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, and also too many interfaces are involved in the loop, which introduce challenges of standardization and inter-operability.

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 (i.e. Application-aware ID) 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.

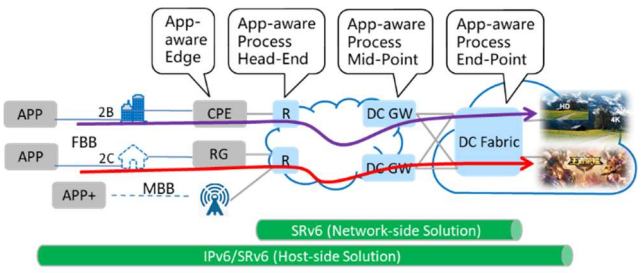

Fig. 1. Application-aware IPv6 Networking Framework and Scenarios

The APN6 framework is shown in Fig. 1, which includes the following key components,

1. APP+: This is an enhanced APP, which is able to encapsulate the application characteristics information into the IPv6 extension headers such as HBH, DOH, and SRH.
2. App-aware Edge: If the application characteristics information is not encapsulated by the APP, this network edge device can obtain such information by packet inspection, Artificial Intelligence (AI), deriving from double VLAN tagging or local policies.
3. App-aware Process Head-End: This headend device maintains the matching relationship between the application characteristic information and the paths between the Head-End and End-Point, and forwards the packets according to the matching relationship into the corresponding path (TE tunnel or Policy).
4. App-aware Process Mid-Point: This device can provide path service according to the application characteristic information, and could also adjust the resource locally to guarantee the service requirements depending on a specific policy.
5. App-aware Process End-Point: The application characteristic information can be removed at the End-Point together with the outer IPv6 encapsulation or go on to be conveyed with the IPv6 packets.

III. DEMONSTARTION

The APN6 Demo setup is shown in Fig. 2. In this Demo, we demonstrated the APN6 framework as well as its key components as shown in Fig. 1 and described in Section II. The key capabilities of the network-side components are shown, that is, the application characteristics information is not encapsulated by the APP but by the App-aware Edge.

As shown in Fig. 2, two applications (VLC and FTP) installed in the Server are injecting IPv6 traffic into the setup, emulating live video flow (in green) and download flow (in yellow). Meanwhile, a tester is injecting background flow (in red). The packets generated from these two applications are differentiated by UDP ports. They are identified by the App-aware Edge device R1, marked with different Application-aware IDs (VLC traffic: Application-aware ID 1 and FTP traffic: Application-aware ID 2) which are encapsulated into the IPv6 HBH Options Header, respectively. The IPv6 packets carrying the Application-aware ID arrive at the App-aware Process Head-End. According to the carried information in the HBH Options Header, the application flows are steered into corresponding SRv6 TE tunnels, i.e. R2-R3-R5 since this path can guarantee their SLA requirements. The background flow is injecting into another path R2-R4-R5.

Before moving further, the packets needs to first go through a VAS, i.e. VAS 1: Firewall as shown in Fig. 2 to examine the legitimacy of the packets of a specific application identified by the Application-aware ID 2, i.e. FTP for downloading. If the examination is passed, the packets will be forwarded along the assigned path.

The real-time network performance monitoring and measurement enabled by iFIT is utilized, which is further enhanced in this setup to make it aware of the VIP application, i.e. VLC for live video streaming. Once the Controller, which is also the iFIT Collector and Analyzer, detects the performance of the VIP application degrading below the pre-configured threshold triggered by adjusting the Network Emulator deployed between R3 and R5, it will send an alarm to the network operator to indicate this performance degrading. Once the network operator initiated the path optimization, the Controller will enforce a new SRv6 policy to the App-aware Process Head-End, and the VIP application's flow will be automatically adjusted away from the path with degrading performance to the one that has good quality, i.e. R2-R4-R5.

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.

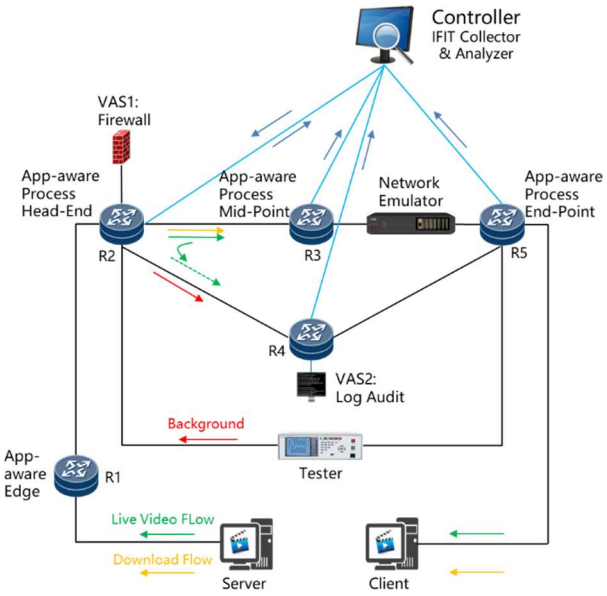

Fig. 2. The APN6 Demo Setup

ACKNOWLEDGMENT

The authors would like to acknowledge the Interop Tokyo Shownet team: Ryo Nakamura, Yukito Ueno, Teppei Kamata, Tatsuya Fujiwara; Kentaro Ebisawa (Toyota), and Fengyu Zhang (Topsec Technologies) for their valuable comments and suggestions on this APN6 Demonstration.

REFERENCES

[1] Zhenbin Li, Shuping Peng, Daniel Voyer, Chongfeng Xie, Liang Geng, Chang Cao, Kentaro Ebisawa, Stefano Previdi, James Guichard, et al, "Application-aware IPv6 Networking (APN6) Framework", IETF, Nov. 2019.

[2] Z. Li, S. Peng, D. Voyer, C. Xie, P. Liu, Z. Qin, K. Ebisawa, S. Previdi, J. Guichard, et al, "Problem Statement and Use Cases of Application-aware IPv6 Networking (APN6)", IETF, Nov. 2019.

[3] https://github.com/APN-Github

[4] Bo Lu, Ling Xu, Yuezhong Song, Longfei Dai, Min Liu, Tianran Zhou, Zhenbin Li, Haoyu Song, "iFIT: Intelligent Flow Information Telemetry", ACM SIGCOM, Demos, pp. 15–17, Aug. 2019

[5] S. Deering, R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", IETF RFC 8200, July 2017.

[6] C. Filsfils, D. Dukes, S. Previdi, J. Leddy, S. Matsushima, D. Voyer, "IPv6 Segment Routing Header (SRH)", IETF 6man WG, Oct. 2019.

[7] C. Filsfils, P. Camarillo, J. Leddy, D. Voyer, S. Matsushima, Z. Li, "SRv6 Network Programming", IETF SPRING WG, Jan. 2020.