MPLS SD&AI NET WORLD22

IPv6 Enhanced and Application-aware Networking (APN)

Zhenbin Li

Chief IP Protocol Expert and Standard Representative

Huawei Technologies

MPLS SD&AI NET WORLD22
5/6/7 APRIL

Zhenbin (Robin) Li

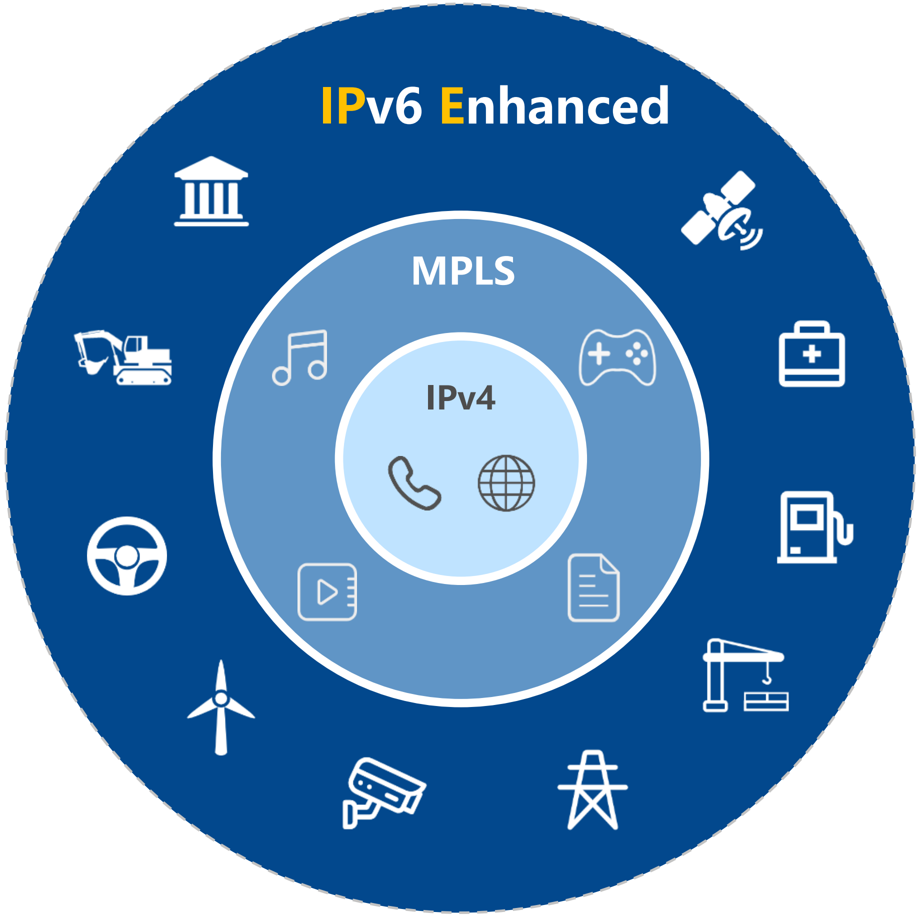
Huawei Chief IP Protocol Expert
IETF Internet Architecture Board (IAB) Member
https://www.iab.org/about/iab-members/

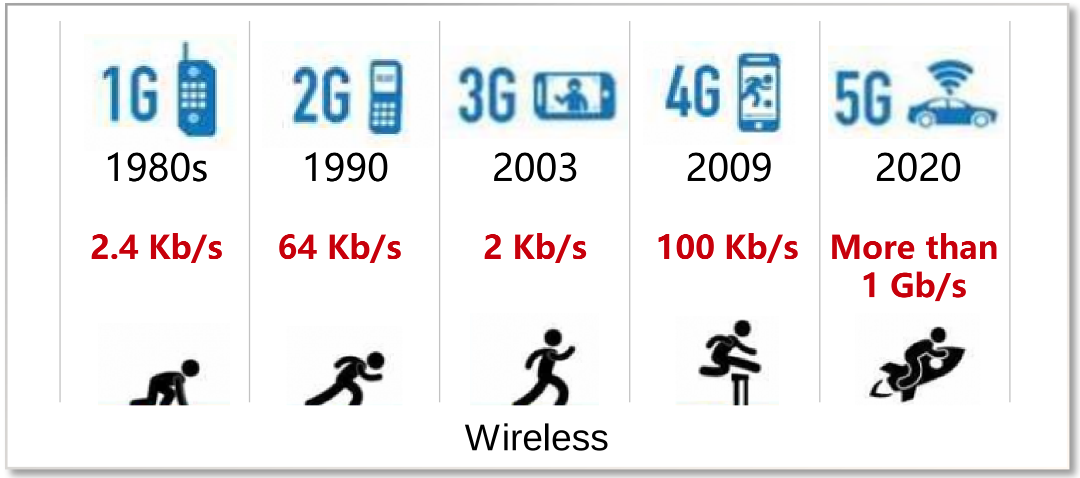
- 15+ years research and development work in IP Operating System and SDN Controller as the system architect.
- Be active in standard activities since IETF75 and propose 100+ drafts/RFCs in RTG/OPS areas (www.ipv6plus.net/ZhenbinLi).
- Promoted SDN Transition (Netconf/YANG, BGP/PCEP, etc.) innovation and standard work in the past years.
- Focus on the innovation standard work of SRv6, 5G Transport, Telemetry, Network Intelligence, etc. since 2016.
- Publish the book "*SRv6 Network Programming: Ushering in a New Era of IP Networks*"
- Be elected as the IETF IAB member to be responsible for Internet architecture work from 2019 to 2020.
- Be elected again as the IETF IAB member to be responsible for Internet architecture work from 2021 to 2022.

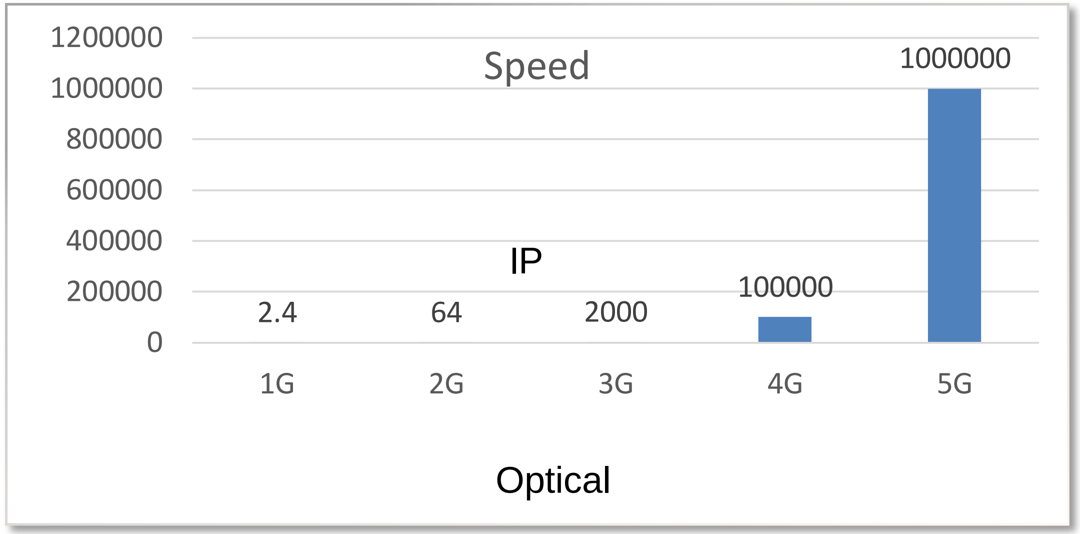
Agenda

- IPv6 Enhanced
- APN: Application-aware Networking
- CAN: Computing-aware Networking
- Summary

IP Evolutions: Applications Drives the Change of IP Network Architectures



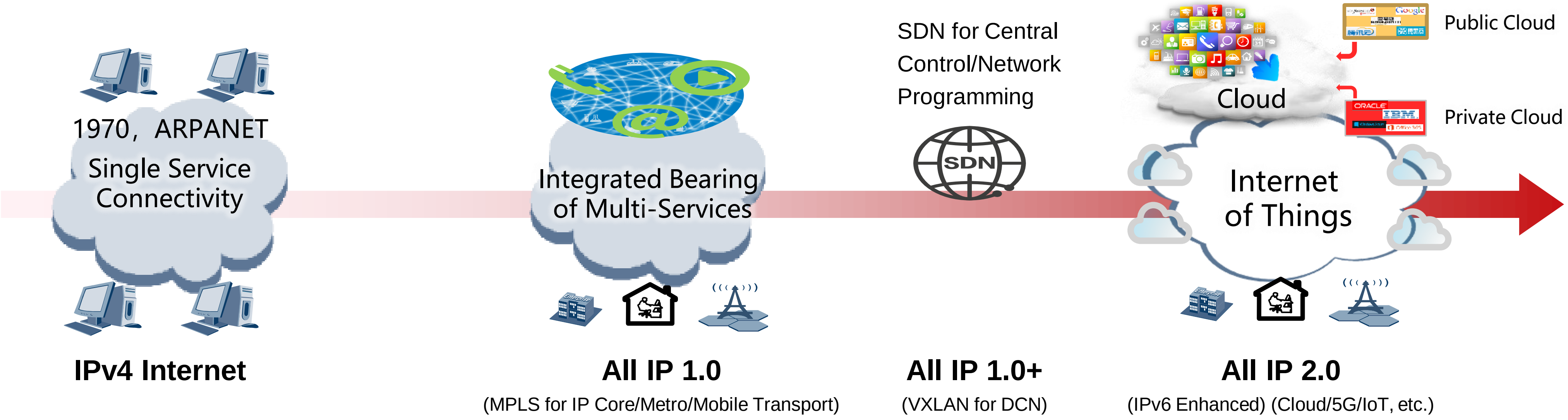




Source: ETSI IPv6 Enhanced Innovation (IPE) - Gap Analysis, August 2021

HUAWEI

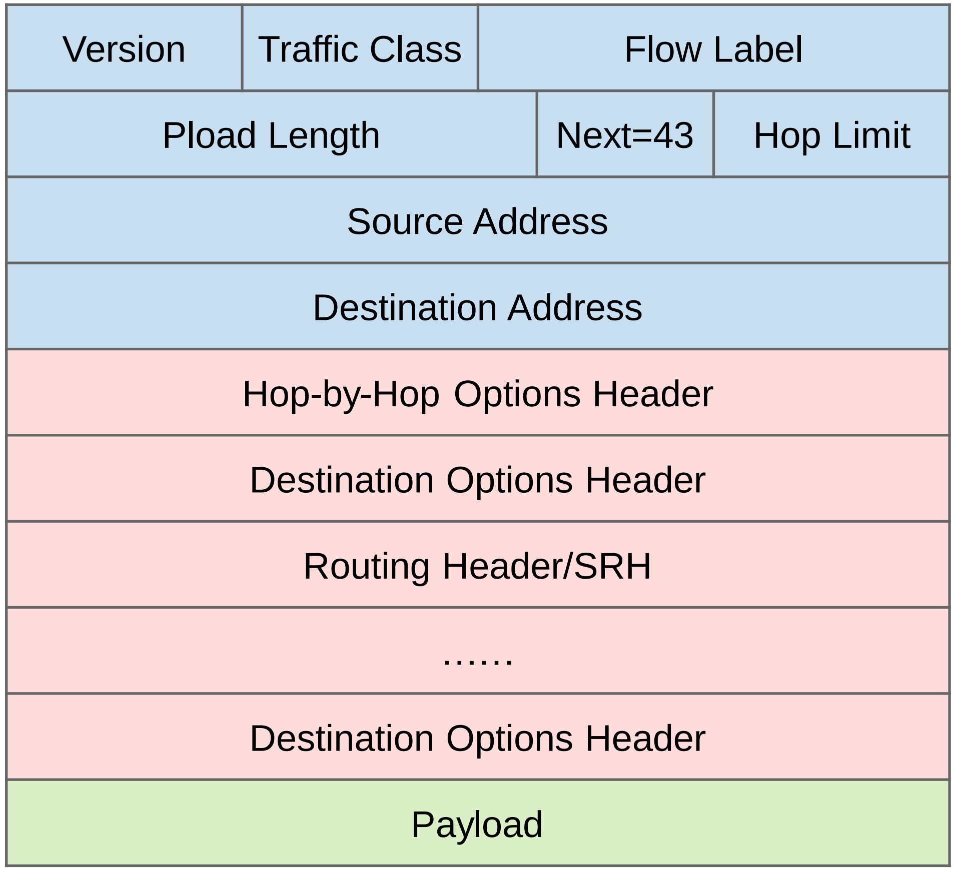
IPv6 Enhanced: A New Era of IP Networks for 5G and Could



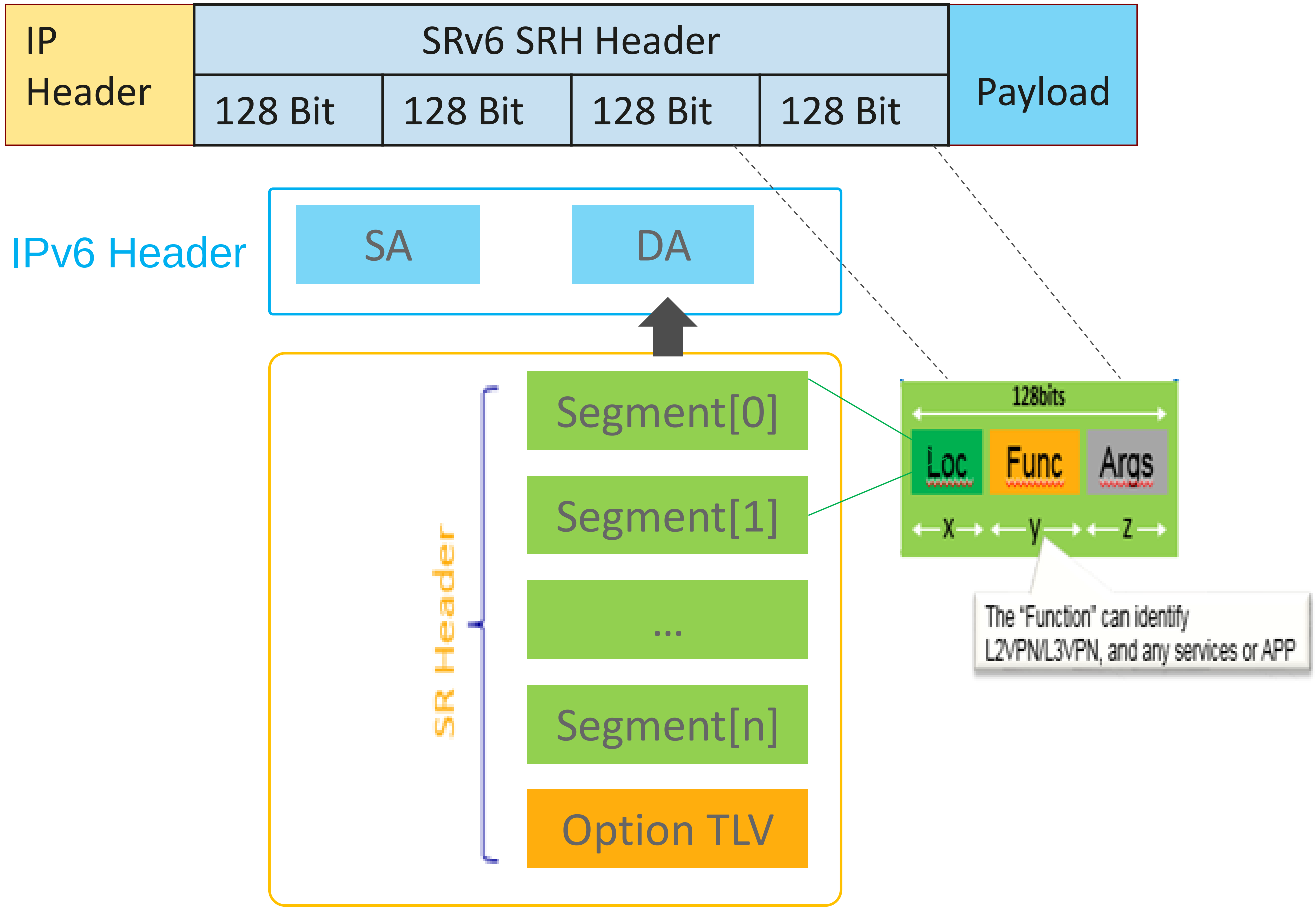
- Rethinking on IPv6: Address Space is not enough.
- New Chance of IPv6: 5G changes the attributes of connections, and cloud changes their scope.
- Mission of IPv6 Enhanced:
  - Integrate different network easier based on affinity to IP reachability.
  - Provide more encapsulations for new network services such as Network Slicing, DetNet, etc.
  - Cross the chasm between application and network based on affinity to IP and Network Programming conveying application information through IPv6 Extension Header into network.
  - Promote IPv6 combining with requirements on more address spaces.

IPv6 Extension Headers and SRv6: Release Network Programming Capabilities

IPv6 Extension Headers



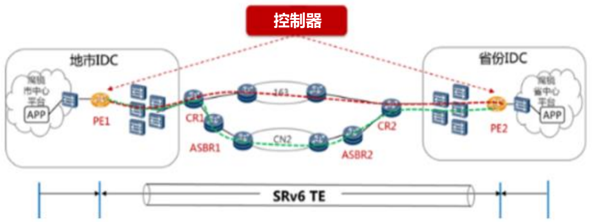
SRH: Three Layers of Programming Spaces



IPv6 Enhanced: Phased Development, Continuously Improving Network Quality

IPv6 Enhanced 1.0
Network programming

2020-2021

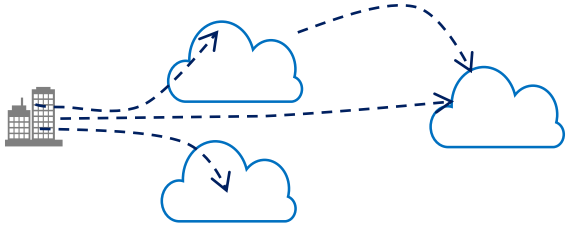


Partial autonomous network

- SRv6 BE/TE/Policy
- Quick provisioning
- Path optimization

IPv6 Enhanced 2.0
Experience assurance

2021-2023



Conditional autonomous network

- Numerous network slices
- In-band flow measurement
- New-type multicast
- Visualized and optimal experience

IPv6 Enhanced 3.0
APN

2023-2025

Highly autonomous network

- Application-based awareness
- Policy mobility, consistent experience, security anywhere
- Per-flow SLA assurance

IPv6 Enhanced Standardization Work Layout

IPv6 Enhanced 1.0
SRv6

- **SRH RFC8754**
- **SRv6 NP RFC8986**
- SR Policy **WGLC**
- ISIS **WGLC**
- OSPFv3
- VPN **WGLC**
- BGP-LS **WGLC**
- PCEP
- Protection
- YANG
- Deployment

IPv6 Enhanced 2.0
5G&Cloud

VPN+: Framework | SR Data Plane | IPv6 DP | IGP | BGP-LS | MT-based | Flex-Algo based

IFIT: Framework | IPv6 Data Plane | IGP | BGP | BGP-LS | PCEP | YANG

G-SRv6: Requirements | Analysis | Framework

BIERv6: Requirements | Encapsulation | IGP

OAM | Path Segment | DETNET | SFC | SD-WAN | PMTU

IPv6 Enhanced 3.0
APN6

Problem Statement | Use cases | Framework | Encapsulation | Protocols Ext.

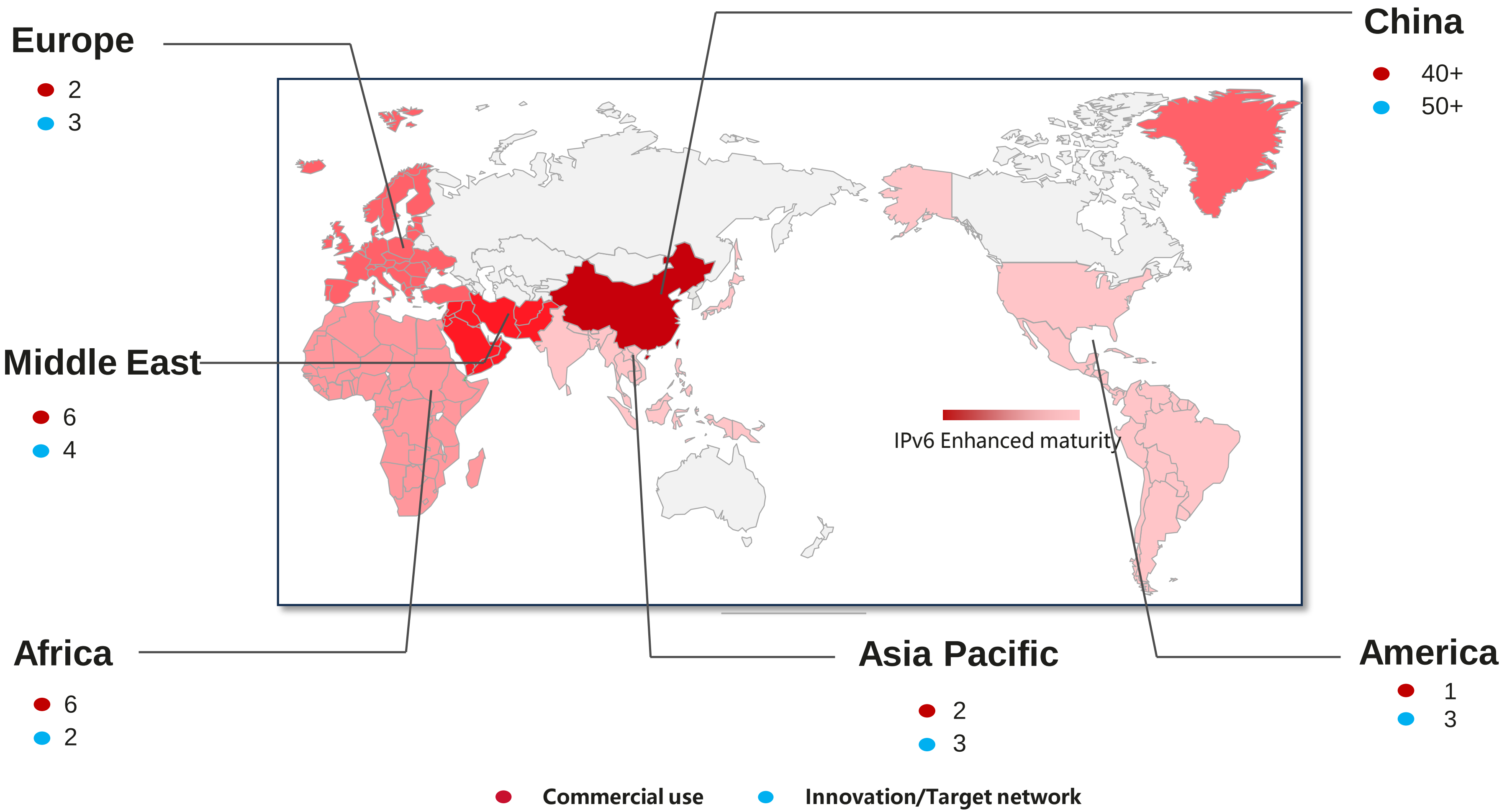
Legend: RFC | WG Draft | Potential WG Draft | Individual Draft

Please visit www.ipv6plus.net for the latest progress

HUAWEI

IPv6 Enhanced: Fast World-Wide Development

IPv6 Enhanced Deployment: 140+ SRv6; 30+ IP Network Slicing



HUAWEI

Agenda

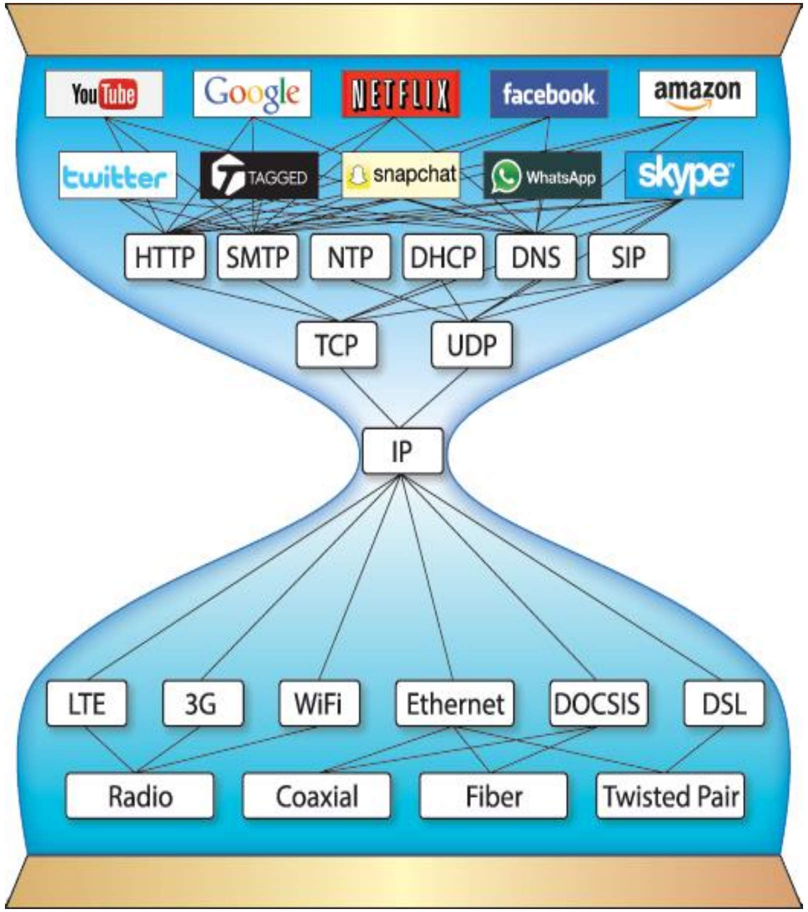
- IPv6 Enhanced Innovations
- APN: Application-aware Networking
- CAN: Computing-aware Networking
- Summary

Background 1: Challenges of Operators' IP Network Services

Bottlenecks in Carriers' Transport Networks

1. Pipelining
• Great BW requirement increase but very **limited revenue** from the network service
• Network does not know about the accurate service requirement from applications, so SLA is actually guaranteed by low bandwidth utilization.
	2. Marginal Utility Diminishing
	• Repeated network function developments
	  • MPLS：VPN/TE/FRR
	  • SR-MPLS：VPN/TE/FRR
	  • SRv6：VPN/TE/FRR

3. Constrained Network Capabilities
• Network capabilities are improved greatly
  • DiffServ/ HQoS/SR Policy/Slicing/ Telemetry/SFC/…
  • Significantly improved scalability
• Lack of flexible fine-grained mapping between applications and network services
	4. Encryption
	• Encryption makes it more difficult to provide fine-granularity network services
	  • QUIC invalidates network middle box
	  • ISOC advocates end-to-end encryption to protect security and privacy: "*Encryption is vital to a safe, secure and functioning world.*"



More and more new applications are ever-emerging.
Network needs to cooperate with applications to provide fine-granularity network services while guarantee security.

HUAWEI

Background 2: Challenges of Traditional Fine-grained Service Provisioning

Traditional methods		Challenges
5 Tuples	Using *{srcIP, dstIP, srcPort, dstPort、protocol} and* ACL/PBR to identify a flow	• Indirect application info which is in need of transition • Forwarding performance issues • Scalability issues from the limitation of dedicated hardware resource • Hardness of getting 5 tuples when encapsulated in tunnel
DPI	Deep Packet Inspection to identify application	• Challenges from privacy issues • Challenges from network security • Forwarding performance issues
Orchestrator and SDN	Applications ask orchestrator to interwork with network SDN controller	• Complex interaction • Too many interfaces to be standardized

TO BE: Convergence of application and network to provide fine-grained services

- Use Identifiers for mapping of applications' requirements and parameters to network service functions， to further release network capabilities
- The application-aware ID and parameters need to solve the challenges in existing methods and reduce CAPEX and OPEX
- IPv6 can act as an important medium in application and network convergence

Three Elements of APN

1. Open Application info carrying

- APP-ID
  - App ID
  - User ID
- APP Parameter Info
  - Bandwidth
  - Latency
  - Loss rate

2. Rich network services

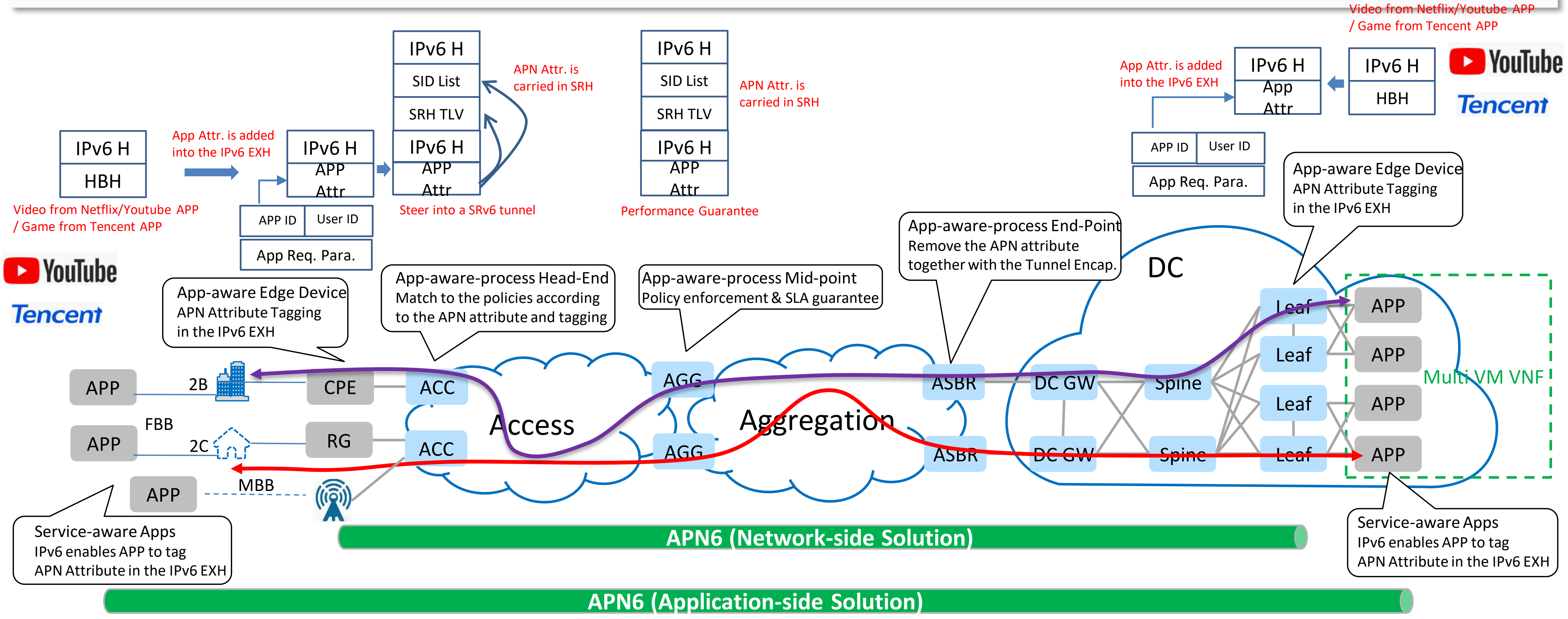
- DiffServ
- H-QoS
- SR Policy
- Network Slicing
- DetNet
- SFC
- Stateless Multicast/BIERv6

3. Accurate Network Measurement

- Finer-granularity
  - per packet vs. per flow, per node vs. E2E, individual vs. statistics, etc.
- Comprehensive measurements
  - per packet with per flow, per node with E2E, individual with statistics, in-band with out-band, passive with active, etc.

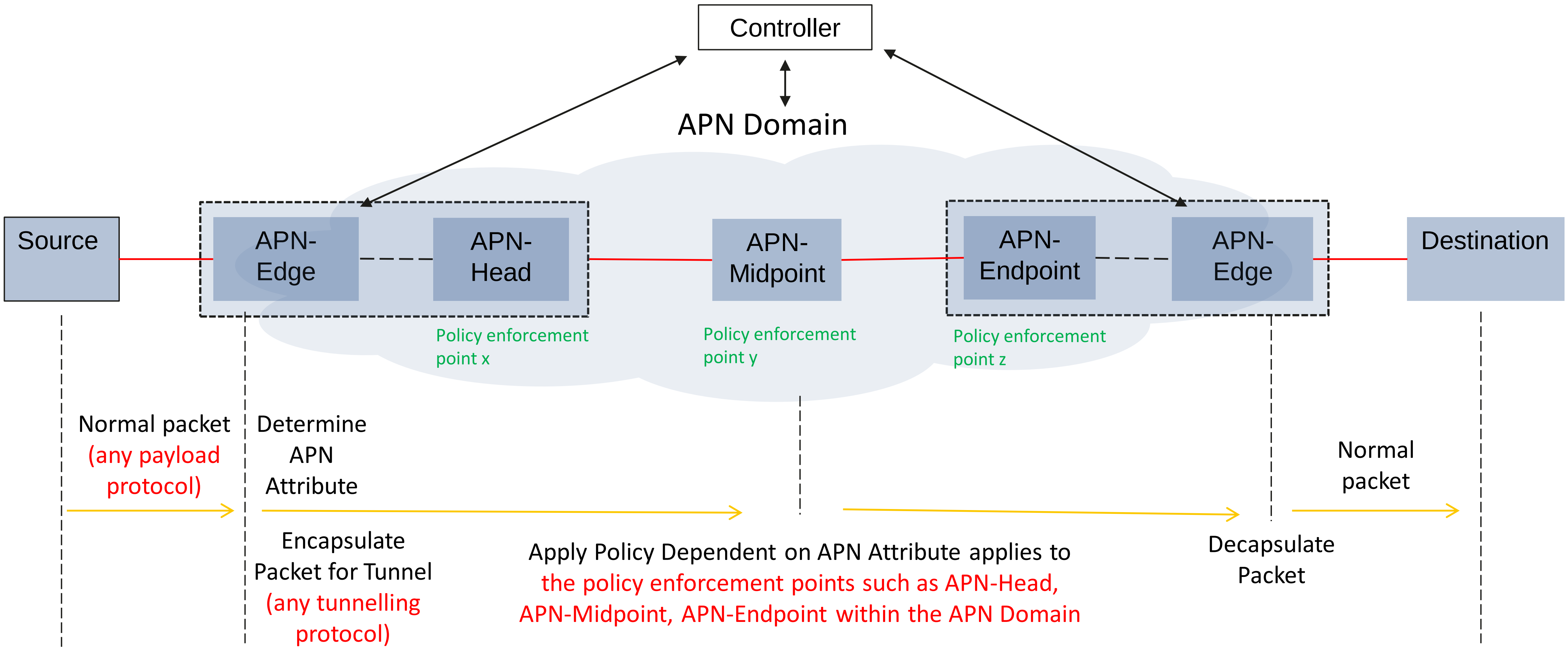
APN6: Application-aware IPv6 Networking

- Make use of IPv6 extensions header to convey APN attribute along with the packets into the network
- To facilitate the flexible policy enforcement and fine-grained service provisioning



https://datatracker.ietf.org/doc/draft-li-apn-framework/
https://ieeexplore.ieee.org/abstract/document/9162934

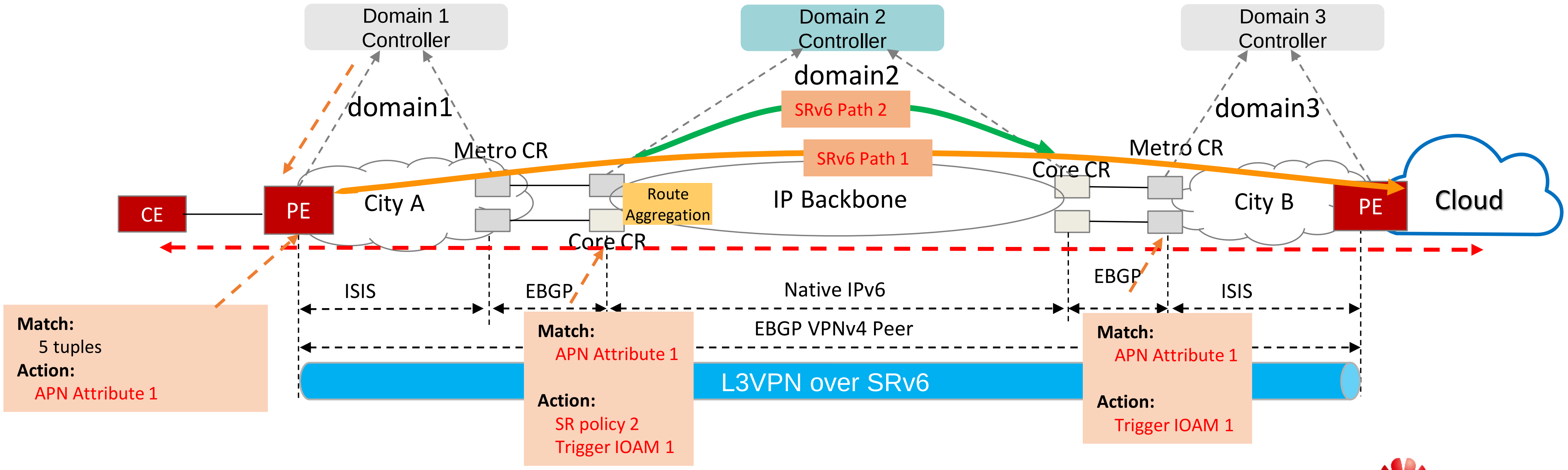
Reference Diagram of APN Network-side Solution



An APN Domain may span multiple network domains controlled by the same operator

Traffic Steering in the IP Backbone with APN

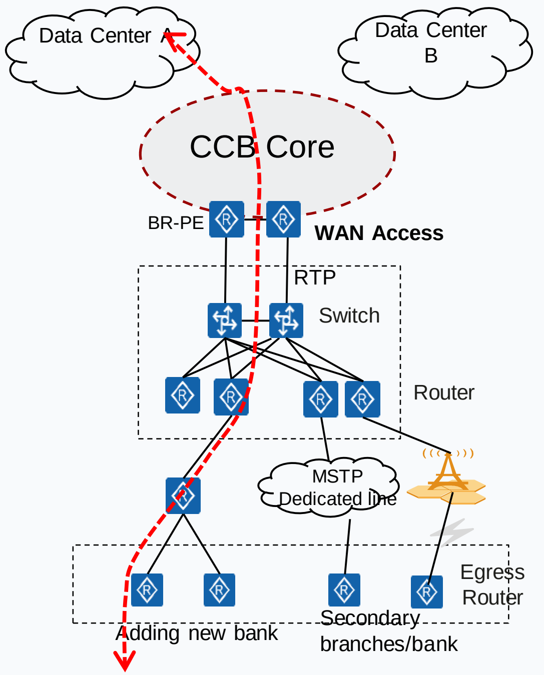
- APN attribute is encapsulated at the ingress node.
- With the APN attribute, the fine-granular traffic steering in the IP backbone can be easily facilitated.
  - To match some field(s) of the APN attribute, a path with low-latency can be selected and steered into.
- Other policy actions (such as IOAM) can also be triggered according to the APN attribute carried in the header.



Finance: App-level Quality Visibility and Assurance, Building Differentiated Service Capabilities through APN6+iFIT

Industry requirements: In finance, government (smart city) and other scenarios, application-level experience quality assurance is a key requirement
Solution : Identify applications on the access device and tag **APN6 ID**, and steer traffic of key applications/important video conferencing to SRv6 tunnel; combine **iFIT** and **APN6** to realize application-leverl quality visibility, quality difference delimitation and intelligent self-healing to improve service

AS IS: Lack of Application-Oriented Differentiated Service Capability



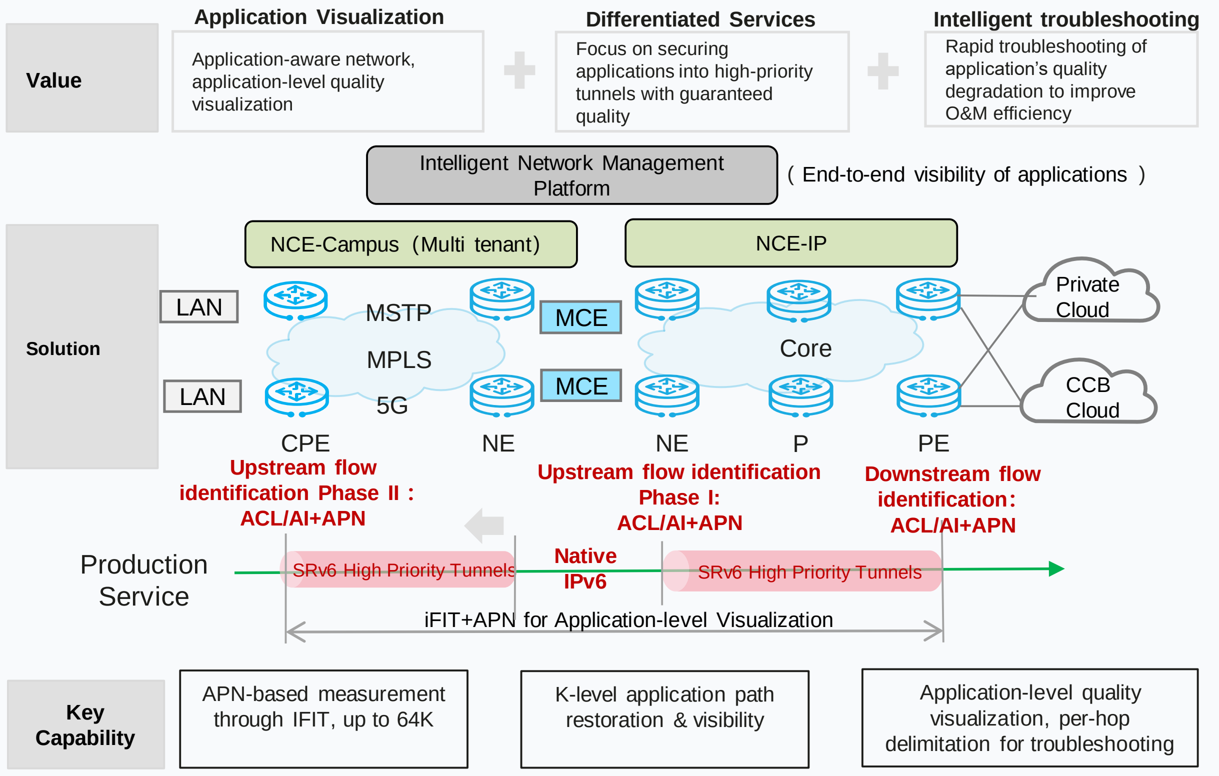
60K+IP addresses, 900+applications

Type	Service	Priority
A	Bank core business, head office/branch front-end system, imaging platform system, channel business	High
B	POS access/terminal front system, managed production system, image archive management system	High
C	OA office business, statistics/reports, file management type business	Middle
D	IT infrastructure business, third-party outreach, information, online training classes	Low

Key pain points: the network cannot sense the application and the experience cannot be guaranteed

Application unified bearing, unable to provide differentiated services	Application experience degradation cannot be quickly troubleshoot	Manual ACL configuration leads to complex network operation and maintenance

TO BE: Network differentiation bearing services, application-level quality visibility, user experience guaranteed



HUAWEI

Service Provider: APN6-based Mux-VPN Solution to Achieve Cloud&Network&Security Integration

Service changes: As business goes to the cloud, more and more value-added services will be centrally deployed and flexibly customized by users; security business is the key demand of enterprises, and the isolation demand between tenants is very popular

Key challenges: The current use of ACL to do business access control and tenant isolation control through ACL, consuming a large number of ACL, high hardware costs, poor business scalability, and costly post-maintenance

Solution : The service function chain is processed based on APN6, and the APNID is used to identify the tenants; the isolation control between users is done based on APNID, which can greatly simplify the configuration and reduce the ACL resource requirements.

Service Orchestration System

1. The service orchestration system send the commercial service to operator's operation platform

Operation Platform

Value Added Services	VAS1	VAS2	VAS3
SID Number	SID1	SID2	SID3

Tenant Service Agreement	User1	VAS1
	User2	VAS2/VAS3

Tenant Isolation Policy	User1
user2	Isolation

2. The operation platform sends the business policy down to the controller

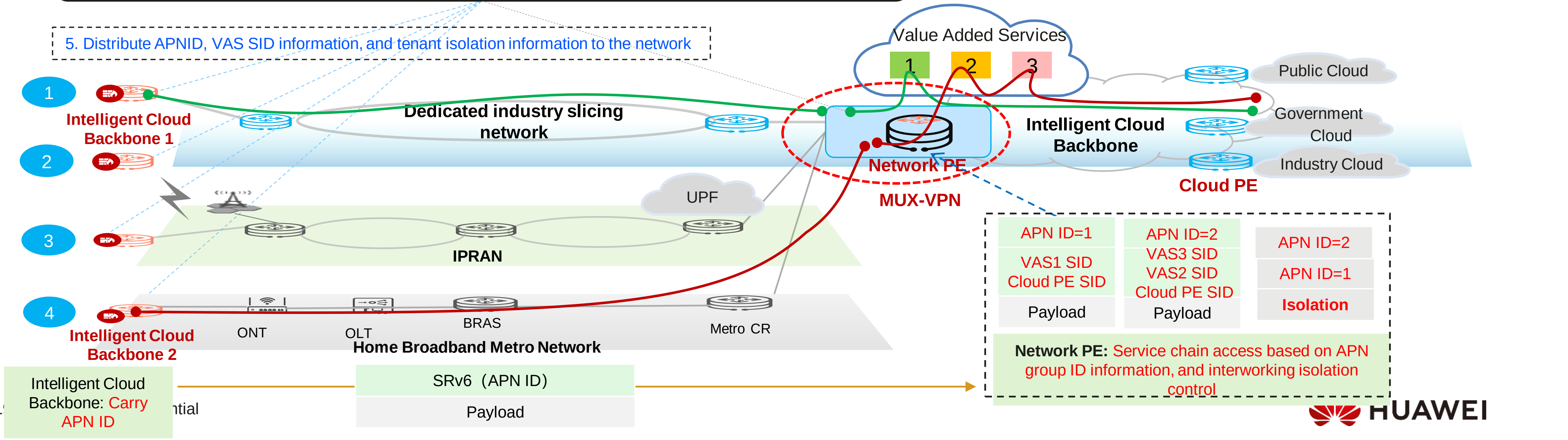
NCE

user1	APN1
user2	APN1

Isolation Policy	APN1
APN2	Isolation

APN Service Chain	APN1	SID1
	APN2	SID2/SID3

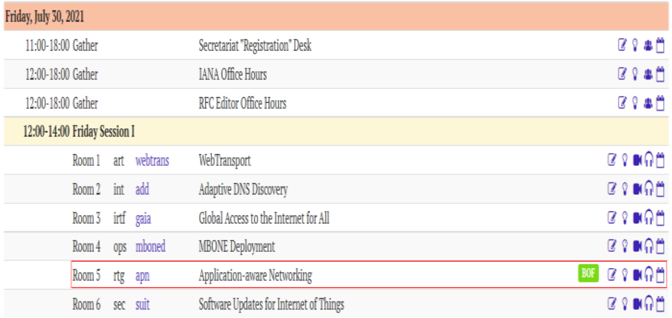
3. Assign APNIDs to users, associate user characteristics (ACL/interface/VPN, etc.)
4. Setup association between APN and VAS, configure APN-based isolation table



More Industry Consensus on APN and Approved IETF APN BOF

- **Side Meetings** @IETF105 & IETF108
- **Hackathons** @IETF108 & IETF109 & IETF110
- **Demos** @INFOCOM2020 & 2021
- **APN Mailing List** Discussions - apn@ietf.org
- **APN Interim Meeting** @IETF 110-111
- **APN BoF** @IETF111, Approved! 30 July 2021, 1200-1400 PDT

IETF111 APN BoF



Friday, July 30, 2021				
11:00-18:00 Gather			Secretariat "Registration" Desk	
12:00-18:00 Gather			IANA Office Hours	
12:00-18:00 Gather			RFC Editor Office Hours	
12:00-14:00 Friday Session I				
Room 1	art	webtrans	WebTransport	
Room 2	int	add	Adaptive DNS Discovery	
Room 3	irtf	gaia	Global Access to the Internet for All	
Room 4	ops	mboned	MBONE Deployment	
Room 5	rtg	apn	Application-aware Networking	BOF
Room 6	sec	suit	Software Updates for Internet of Things	

IETF105

IETF108

IETF109

IETF110

https://github.com/APN-Community

https://www.ietf.org/blog/ietf109-bofs/
https://www.ietf.org/blog/ietf110-bofs/
https://trac.tools.ietf.org/bof/trac/wiki/WikiStart (IETF111 BoF)

APN Papers for the Academia World

APN6: Application-aware IPv6 Networking

Shuping Peng, Jianwei Mao, Ruizhao Hu, Zhenbin Li
Datacom Research Department
Huawei Technologies, Beijing, China
pengshuping@huawei.com

Abstract—**This Demo showcased the Application-aware IPv6 Networking (APN6) framework, which takes advantage of the programmable space in the IPv6/SRv6 (Segment Routing on the IPv6 data plane) encapsulations to convey application characteristics information into the network and make the network aware of applications in order to guarantee their Service Level Agreement (SLA). APN6 is able to resolve the drawbacks and challenges of the traditional application awareness mechanisms in the network. By utilizing the real-time network performance monitoring and measurement enabled by Intelligent Flow Information Telemetry (iFIT) and further enhancing it to make it application-aware, we showed that the VIP application's flow can be automatically adjusted away from the path with degrading performance to the one that has good quality. Furthermore, the flexible application-aware SFC stitching application-aware Value Added Service (VAS) together with the network nodes/routers is also demonstrated.**

Keywords—IPv6, iFIT, Segment Routing, SRv6, SFC

I. Introduction

The network operators have been facing the challenges of providing better services to their customers. Nowadays it becomes even more challenging. As 5G and industry verticals evolve, the ever-emerging new services with diverse but demanding requirements such as low latency & high reliability are accessing to the network. Applications such as on-line gaming, live video streaming, and video conferencing have highly demanding requirements on the network performance. Meanwhile, they are the actual revenue-producing applications. The customers of network operators desire to have differentiated SLA guarantee for their various demanding new services. However, the current network operators are still not aware of which applications the traffic traversing their network actually belong to. Therefore, the network infrastructure of the network operators gradually becomes large but dumb pipes. Accordingly the network operators are losing their opportunities of making revenue increase in the 5G era and beyond.

There are already some traditional ways to make the network aware of the applications it carries. However, they all have some drawbacks: 1) Five Tuples are widely used for the traffic matching with Access Control List (ACL)/Policy Based Routing (PBR), but still not enough information for supporting the fine-grained service process, and can only provide indirect application information which needs to be further translated in order to indicate a specific application; 2) Deep Packet Inspection (DPI) can be used to extract more application-specific information by deeply inspecting the packets, but more CAPEX and OPEX will be introduced as well as security challenges; 3) Orchestration and SDN-based Solution is used in the era of SDN, with the SDN controller being aware of the service requirements of the applications on the network through the interface with the orchestrator and the service requirement used by the controller for traffic management over the network, but the whole loop is long and time-consuming which is not suitable for fast service provisioning for critical applications.

We proposed Application-aware IPv6 Networking (APN6) framework[1][2][3], which is able to resolve the drawbacks and challenges of the above-mentioned traditional application awareness mechanisms. In this Demo, we demonstrated a showcase that includes all the key components in the APN6 framework and their capabilities. According to the application characteristics information carried in the IPv6/SRv6 packets, the application flows are steered into corresponding SRv6 TE tunnels. Utilizing the real-time network performance monitoring and measurement enabled by Intelligent Flow Information Telemetry (iFIT) [4] and further enhancing it to make it application-aware in this setup, we showed that the VIP application's flow can be automatically adjusted away from the path with degrading performance to the one that has good quality in order to guarantee its SLA requirements. Furthermore, we also demonstrated the flexible application-aware SFC within the framework of APN6.

II. Application-aware IPv6 Networking

IPv6/SRv6 has some programmable space in their encapsulations, i.e. the IPv6 extension headers such as Hop-by-hop Options Header (HBH), Destination Options Header (DOH) [5], and Segment Routing Header (SRH) [6] which is a new type of Routing Header (suggested value 4) currently being standardized in IETF. SRH itself also has some programmable space, e.g. the tag field, the argument field of each Segment ID (SID), and the SRH Type Length Value (TLV) [7]. These programmable space can be used to convey application characteristics information into the network and make the network aware of applications as well as their requirements. Accordingly, the network is able to steer the application flow into corresponding SRv6 TE tunnel or Policy to guarantee its SLA or set up a new one. This is the essential idea of APN6. The application characteristic information includes application-aware ID which identifies application, the user of application, and the SLA level, i.e. to indicate the packets as part of the traffic flow belonging to a specific Application/User/SLA level. It could also include network performance requirements information, specifying at least one of the following parameters: bandwidth, delay, loss ratio, etc.

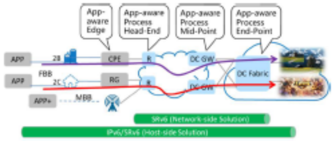


Fig. 1. Application-aware IPv6 Networking Framework and Scenarios

Now the VIP live video streaming is flowing along the path R2-R4-R5, which has deployed a VAS2: Log Audit at R4 against the VIP Application-aware ID 1. The video streaming flow will be audited accordingly. Therefore, we demonstrated the flexible application-aware SFC stitching application-aware VAS together with the network nodes/routers.

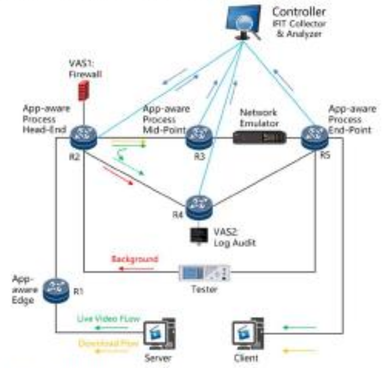


Fig. 2. The APN6 Demo Setup

Application-aware G-SRv6 network enabling 5G services

Cheng Li, Jianwei Mao, Shuping Peng, Yang Xia, Zhibo Hu, Zhenbin Li
Huawei Technologies, Beijing, China
{c.l, maojianwei, pengshuping, yolanda.xia, huzhibo, lizhenbin} @huawei.com

Abstract—**This demo showcased how application-aware G-SRv6 network provides fine-grained traffic steering with more economical IPv6 source routing encapsulation, effectively supporting 5G eMBB, mMTC and uRLLC services. G-SRv6, a new IPv6 source routing paradigm, introduces much less overhead than SRv6 and is fully compatible with SRv6. Up to 75 percent overhead of an SRv6 SID List can be reduced by using 32-bit compressed SID with G-SRv6, allowing most merchant chipsets to support up to 10 SIDs processing without introducing packet recirculation, significantly mitigating the challenges of SRv6 hardware processing overhead and facilitating large-scale SRv6 deployments. Furthermore, for the first time, by integrating with Application-aware IPv6 networking (APN6), the G-SRv6 network ingress node is able to steer a particular application flow into an appropriate G-SRv6 TE policy to guarantee its SLA requirements and save the transmission overhead in the meanwhile.**

Keywords—SRv6 Compression, G-SRv6, APN6

I. Introduction

As 5G and industry verticals evolve, ever-emerging new services with diverse but demanding requirements such as low latency and high reliability are accessing to the network. Different applications have differentiated network Service Level Agreement (SLA). For instance, on-line gaming has highly demanding requirements on latency, live video streaming has high requirements on both latency and bandwidth, while backup traffic mainly requires more bandwidth but is less sensitive of latency. However, in current networks, the operators remain unaware of the traffic type traversing their network, making the network infrastructure essentially dumb pipes and losing application performance optimization opportunities. To solve this issue, Application-aware IPv6 networking(APN6) [1] is proposed, which takes advantage of the programmable space in the IPv6/SRv6 packet encapsulations to convey application-aware information into the network layer, and makes network aware of applications and their requirements in order to provide fine-grained application-aware services.

SRv6 [2], as the underlying network protocol supporting APN6, enables the ingress node to explicitly program the forwarding path of packets by encapsulating/inserting ordered Segment ID (SID) list into the Segment Routing Header (SRH) at the ingress node, where each SID is 128-bit long. The SLA can be satisfied by steering the application packets into an explicit SRv6 programmable forwarding path. However, in some scenarios such as strict Traffic Engineering(TE), many SIDs will have to be inserted in the SRH, resulting in a lengthy SRH which imposes big challenges on the hardware processing, and affects the transmission efficiency especially for the small size packets in 5G uRLLC or mMTC scenarios. For instance, the size of an SRv6 encapsulation with 10 SIDs is 208 bytes, ... recirculation. This has become a big obstacle for SRv6 deployment in practice.

We proposed Generalized Segment Routing over IPv6 (G-SRv6) [3][4][5] to address the challenges of SRv6 overhead. While compatible with SRv6, G-SRv6 provides a mechanism to encode Generalized SIDs (G-SID) in the Generalized SRH (G-SRH), where a G-SID can be a 128-bit SRv6 SID, a 32-bit compressed SID (C-SID) or some other types. A 32-bit C-SID saves 75% overhead of the SID, so that the size of SRH can be significantly compressed. It also supports incremental upgrade from SRv6 by encoding both SRv6 SIDs and C-SIDs in the SRH. With G-SRv6, most the merchant chipsets can support up to 10 SIDs processing without packet recirculation so that the challenges of SRv6 hardware processing is mitigated, facilitating the large-scale SRv6 deployment. So far, G-SRv6 has been implemented in Linux Kernel, and hardware devices from more than 10 vendors.

This demo showcases that APN6 over G-SRv6 enables fine-grained traffic scheduling and efficient IPv6 source routing encapsulation for services in 5G scenarios, and what benefits G-SRv6 can provide over SRv6. Using APN6, the eMBB, mMTC, and uRLLC traffic is forwarded following the high-bandwidth path, the Service Function Chain (SFC) path, and the lowest latency path, respectively. Using APN6 over G-SRv6, over 50% transmission overhead is reduced, and the Flow-Completion Time (FCT) is shortened from 923s to 102s. Comparing to SRv6 (with 10 SIDs in SRH), the forwarding rate of an SRv6 endpoint node is raised by 55% from 400Mpps to 620Mpps. In summary, the application-aware G-SRv6 helps network operators to reduce the cost and generate more revenue in the 5G area.

II. Application-aware G-SRv6

Normally, SRv6 SIDs are allocated from an address block within an SRv6 domain, so the SIDs share the common prefix (CP) of the address block[5]. An SRv6 SID has the format shown in Fig. 1.

Fig. 1. Format of the128-bit SRv6 SID and 32-bit G-SID

In most cases, only Node ID and Function ID are different among the SIDs in a SID list, while the common prefix and argument parts are redundant. Removing the redundant parts of the SID list can reduce the overhead. Generalized SRv6 (G-SRv6) realizes this idea. It only carries the compressed SID consisting of node ID and Function ID in the SRH, so that the size of the SRH is compressed. Theoretically, up to 75% ...

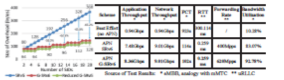


Fig. 2. Comparison between SRv6 and G-SRv6

In order to locate the 32-bit C-SID within the 128-bit space located by Segment Left (SL) in SRH, Segment Index (SI) is defined, and it is the least 2 bits in the argument of the active SID in the IPv6 destination address (DA) field. Furthermore, a Continuation of Compression (COC) flavor is defined [5] to instruct the Segment Endpoint Node to continue to process the 32-bit C-SID in the SRH. When an SRv6 endpoint node receives a SID with COC Flavor, it updates the 32-bit G-SID in the IPv6 DA with the next 32-bit G-SID, and the next G-SID is located at SRH[SL][SI]. Otherwise, the node performs normal SRv6 processing[5]. In application-aware G-SRv6 networks, APN6 ID is added into the IPv6 Hop-by-Hop (HBH) header by application clients and servers to convey the application information to the network layer, so that the network nodes can be aware of the application type of a user group and its requirements. When APN6 packets with APN6 ID are received at the G-SRv6 ingress node, the node steers the packets into corresponding G-SRv6 tunnel based on the APN6 ID and associated policies.

III. Demonstration

We have implemented APN6 function in Linux kernel to support adding APN6 ID to packets. Next, we enhanced Nginx ...

102s, 53.33% transmission overhead is reduced, and bandwidth utilization is increased from 83.07% to 92.79%.

2) mMTC, IoT metadata transmission (Payload size: 128 Bytes) over a 10-hop path: Without APN6, the traffic is forwarded following the shortest path. Using APN6 over SRv6/G-SRv6, the traffic is forwarded over the Service Function Chain (SFC) path with a firewall deployed in MEC for security checking. Comparing to SRv6, the SID list (10 SIDs) is compressed from 160 bytes to 64 bytes in G-SRv6. In this situation, the forwarding rate of an SRv6 endpoint node is raised by 55% from 400Mpps to 620Mpps in G-SRv6 due to no packet recirculation.

3) uRLLC, real-time message exchanging traffic (Payload size:128 Bytes) over the 9-hop shortest path: Using APN6, the traffic is forwarded through the lowest latency path, and the latency is shortened from 300.114ms to 0.259ms comparing to another path. Comparing to SRv6, 45.45% transmission overhead is reduced in G-SRv6, and bandwidth utilization is increased from 42.11% to 57.14%.

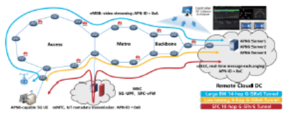


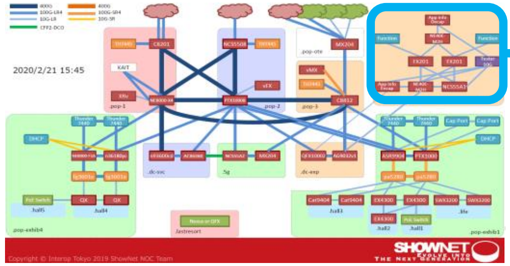
Fig. 3. Application-aware G-SRv6 demo setup

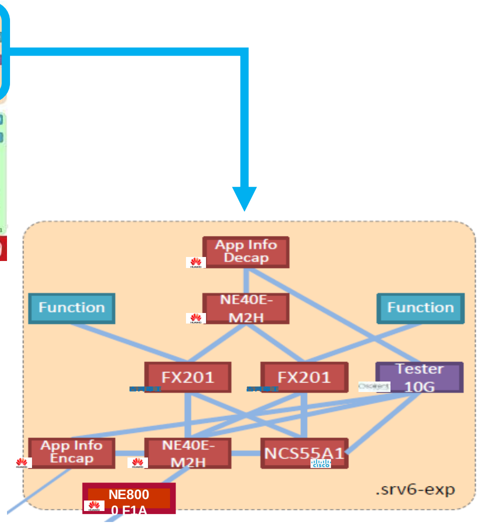
https://ieeexplore.ieee.org/abstract/document/9162934, https://www.youtube.com/watch?v=ONqwxKVmPp0

HUAWEI

APN6@Interop Tokyo2020

HUAWEI | CISCO | spirent | NTT Communications | 古河電工 | 東京大学 THE UNIVERSITY OF TOKYO





Interop 20 Tokyo

SHOWNET EVOLVE INTO THE NEXT GENERATION

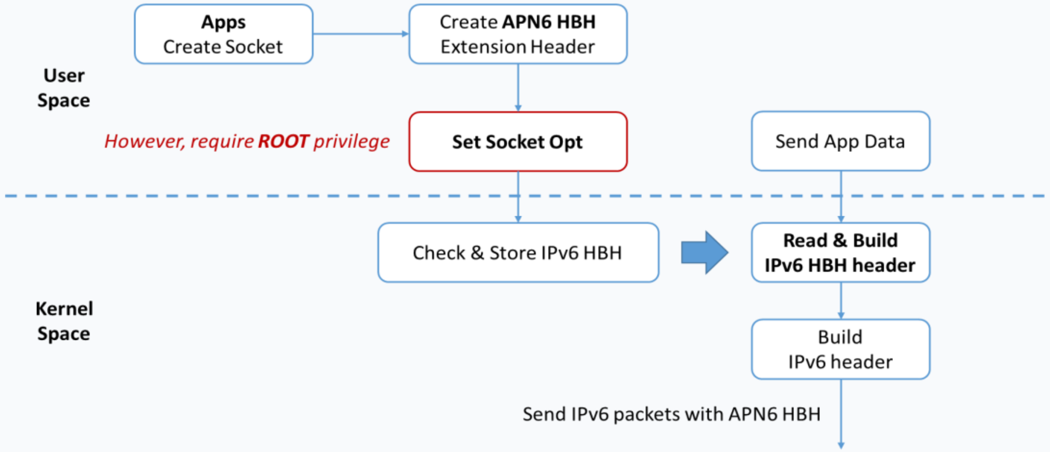
- **2019.7** — IETF 105 Montreal, *20 Jul 2019 - 26 Jul 2019* — **APN6 Side Meeting**
- **2019.11** — HUAWEI, CISCO, NTT Communications, TOYOTA, 東京大学 THE UNIVERSITY OF TOKYO — IETF 106 Singapore, *16 Nov 2019 - 22 Nov 2019* — **F2F meeting with Shownet NOC team**
- **2019.12** — HUAWEI, CISCO, 古河電工, spirent, NTT Communications, 東京大学 THE UNIVERSITY OF TOKYO — **APN POC Collaboration**
- **2020.1** — SHOWNET EVOLVE INTO THE NEXT GENERATION — **APN Shownet Setup Plan**
- **2020.2** — SHOWNET EVOLVE INTO THE NEXT GENERATION — **APN6 in Shownet Topology**
- **2020.4** — **Interop 2020** — Finalist

Interop to Cloud – APN6 Shownet

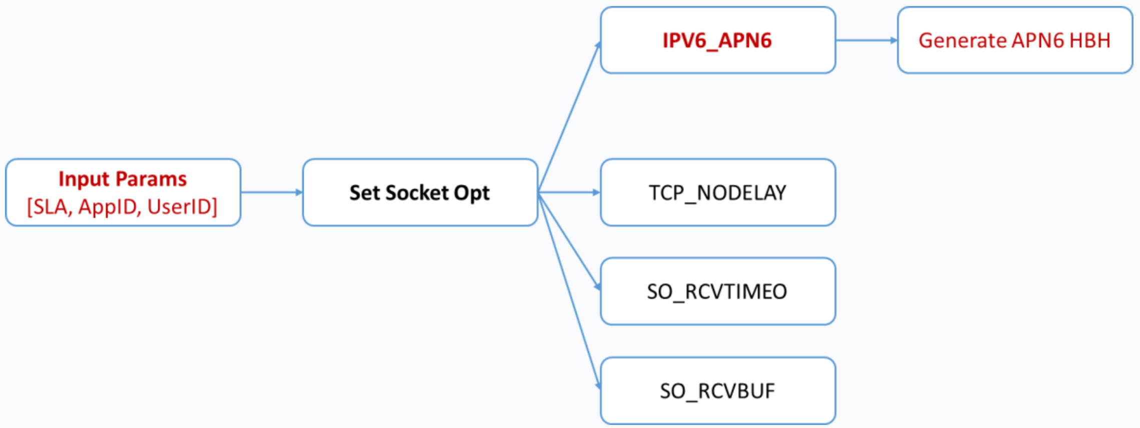
HUAWEI

Exploring APN Application-side Solution: Open Source Implementation with Linux

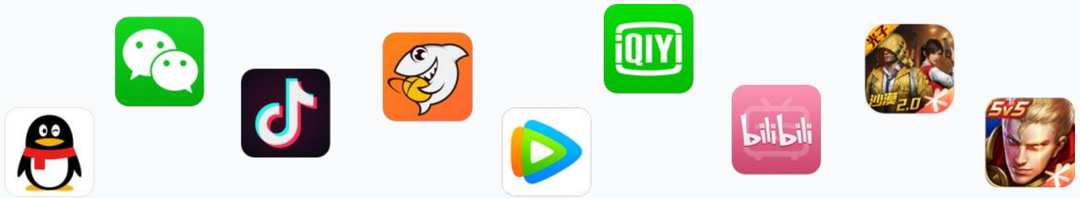
① Latest kernel supports to bind an arbitrary HBH extension header with a socket, but that **requires the ROOT privilege**. That is unacceptable.



② So, we need to **extend the socket API**, to allow Apps passing in APN attributes, and to generate HBH extension header securely in the kernel.



③ Then, Apps need to be upgraded to take advantage of the extended API, **binding the socket with APN attributes.**



Demo_TCP_Client.c

```
unsigned int apn6_id[] = {0x20150810, 0xAABBCCDD, 0x00522703};
int ret = setsockopt(connectSocket, IPPROTO_IPV6, IPV6_APN6, apn6_id, sizeof(unsigned int)*3);
```

④ **Demo:** with TCP Echo application, the packets of sent messages carry the specified HBH extension header **with APN attributes** successfully.

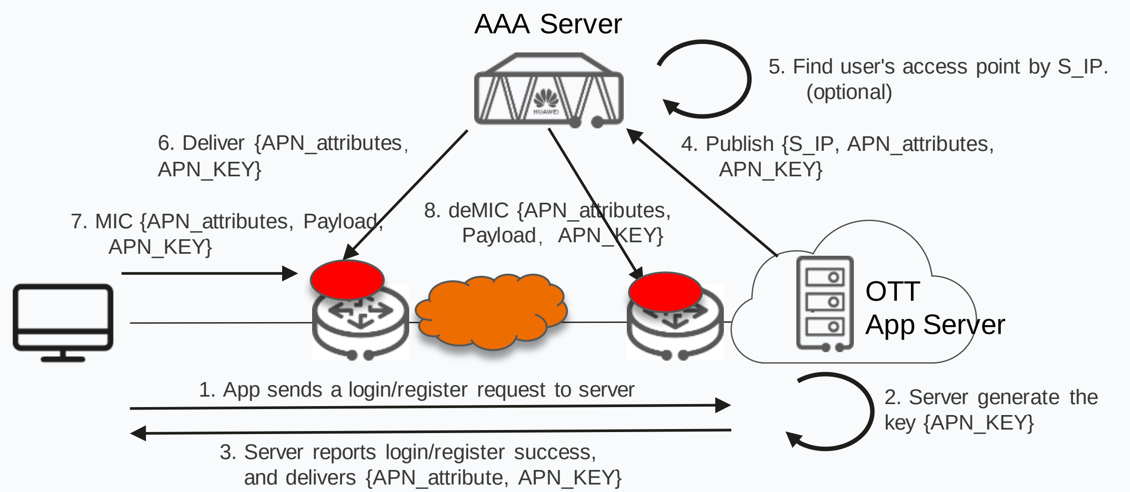
```
0000  e2 4c 96 0e b1 94 fe 7a  f5 48 09 16 86 dd 60 05   ·L·····z ·H····`·
0010  b5 df 00 63 00 40 20 01  0d a8 02 15 00 0a 00 00   ···c·@ · ········
0020  00 00 00 00 aa aa 20 01  0d a8 02 15 00 0a 00 00   ······ · ········
0030  00 00 00 00 bb bb 06 01  03 0c aa aa 08 10 00 00   ······ ·· ········
0040  aa aa 00 52 27 03 e0 68  15 87 07 ea 1d 62 6d b9   ···R'··h ·····bm·
0050  79 6e 80 18 01 fb c6 4f  00 00 01 01 08 0a 85 27   yn·····O ·······'
0060  28 ac 15 b4 b4 07 2e 2e  2e 2e 2e 2e 2e 2e 2e 2e   (······.. ........
0070  63 6f 6e 74 61 63 74 20  42 65 69 6a 69 6e 67 20   contact  Beijing
0080  54 6f 77 65 72 20 6f 6e  20 31 31 38 2e 35 2c 20   Tower on  118.5,
0090  67 6f 6f 64 20 64 61 79  21                        good day !
```

Exploring APN Application-side Solution: Potential Security Solutions

Objective: Securely deliver and transport APN attributes to defend against attacks such as falsification, resource stolen, and DDoS attacks.

Solution A:

Control plane delivers the cryptographic key. Data plane encrypts the APN attributes.

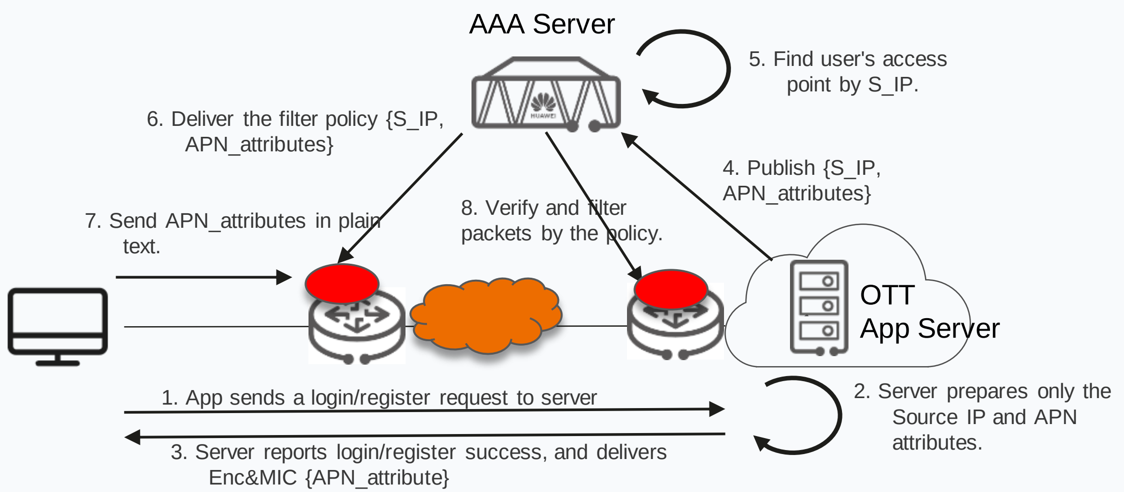


App Servers are responsible for update and management of cryptographic key, and secure delivery of APN attributes and the key.
Access devices in the network decrypt and verify the APN attributes.

Advantage:
A) Clear security boundaries. B) Reliable cryptographic mechanisms
Challenge:
A) Management of massive keys. B) Performance pressure from cryptographic algorithms.

Solution B:

Control plane delivers the filter policies. Data plane sends APN attributes in plain text.



App Servers are only responsible for secure delivery of APN attributes.
Access devices in the network deploy filter policy for security.

Advantage:
A simple and high-efficient method to maintain access security.
Challenge:
A) Management of increasing policies
B) Rely on the location of user's access point, which means relying on the network topology.

Protect high-quality resources. Protect subscribers' charging. Enhance stability and trust of the network.

Agenda

- IPv6 Enhanced
- APN: Application-aware Networking
- CAN: Computing-aware Networking
- Summary

Computing and Network Joint Optimization

Network Requirements

- Multi & heterogeneous access
- Edge-cloud synergy, Cross-domain Edge-cloud synergy
- Inter-network interconnection and interoperation
- Reliable connectivity, No detour
- Deterministic & low latency, High bandwidth and concurrency
- Security & Trust

Computing Requirements

- Quick service discovery and combination
- Experience assurance in High-concurrency scenario
- On-demand scheduling of computing resource
- Improves resource utilization and reduces resource waste.

Computing & Network Joint Optimization

- Requirements and Resources fast mapping
- Communication SLA assurance
- Efficient resource collaboration
- Cloud edge computing fabric

Typical Application - AR/VR in MEC: Traffic Steering based on Comprehensive Network and Service Metrics

Upper bound latency for motion-to-photon(MTP): includes frame rendering and requires less than **20 ms** to **avoid motion sickness,** consisted of**:**

1. sensor sampling delay: <1.5ms (client)
2. display refresh delay: ≈7.9 ms(client)
3. frame rendering computing delay with **GPU≈ 5.5ms** (server)
4. network delay(budget) =20-1.5-7.9-5.5 = **5.1ms**(network)

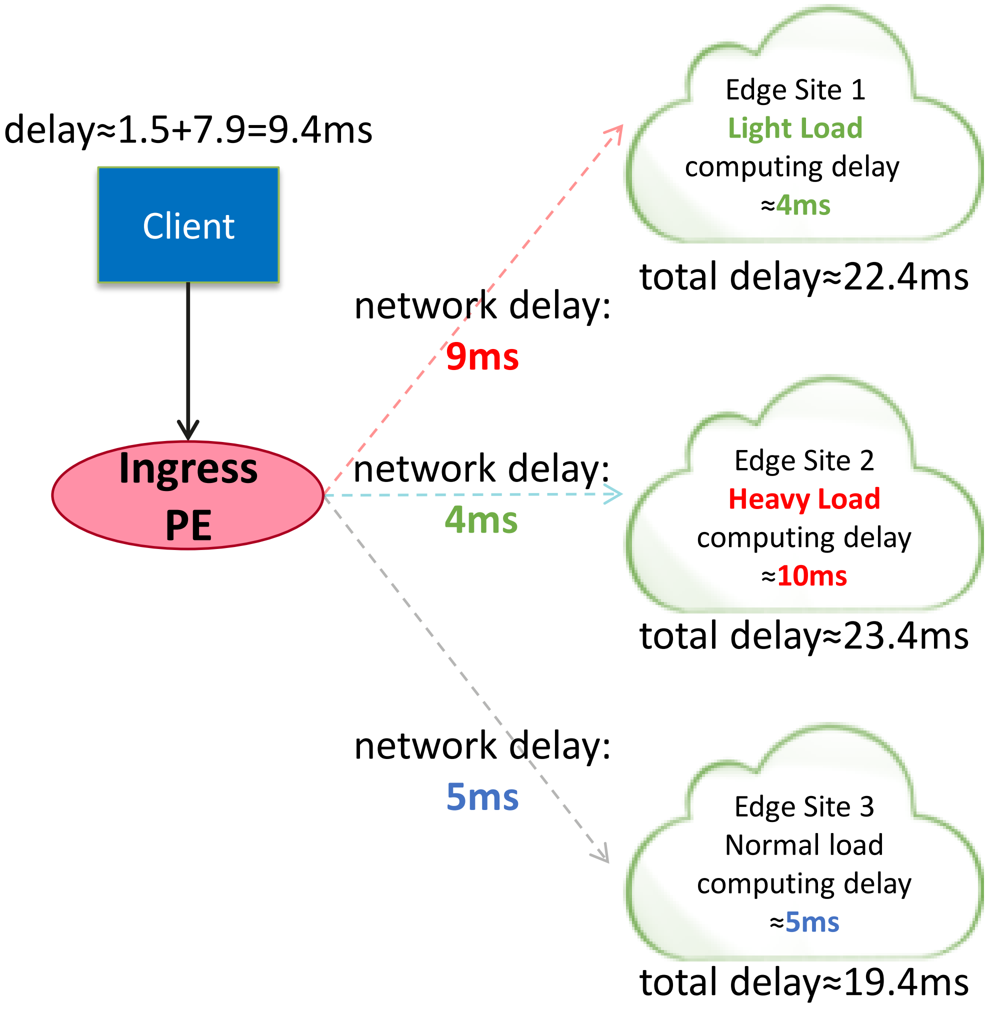
Budgets for computing delay and network delay are almost equivalent!!

\+

- choose edge site 1 according to load only, total delay≈22.4ms
- choose edge site 2 according to network only, total delay≈23.4ms
- choose edge site 3 according to both, **total delay≈19.4ms**

It can't meet the total delay requirements or find the best choice by either optimize the network or computing resource:

Require to dynamically steer traffic to the appropriate edge to meet the E2E delay requirements considering both network and computing delay



PS: Computing resources have a big difference in different edges, and the 'closest site' may be good for latency but lacks GPU support and should therefore not be chosen.

Distributed mode: Dyncast for Computing-aware Routing

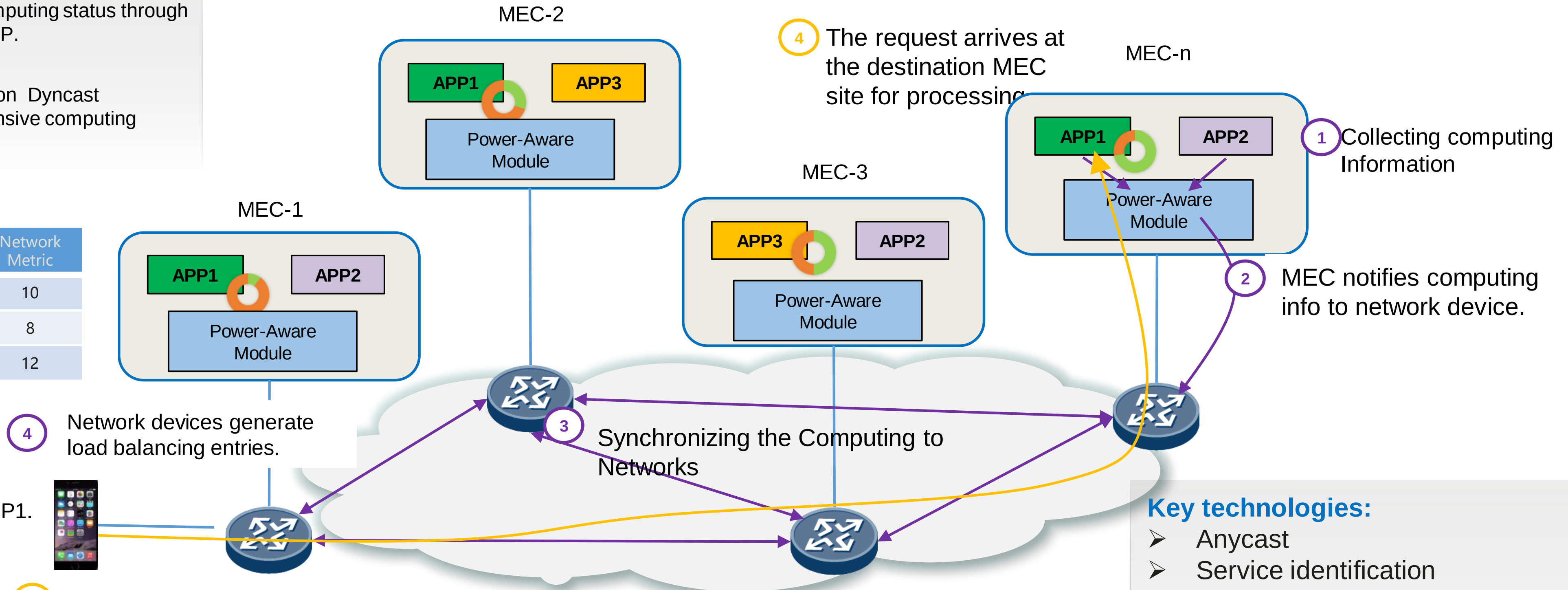
Dyncast（Dynamic Anycast） is a key technology of Computing aware routing. It inherits the advantages of anycast in **fast**, **reliable**, and **anti-DDoS**.

- Distributed computing is the endogenous resource in the computing aware network. Dyncast is used to connect the distributed computing to the network to provide optimal computing allocation and network connection for customers, achieving **high reliability of edge computing and optimal overall system utilization efficiency**.

Control plane: distributes computing status through network protocols, such as BGP.

Data plane: forwards based on Dyncast service identifiers, comprehensive computing status, and network status.

IP Prefix	Nexthop	Computing Metric	Network Metric
APP1 Anycast IP	MEC-1	60	10
	MEC-2	20	8
	MEC-n	10	12



2 Network devices select routes based on the computing information and network status of applications at each site.

3 The network device adds an entry to the session table to persist the session

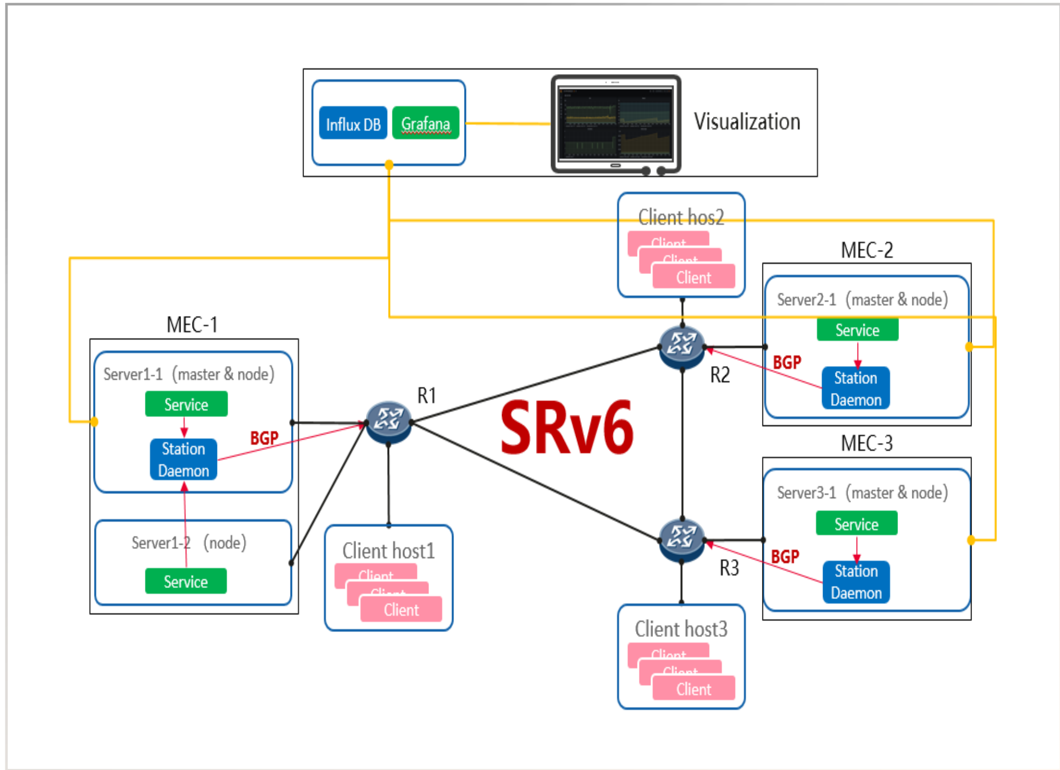
Key technologies:

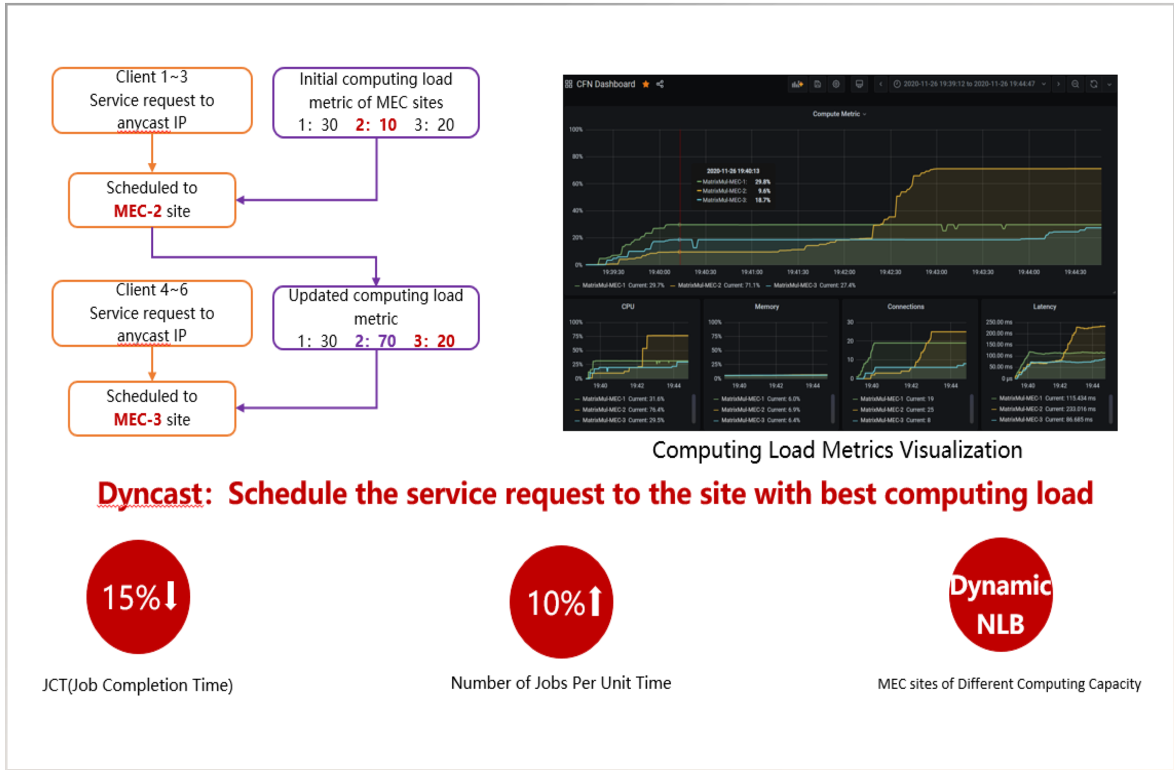
- Anycast
- Service identification
- Computing metric measurement
- Computing awareness
- scheduling algorithm
- Session persistence

HUAWEI

Computing-aware Routing (Dyncast) Demo

Computing-aware routing (Dyncast) demo based on physical D-Router in Chinese ECIS2020 (Edge Computing Industrial Summit), Partner: China Mobile

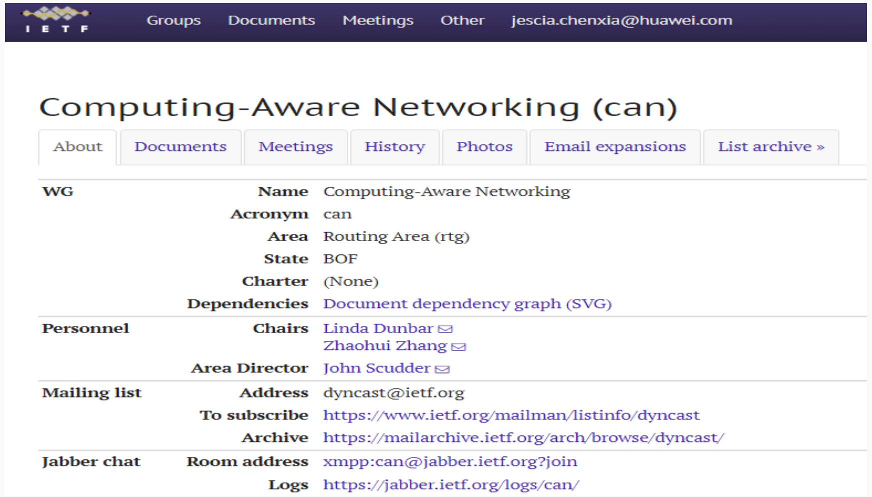




Standard Progress in IETF: CAN BOF of IETF 113

Meeting

- **Dyncast Side Meeting @IETF109 & @IETF110**
  - https://github.com/dyncast/ietf109
  - https://github.com/dyncast/ietf110
- **CAN BOF @IETF113**
  - https://datatracker.ietf.org/group/can/about/


Groups Documents Meetings Other jescia.chenxia@huawei.com

Computing-Aware Networking (can)

About | Documents | Meetings | History | Photos | Email expansions | List archive »

WG	Name	Computing-Aware Networking
	Acronym	can
	Area	Routing Area (rtg)
	State	BOF
	Charter	(None)
	Dependencies	Document dependency graph (SVG)
Personnel	Chairs	Linda Dunbar Zhaohui Zhang
	Area Director	John Scudder
Mailing list	Address	dyncast@ietf.org
	To subscribe	https://www.ietf.org/mailman/listinfo/dyncast
	Archive	https://mailarchive.ietf.org/arch/browse/dyncast/
Jabber chat	Room address	xmpp:can@jabber.ietf.org?join
	Logs	https://jabber.ietf.org/logs/can/

Draft

Draft topic	Draft name
Dynamic-Anycast (Dyncast) Use Cases & Problem Statement	draft-liu-dyncast-ps-usecases
Dynamic-Anycast (Dyncast) Requirements	draft-liu-dyncast-reqs
Dynamic-Anycast Architecture	draft-li-dyncast-architecture
Providing Instance Affinity in Dyncast	draft-bormann-dyncast-affinity
LISP Support for Dynamic Anycast Routing	draft-kjsun-lisp-dyncast
BGP NLRI App Meta Data for 5G Edge Computing Service	draft-dunbar-idr-5g-edge-compute-app-meta-data
Computing-aware Networking Use case of ALTO	draft-liu-alto-can-usecase
Use Cases for Computing-aware Software-Defined Wide Area Network(SD-WAN)	draft-zhang-dyncast-computing-aware-sdwan-usecase

Agenda

- IPv6 Enhanced
- APN: Application-aware Networking
- CAN: Computing-aware Networking
- Summary

Whole Picture of IPv6 Enhanced Phases and APxN Systems (APTN/APIN/APCN)

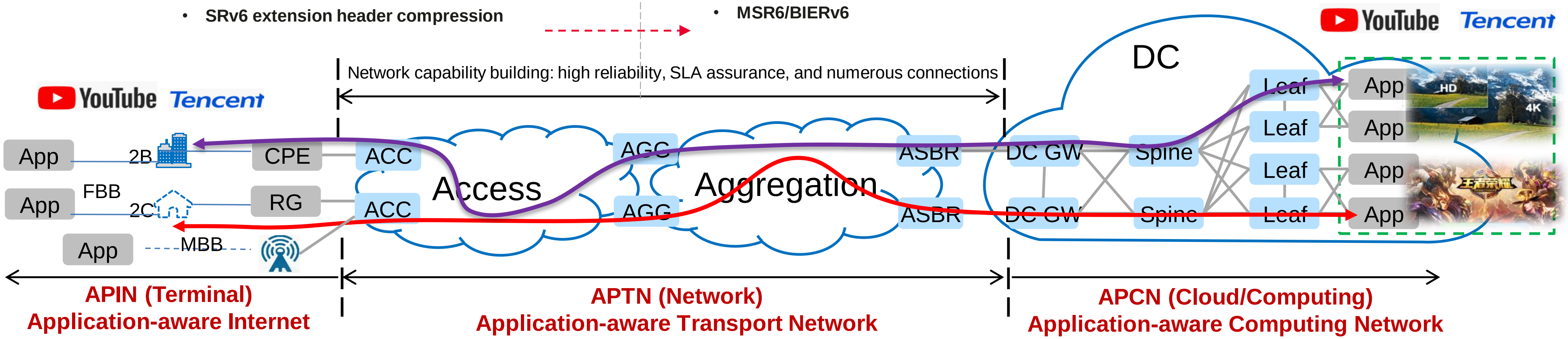
IPv6 Enhanced has essentially completed network-side capability construction, and is now expanding to the terminal side to enable application-aware networks.

IPv6 Enhanced 1.0 (Network Programming)

- SRv6 BE
- SRv6 TE/Policy
- SRv6 VPN/EVPN
- SRv6 TI-LFA (local protection switching within 50 ms)
- SRv6 extension header compression

IPv6 Enhanced 2.0 (Experience assurance)

- IPv6-based IFIT
- IPv6-based Network Slicing (plus resource planning algorithm)
- IPv6-based Deterministic Network
- IPv6-based SFC and SDWAN
- MSR6/BIERv6



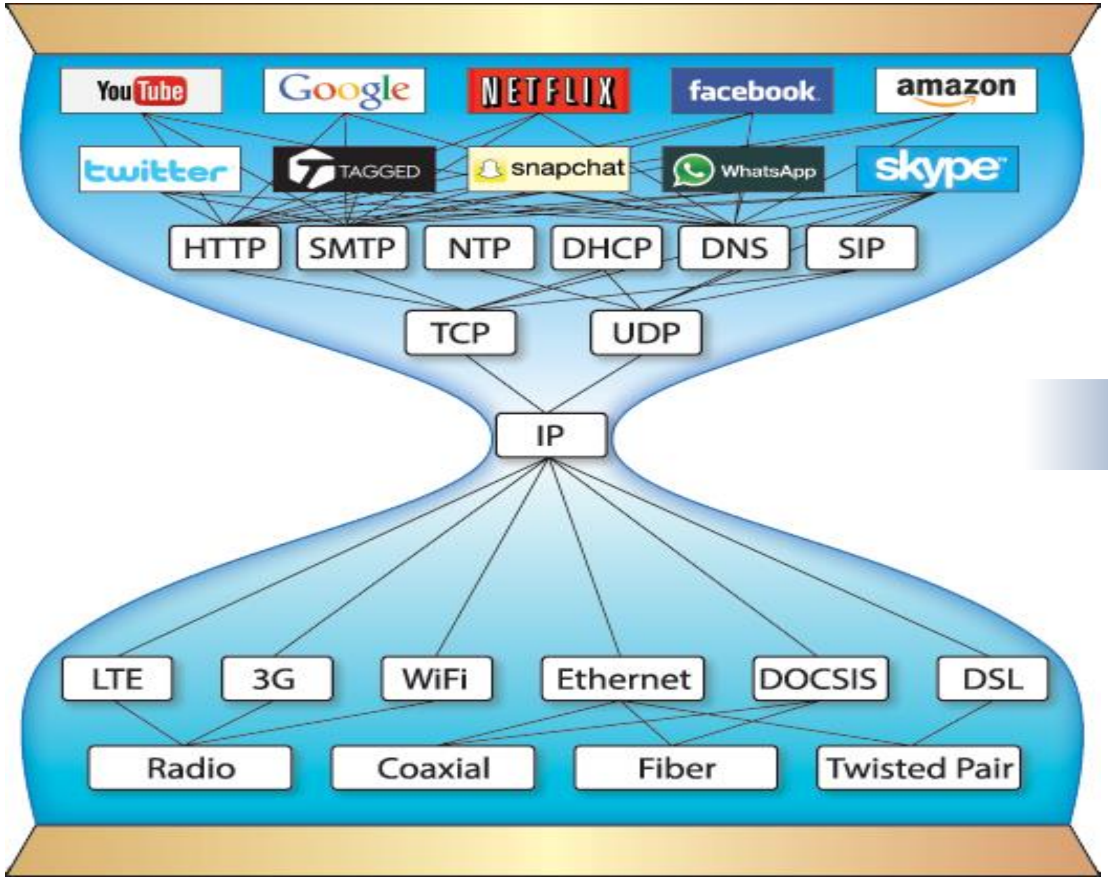
IPv6 Enhanced 3.0 (application-aware networking)

- **APIN: (Terminal)**
  - APN+IFIT (terminal)
  - APN security (2C)
  - Application-level multicast
- **APTN: (Network side)**
  - APN+IFIT/Network Slicing
  - APN-based QoE
  - APN security (2B)
- **APCN: (Cloud/Computing)**
  - Computing power modeling
  - Computing power scheduling
  - Computing power + Network scheduling

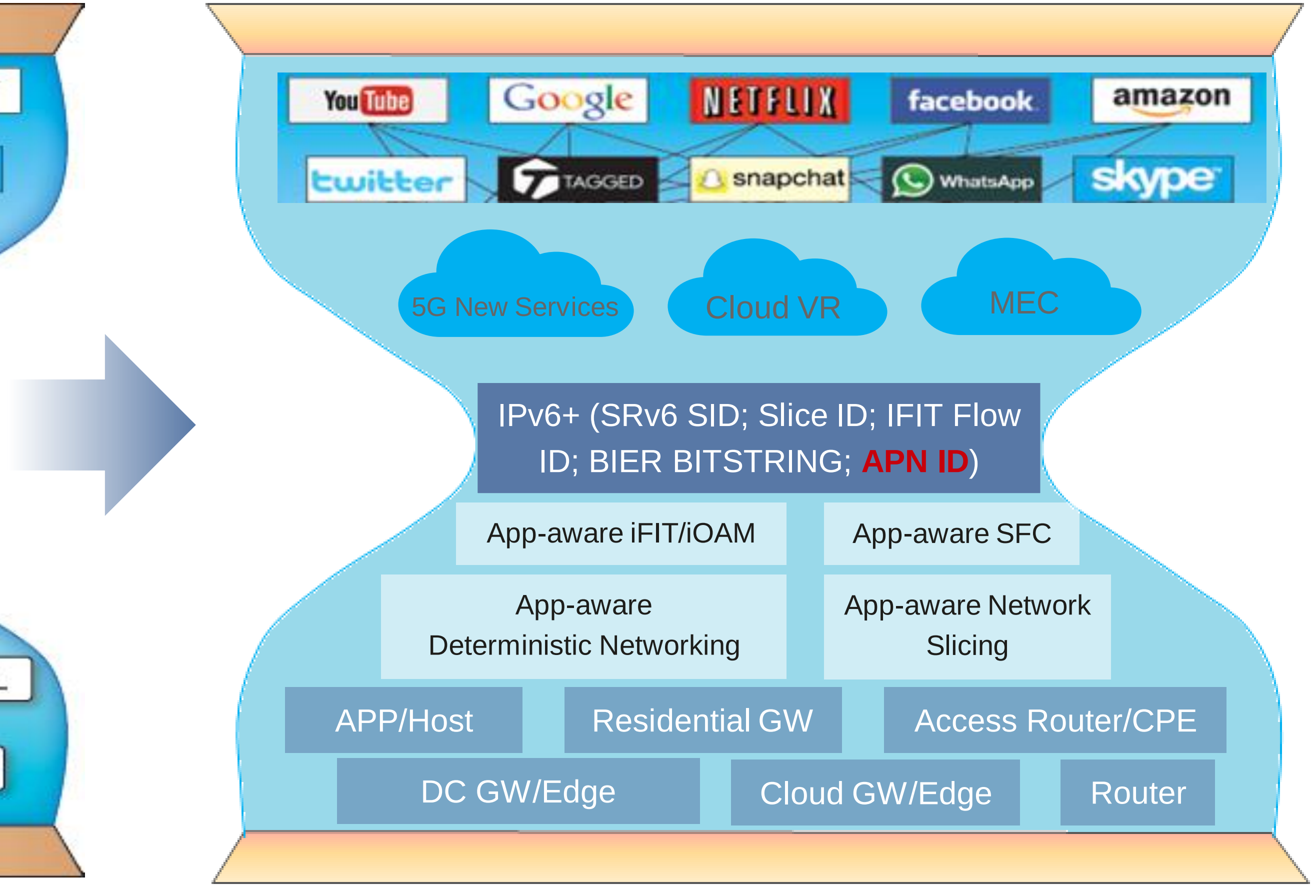
Defines the service layer beyond the underlay and overlay to implement application-level visualization, optimization, and assurance.

HUAWEI

Change of TCP/IP "Thin Waist" Model and IPv6-based 3.5 Layer Innovation



Internet-Oriented
TCP/IP "Thin Waist" Model



Limited-Domain-Oriented
IPv6-based "Fat Waist" Model

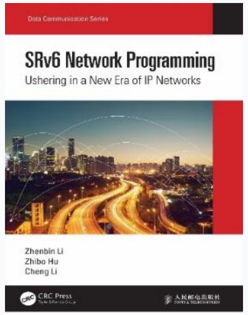
Summary of Usage of IPv6 Extension Headers

Functionalities	RFC/Drafts	IPv6 Extension Header		
		HBH Header	Routing Header	DO Header
SRv6	RFC8754		√	
VPN+ (Network Slicing)	1. draft-ietf-spring-resource-aware-segments 2. draft-ietf-6man-enhanced-vpn-vtn-id	√	√	
IFIT (In-situ Flow Telemetry)	1. draft-ietf-6man-ipv6-alt-mark 2. draft-ietf-ippm-ioam-data 3. draft-ietf-ippm-ioam-ipv6-options	√	√	√
MSR6/BIERv6	1. draft-lx-msr6-rgb-segment 2. draft-geng-msr6-traffic-engineering		√	√
APN6	1. draft-li-apn-header 2. draft-li-apn-ipv6-encap	√	√	√

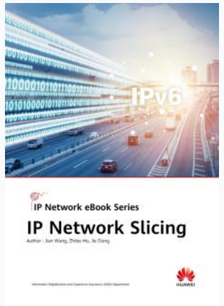
HUAWEI

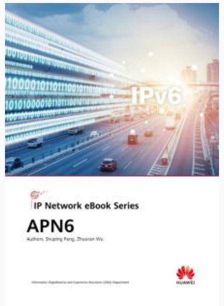
IPv6 Enhanced Series Books and Videos

IPv6 Enhanced Books



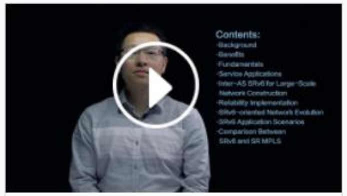
IPv6 Enhanced Series Books





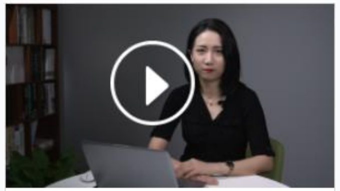
IPv6 Enhanced Series Videos

(Video) IP New Technology Series (Advanced) - Deep Dive into EVPN L3VPNv4 over SRv6 TE Policy



(Video) IP New Technology Series (Advanced) - Segment Routing IPv6 (SRv6)

(Video) IP New Technology Series (Advanced) - Segment Routing MPLS (SR-MPLS)



(Video) IP New Technology Series (Advanced) - Deep Dive into Ping & Tracert for SRv6

IPv6 Enhanced Series Books and Videos

IPv6 Enhanced Books

https://www.amazon.com/SRv6-Network-Programming-Ushering-Communication/dp/1032016248

IPv6 Enhanced Series eBooks

IPE Series eBook

Scan to obtain the electronic version

https://e.huawei.com/en/material/bookshelf/bookshelfview/202109/29105716

IPv6 Enhanced Series Videos

https://support.huawei.com/enterprise/en/routers/netengine-8000-pid-252772223/multimedia

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home and organization for a fully connected, intelligent world.

HUAWEI