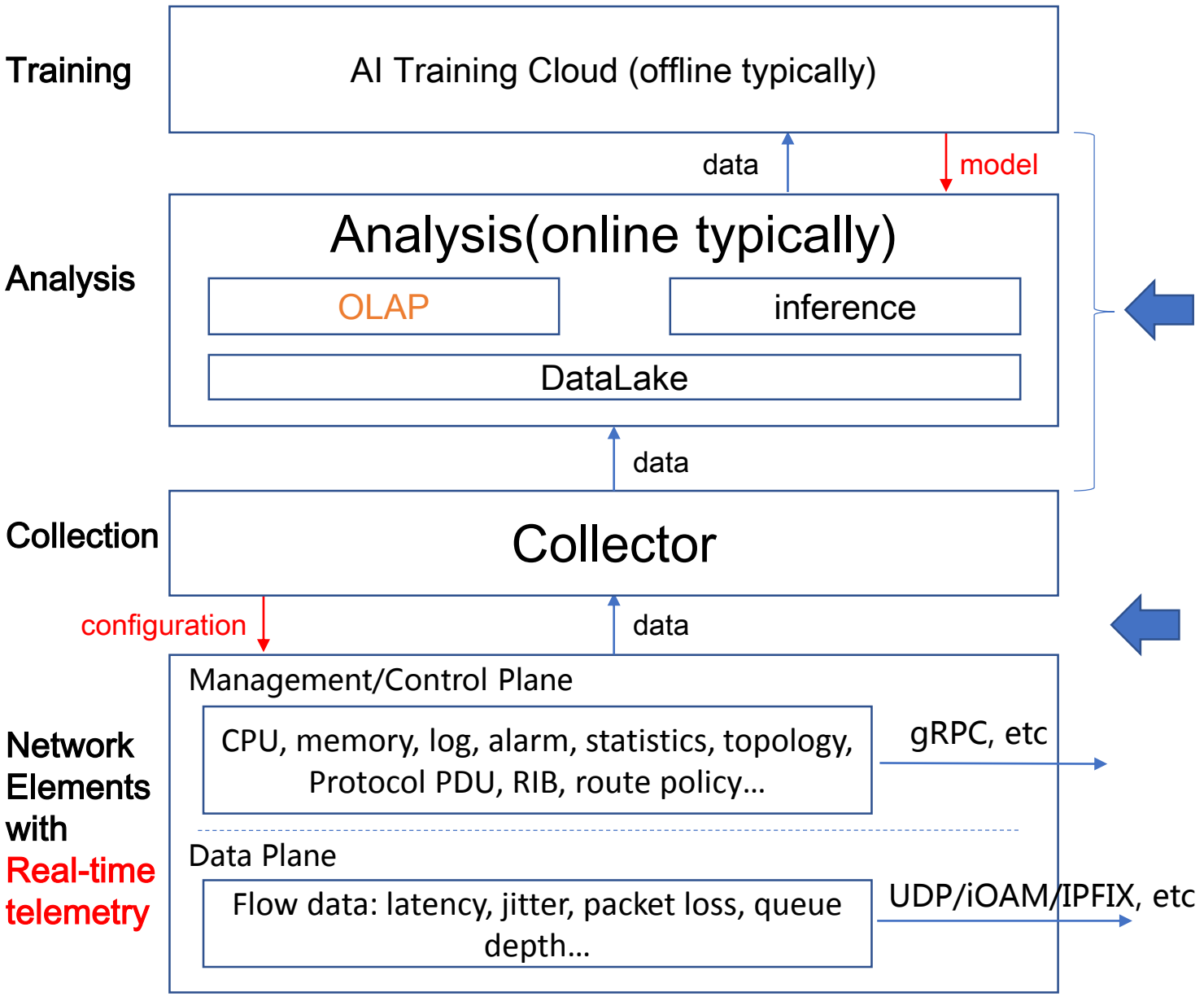
- **Lack of data** for fault cause analysis
  - Not coverage completely from chipset, device, network, IT infrastructure, flow and applications
  - Low sampling frequency, min -> ms;
  - Lack of historic data, **>90%** does not support fault playback
- **Unaware of abnormal** application and network **status**, majority faults are detected **passively**
- Lack of capability to **correlate** the issues between network and applications
- Capability to **predictive** resource exhaustion(<7%), bugs of HW/SW(<20%), configuration error(<43%)

- Data from some real typical medium **DC(5300+ VM, 65 subnet)**
- Average number of flow:96,545,774/day，among them 3,543,230(3.67%) are abnormal

How to improve the analysisin capability of autonomous network



Technology full stack of network analysis & Intelligence



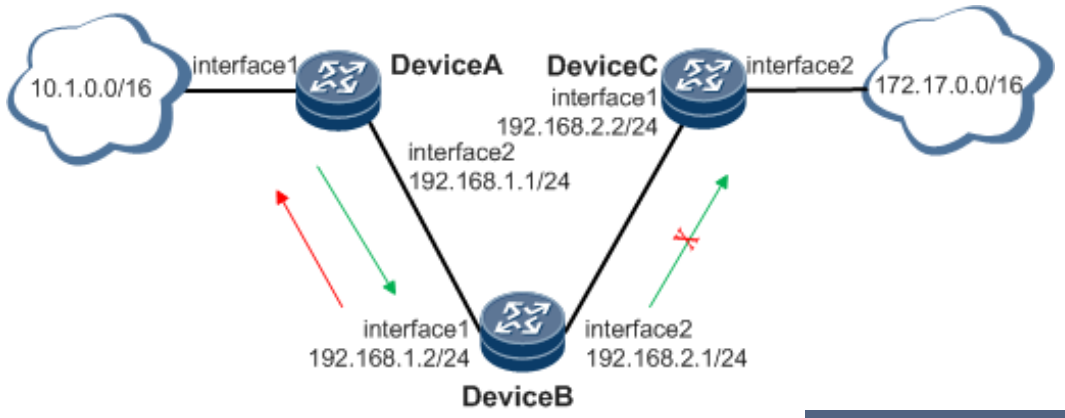
The interface among Training, Analysis and Collection components are service interfaces. Service models can be standardized but in many case not required because it's internal to software system.

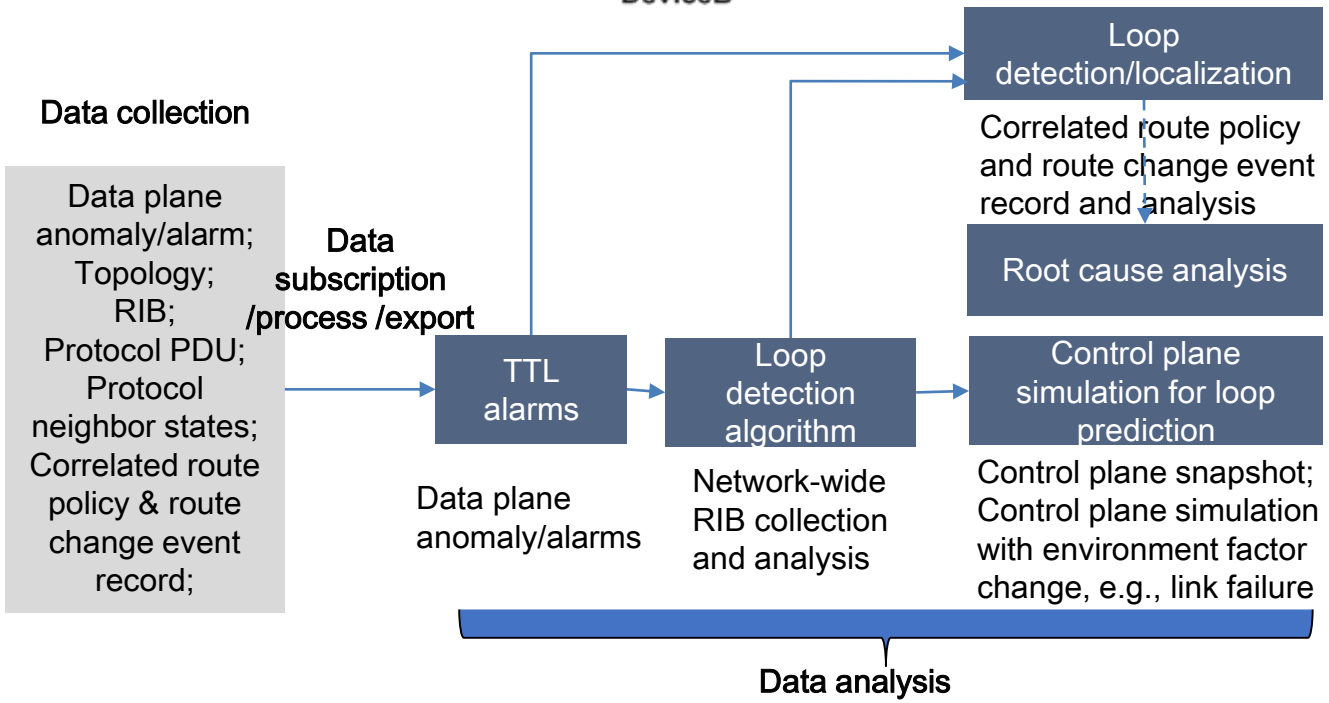
To define what the network element should submit, in what format, encoding, protocols, the domain of standardization, especially the capability of network elements.

- ✓ **Data Subscription:** YANG push
- ✓ **Data Process:** Smart filter, soft/hard DNP (dynamic network probe), Sketch, Marking Trigger
- ✓ **Data Export:** BMP, iOAM, IPFIX, UDP, Netconf, gRPC…

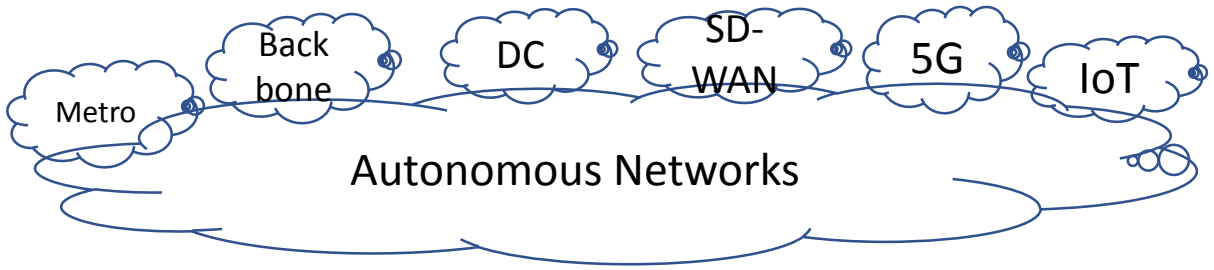
Case Study: Route loop detection, localization, root cause analysis and prediction

- Troubleshooting use cases
  - Routing table error, e.g., route loop
  - Route loop types
    1. Loop currently exists, and reflected at the data plane
    2. Loop currently exists, but not yet reflected at the data plane (i.e., no data flow is currently traversing the path)
    3. Loop currently does not exist, with environment change (e.g., link failure), the loop appears
- Gap and Motivation
  - Traditional device-by-device CLI check is both time and labor consuming
  - Having difficulty correlating the route loop with root cause
  - Not capable of predicting route loop
- Objective
  - Detecting and locating issues in seconds/minutes
  - Accurate root cause analysis to module /configuration /policy
  - Control plane simulation for loop prediction





Security Consideration



DDoS	Routing
	Transport Protocol
	Layer 2 Security
Physical Security Issues	

IETF security protocols:

- E2E encryption: TLS, IPSec
- AAA: EAP,
- AUTH: Kerberos, Radius, Diameter
- Routing: RPKI, IPv6Sec, PKIX
- DNS: DNSSEC, DANE
- Internet: httpauth, Oauth, Tokbind
- Codec: CMS,JOSE
- IoT: ace, core, suit, t2trg…

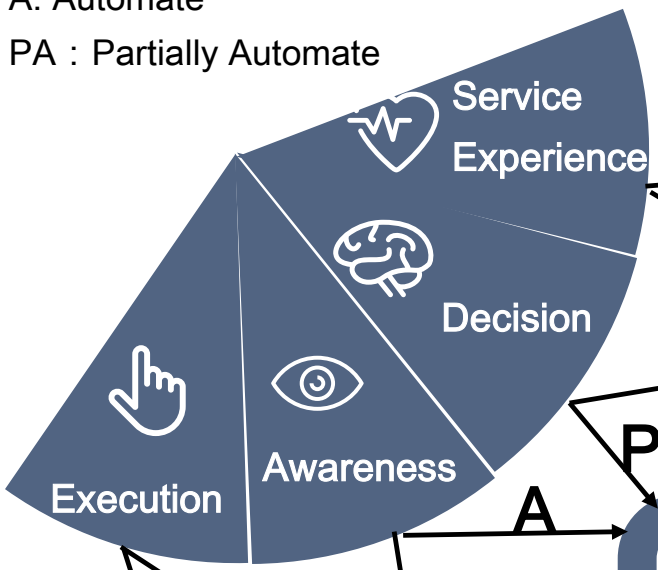
Question : Different network scenarios face different security issues, how to design a reasonable security for each of them.

Suggestion : IETF works more closely with other SDOs (IEEE-802.11/802.15, BBF, 3GPP, etc.) to design the suitable security solutions, prevent network security from impeding the interworking of global network.

Maturity level suggestion of autonomous network

A: Automate

PA：Partially Automate



A

PA

L5： Full Autonomous Network

✓ Closed-loop automation capabilities across multiple services, multiple domains, and the entire lifecycle.

A

PA

L4：Highly Autonomous Network

✓ In a multi-domain environment, predictive or proactive closed-loop management of service and networks.

A

PA

L3： Conditional Autonomous Network

✓ Senses environmental changes in real time, optimize and adjust itself to the external environment for closed-loop management.

A

PA

L2： Partial Autonomous Network

✓ Closed-loop O&M for some component under specific external environments, lowering the bar for personnel experience and skills.

PA

L1：Assisted O&M

✓ Executes certain sub-tasks based on existing rules to increase execution efficiency.

L0：Manual OAM

✓ Assisted monitoring capabilities, which means all dynamic tasks have to be executed manually.

Summary

Key for autonomous network:

Decoupling network transportation and service, transportation prefer to HW and service prefer to SW

- Simplify the protocol for network transportation, realize e2e seamless network
- Enhanced the protocol for network service, esp. for scalability, flexibility and security

Decoupling network operation and service IT system based on model-driven automation engine

- Standard for network and service YANG model are very important

Close-loop control is the key for autonomous and AI is essential for proactive maintenance

- Telemetry definition is very important for network analysis and intelligence
- Domain knowledge is critical for data analysis efficiency

Autonomous network is a long journey and need collaboration of industry

Thanks!