Application-aware Networking (APN)

Shuping Peng/Zhenbin Li

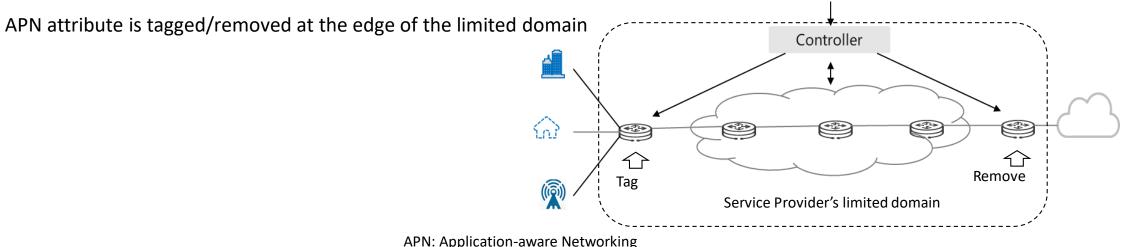
1

Purpose of presenting in this WG

- We would like to introduce the concepts, clarify the scope, attract people to understand and discuss the topic, and collect feedback and suggestions on this work, to further address the main concerns that were raised by the IESG.
- APN is mainly relevant to RTG since our idea is to enable packets to be routed through different network links depending on the user (group) and/or application (group) needs.
- We have presented in the RTGWG a couple of times before and involved the RTGWG in some of the APN mailing list discussions (<u>https://datatracker.ietf.org/wg/apn/about/</u>). Progress has been made.
- We would like to introduce the latest understandings and have your feedbacks after this presentation.

What is APN (Application-aware Networking)?

- APN is focused on developing a framework and set of mechanisms to derive, convey and use an attribute information to allow for the implementation of fine-grain user (group)-, application (group)-, and service-level requirements at the network layer.
- Such information is acquired, constructed, and encapsulated in the packets.
- Such information is treated as an object in the network
 - To it, the network operator applies policies in various nodes/service functions along the path and provides corresponding services.
- APN works within a limited trusted domain.
 - Typically, an APN domain is defined as a service provider's limited domain in which MPLS, VXLAN, SR/SRv6 and other tunnel technologies are adopted to provide services.

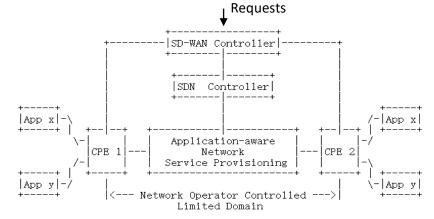


What APN is Not

- APN is not about identifying the application to or within the network
 - The network does not need to know which applications are sending traffic
 - Telling the network which applications are running would break privacy
- So, APN is about telling the network what policies to apply to traffic
 - An application can apply multiple policies to different traffic flows
 - Multiple applications can ask for the same policies
- APN is not PANRG/SPUD/PLUS/Network Tokens
- Conveying the information via the transport/application layer and the network layer are different technologies. APN uses the network layer. – APN Side Meeting @IETF108

Why APN? - The SD-WAN use case

- In the case of SD-WAN, network operators can provide SLA-guaranteed WAN lines to help enterprises to access the clouds.
- When mapping the WAN line into the operator's network, there are usually multiple network paths with different SLA guarantees available between the two endpoints of the tunnel connecting the CPE nodes.
- In MEF70, a list of Match items are specified at the CPE nodes to steer the traffic into corresponding WAN lines across the network operator's network according to users'/applications' requirements.
 - E.g, 5-tuples (i.e. Source/Destination Address, Source/Destination Port, Protocol)
- There is a need to communicate user/application requirements to match to the capabilities of the WAN lines different from MEF70
- Once the traffic goes into the operator's network, there is a need to apply various policies in different nodes along the network path onto the traffic flow, e.g.,
 - at the headend to steer into corresponding path satisfying SLAs
 - at the midpoint to collect corresponding performance measurement data
 - at the service function to execute particular policies



MEF70

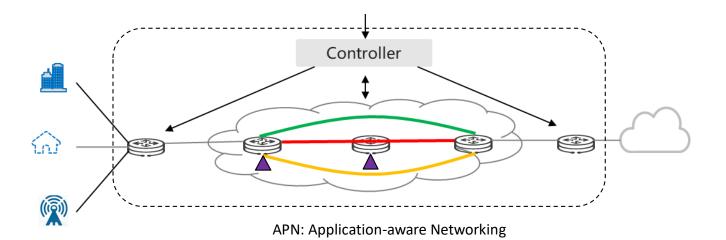
SD-WAN Service Attributes and Services

ACName	Layer	Match	Values for ACValue	Reference
ETHERTYPE	2	Ethertype	Integer in the range 0x0600 to 0xffff, e.g. 0x0800 for IPv4	802.3 [4]
CVLANS	2	C-VLAN ID List	Integer in the range 0 to 4094	802.1Q[3]
SAV4	3	IPv4 Source Address	IPv4 prefix	RFC 791 [5]
DAV4	3	IPv4 Destination Address	IPv4 prefix	RFC 791 [5]
SDAV4	3	IPv4 Source or Destination Ad- dress	IPv4 prefix	RFC 791 [5]
PROTV4	3	IPv4 Protocol List	List of integers in the range 0 to 255	IANA Proto- col Numbers Registry [1]
SAV6	3	IPv6 Source Address	IPv6 prefix	RFC 8200 [17]
DAV6	3	IPv6 Destination Address	IPv6 prefix	RFC 8200 [17]
SDAV6	3	IPv6 Source or Destination Ad- dress	IPv6 prefix	RFC 8200 [17]
NEXT- HEADV6	3	IPv6 Next Header List	List of integers in the range 0 to 255	IANA Proto- col Numbers Registry [1]
SPORT	4	TCP/UDP Source Port List	List of integers in the range 0 to 65535	IANA Service Name and Port Number Reg- istry [2]
DPORT	4	TCP/UDP Destination Port List	List of integers in the range 0 to 65535	IANA Service Name and Port Number Reg- istry [2]
SDPORT	4	TCP/UDP Source or Destination Port List	List of integers in the range 0 to 65535	IANA Service Name and Port Number Reg- istry [2]
APPID	4 - 7	Application Identifier	List of arguments starting with the Application Identifier.	Custom Match
ANY	1-7	Match Any IP Packet	No arguments	

Table 4 - Required Application Flow Criteria

Why APN? - The issues

- There is currently no way to request policies to be applied to all packets in a traffic flow on various nodes along the network path.
- It may be possible to stack those various policies in a list of TLVs in the header of each packet.
 - This approach would introduce great complexities, damage MTU, and impose big challenges on the hardware processing and forwarding.
- When doing the policy-based routing along the network path, normally ACL via 5 tuples is used, but it is complicated to resolve.
 - With tunnel encapsulation, it is hard to resolve the 5 tuples since the transport layer information is down so deep.
 - With IPSec, it becomes impossible to obtain any transport layer information.
 - In the IPv6 data plane, with the extension headers being added before the upper layer, in some implementations it becomes very difficult and even impossible to obtain transport layer information because that information is so deep in the packet. So there is no 5 tuples anymore, and maybe only 2 tuples are available.



How to solve the issues? – Possible solutions and benefits

- Acquire and construct an attribute at the network edge, and encapsulate it in the packets.
- Such information is treated as an object in the network
 - Network operator applies policies and provides services in various nodes/service functions along the path depending on the information
 - Policy choice is effectively according to user/application group and/or service-level requirement
- Such information will also bring benefits, for example,
 - Improve the forwarding performance since it will only use 1 field in the IP layer instead of resolving 5 tuples, which may also improve the scalability.
 - Very flexible policy enforcement in various nodes and service functions along the network path.
- Furthermore, with such information, more new services could be enabled, for example,
 - The policy execution on the service function can be based only on this value and not based on 5-tuple, which can eliminate the overhead involved by ACL
 - Even more fine-granularity performance measurement could be achieved and the granularity to be monitored and visualized can be controllable, which is able to relieve the processing pressure on the controller when it is facing the massive monitoring data
 - The underlay performance guarantee could be achieved for SD-WAN overlay services, such as explicit traffic engineering path satisfying SLA and selective visualized accurate performance measurement.
- This can be easily done by utilizing this information, which is not possible with any of the current existing mechanisms.

How to solve the issues? – Gap Analysis

- Some mechanisms have been specified in IETF using attribute/identifier to perform traffic steering and service provisioning.
- 1. DSCP in the IPv4 and IPv6 Headers [RFC2474]
 - The field is not big enough.
- 2. IPv6 Flow Label [RFC6437] /MPLS Entropy Label [RFC6790]
 - The IPv6 flow label is mainly used for Equal Cost Multipath Routing (ECMP) and Link Aggregation [<u>RFC6438</u>].
 - [RFC6391] adds the Label Stack Entry (LSE) to facilitate the load balancing of the flows within a pseudowire (PW) over the available ECMPs.
- 3. SFC ServiceID [I-D.ietf-sfc-serviceid-header]
 - Subscriber Identifier and Performance Policy Identifier are carried in the Network Service Header (NSH) [<u>RFC8300</u>] Context Header.
 - The APN attribute can be carried in various data plane encapsulations.
 - The APN attribute is treated as an object in the network, to which the network operator applies policies in various nodes/service functions along the path and provide corresponding services.
- 4. IOAM Flow ID [I-D.ietf-ippm-ioam-direct-export]
 - Flow ID is used to correlate the exported data of the same flow from multiple nodes and from multiple packets.
 - The APN identifier can serve more various purposes.
- 5. Binding SID [<u>RFC8402</u>]
 - BSID is bound to an SR Policy, instantiation of which may involve a list of SIDs.
 - The APN identifier is not bound to SRv6 only, and it can be carried in various data plane encapsulations.
- 6. FlowSpec Label [<u>RFC5575</u>], [<u>I-D.ietf-idr-flowspec-mpls-match</u>], [<u>I-D.ietf-idr-bgp-flowspec-label</u>], [<u>I-D.liang-idr-bgp-flowspec-route</u>]
 - In BGP VPN/MPLS networks, BGP FlowSpec can be extended to identify and change (push/swap/pop) the label(s) for traffic that matches a particular FlowSpec rule. BGP is used to distribute the FlowSpec rule bound with label(s).
 - APN identifier is not bound to MPLS only, and it can be carried in various data plane encapsulations.

APN: Application-aware Networking

How to solve the issues? – Gap Analysis

- The existing solutions are specific to a particular scenario or data plane, not the same as APN and unable to achieve the same effects.
- As driven by ever-emerging new 5G services, fine-granularity service provisioning becomes urgent.
- APN aims to define a generalized attribute used for service provisioning, and can be carried in various data plane encapsulations.

Frequently Asked Questions

• 1. Are there any applications that can benefit from APN?

I would like to ask how many of us have experienced the Meetecho issues in this IETF and the virtual ones before. This is one of the applications that can benefit from APN. :)

In this IETF, we had a hackathon "Application-aware G-SRv6 networking", which shows the improvements that can be achieved with APN, using which the traffic is steered into the SRv6 path [1]. The results are going to be presented and demonstrated in the INFOCOM2021. There was also the first demonstration of APN in the INFOCOM2020[2].

[1] <u>https://github.com/APN-Community/IETF-110-Hackathon-Demo/blob/master/Application-aware_G-SRv6_networking__Demo_and_Test.pdf</u>
 [2] <u>https://ieeexplore.ieee.org/abstract/document/9162934</u>

2. How APN can help resolve the QoE issues?

As shown in the demonstrations, we can see the differences/improvements which APN can make in the network. QoE is complex and has many impacting factors including both the terminal, access and the network. APN aims to provide ways to improve the QoE within the network.

3. Who is to set the APN attribute?

It is the network edge device such as CPE (Customer Premises Equipment) not the application.

4. How to set the APN attribute?

There are many possible ways that can be used to classify the traffic flow at the network edge, e.g., the N-tuples defined in the MEF70 and the AI technologies. An APN attribute can be derived by using the match items published in MEF70 as well as the access port in the edge device.

5. How the APN attribute is used in the network?

The APN attribute is carried in the data packet's header, and it can be used in the various nodes/service functions along the network path to enforce the policies on the differentiated traffic flow, e.g.,

- 1) at the headend to steer into corresponding path satisfying SLAs
- 2) at the midpoint to collect corresponding performance measurement data
- 3) at the service function to execute particular policies

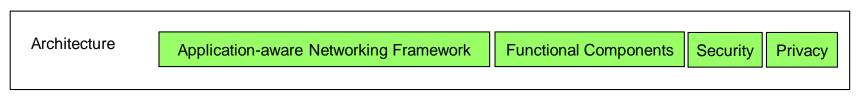
Questions still need to be addressed

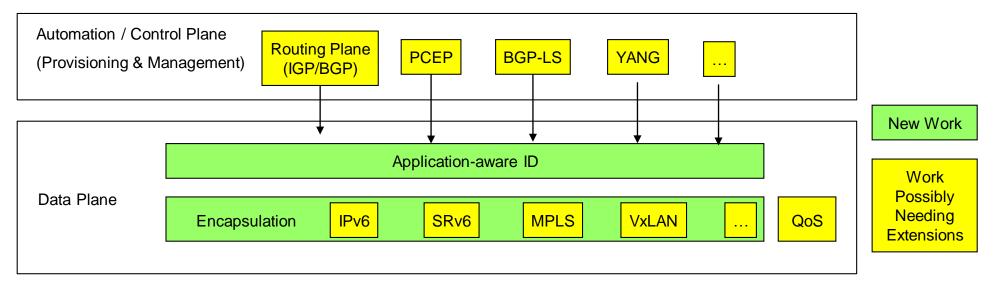
- Security Issues
 - What are the security issues when the APN attribute is used within the limited operators' controlled domain?
- Privacy Issues
 - Mitigate the issues by grouping the users and applications
 - ✓ User group
 - Application group
 - Use an opaque value
 - Focus on describing the classes of policy to be applied to the traffic

Plan to form a working group

• The potential work items as below,

New Services App-aware Network Slicing App-aware Detnet App-aware SFC App-aware Network Slicing SLA Guarantee





APN: Application-aware Networking

APN Activities

- Side Meetings @IETF105 & IETF108
- Hackathons @IETF108 & IETF109 & IETF110
- Demos @INFOCOM2020 & 2021
- **APN Mailing List** Discussions apn@ietf.org



Google	
Perglucotco Den	Telefini
And Stand Jonania (Jandia and Jandia and Jan	Chino citata
Chell Carlor (Monte) Annuel Carlo Naue Facel, Society (Strange) Annuel Naue Society, synchrodinausain Naue Annuel Carlo (Strange) Naue Society, Strange) Naue Society, Strange) Naue Society, Strange) Naue Society, Strange) Naue Society, Strange) Naue Society, Strange) Naue Society, Strange)	
Door reg In Guiden Charens, genes gabriell Marriers Door (Expection) Door inget, streme up to III. Son illinget, streme up to III. Son illinget, streme up to III. Reg is General (Streme).	
barea Contr. (Turkis bare, raises all: Berbancheid) Strawi dogs Lack, Ruthera, dogs under performances dogs lacker en practice meg. 2017 (nume) eng. 2017 (nume) eng. 2017 (nume)	
Lun Sport Con Mana Ten Dava Julia Ten Dava Julia	

https://github.com/APN-Community

Application-aware G-SRv6 network

- Champions
 - Jianwei Mao (maojianwei@...)
 - Chena Li (c.l@...)
 - Shuping Peng (pengshuping@...)
- Projects
 - Develop functions of Generalized SRv6 (G-SRv6
 An Instance
 - Combine G-SRv6 with APN6, to achieve Applica
- Specifications

 - Implementation of the second se
 - o
 ⊕ draft-cl-spring-generalized-srv6-for-cmpr

IETF108 Ŵ ica Birds of a Feather at IETF 109 wo proposals for Birds of a Feather (BOF) sessions at IETF 10

> https://www.ietf.org/blog/ietf109-bofs/ https://www.ietf.org/blog/ietf110-bofs/

Application-aware traffic control.

https://trac.ietf.org/trac/ietf/meeting/wiki/110hackathon https://trac.ietf.org/trac/ietf/meeting/wiki/109hackathon

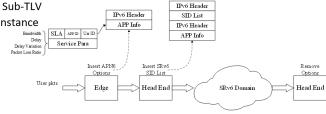
https://trac.ietf.org/trac/ietf/meeting/wiki/108hackathon

- Make use of the IPv6 extensions header to convey the service requirements, in the form of APN6 options and optional Sub-TLV.

IETF109

ine the path for potential new work, generate

- Determine the SRv6 SID List based on the encapsulated options and





said with decade

The network over

IE Deserve rade the network every of applications in real as the so ID which identifies and the over of application, and the SLA level, i.e. to indicate t 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 while a local it could also include an

must ever the actuals, but the whole loop is long a

comming which is not sainlike for her

We proposed Application invested Prin Nationals manufal (1979), which is able to results the

nine for other and

Demo Abstract:

APN6: Application-aware IPv6 Networking

to rackets according to the matching subgrounds

the rath article according to the predicate

printic information, and could also adopt the

ing only because

of with the Post markets

and the continuous diagonal of TE summing Publics Appenus Press Mid-Paint This double can

https://ieeexplore.ieee.org/abstract/document/9162934

Processing Latency

Implemented Functions

- We've implemented the demo based on P4, and conducted some simulations based on BMv2.
- Functions in Demo
- APN6:
- 1. The encapsulation of APN6 Options and Serice-Para Sub-TLV, support 2 types of APN6 Options and 4 types of Sub-TLV
- The encapsulation of the SRv6 SID List according to IPv6 DA and APN6 options
- Basic SRv6 END SID processing

Result

- Send 50,000 packets in each experiment
- The interval between 2 packets is 1ms.
- All results are in nanoseconds

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. maoijanwei, pengshuping, volanda xia, huzhibo, lizhenbin) @huawei.co

hstract-This demo showcased how application-aware Grecirculation. This has become a big obstacle for SRv 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 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 w IPv6 source routing paradigm, intro than SRvő and is fully compatible with SRvő. Up to 75 percent overhead of an SRv6 SID List can be reduced by using 32-bit encode Generalized SIDs (G-SID) in the Generalized SRH (G ompressed SID with G-SRv6, allowing most me upport up to 10 SIDs processing with SRH), where a G-SID can be a 128-bit SRv6 SID, a 32-bit Angeland Templand Art are Annual and and a

ecirculation, significantly mitigating hardware processing overhead and facil deployments. Furthermore, for the first Application-aware IPvő networking (AF ngress node is able to steer a particula propriate G-SRv6 TE policy to guara

tion type of a user group and it

network infrastructure essentially do nted APN6 function in Linux kernel to ID to packets. Next, we enhanced Nginx oplication performance optimization Fig. 3. Application-aware G-SRv6 dep this issue, Application-aware IPv6 networking(ArN6) [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

Segment ID (SID) list into the Segment Routing Header (SRH) at the ingress node, where each SID is 128-bit long. The SLA Fig. 1. Format of the128-bit SRv6 SID and 32-bit G-SII 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 In most cases, only Node ID and Function ID are differen 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-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, SRv6) realizes this idea. It only carries the compressed SID consisting of node ID and Function ID in the SRH, so that the the size of an SRv6 encapsulation with 10 SIDs is 208 bytes, which exceeds the parser window of most merchant silicon chipsets (e.g., Jericho2) and causes expensive packet size of the SRH is compressed. Theoretically, up to 75% overhead of the SRv6 SID list can be reduced. The SID size comparison between SRv6 and G-SRv6 with 32-bit C-SIDs is shown in Fig. 2.

Getting Ingress timestamp ID option riment 2 Experiment 1: Switching based on IPv6 DA Switching based on IPv6 DA rting an APP aware ID op Inserting APN6 option Without processing of APN6 Switching based on IPv6 DA



Performance Evaluation

Experiment	Mean	STDEV	МАХ	MIN	Range
1 (IPv6)	364.07436	0.56514087	366	363	3
2 (IPv6 & APN6)	370.63256	0.611774343	373	369	4
DIFF	6.5582	0.046633473	7	6	



Keywords-SRv6 Compression, G-SR Amongs Properties The ambasis I. INTRODUCTION and or the Link As 5G and industry verticals evol services with diverse but demanding re latency and high reliability are acce Different applications have differentiate Agreement (SLA). For instance, on-1 demanding requirements on latency, h high requirements on both latency and b traffic mainly requires more bandwidt latency. However, in current network maware of the traffic type traversing t

nd save the transmission overhead in th

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

102s, 53.33% transmission overhead is reduc utilization is increased from \$3.07% to 92.79

2 mMTC IoT metadata transmission (Pavle

shown in Fig. 1

References

Please find the APN BoF proposal in the IETF wiki for more information.

• <u>https://trac.tools.ietf.org/bof/trac/wiki/WikiStart</u>

The archived discussions in this APN mailing list can be found here.

• <u>https://mailarchive.ietf.org/arch/browse/apn/</u>

To subscribe the APN Mailing list,

<u>https://www.ietf.org/mailman/listinfo/apn</u>

Here are some relevant drafts and materials for your reference. Scope & Gap analysis

• <u>https://tools.ietf.org/html/draft-peng-apn-scope-gap-analysis</u>

Problem statement & Use cases

- <u>https://tools.ietf.org/html/draft-li-apn-problem-statement-usecases</u>
- <u>https://tools.ietf.org/html/draft-liu-apn-edge-usecase</u>
- <u>https://tools.ietf.org/html/draft-zhang-apn-acceleration-usecase</u>
- <u>https://tools.ietf.org/html/draft-yang-apn-sd-wan-usecase</u>

Framework

• <u>https://datatracker.ietf.org/doc/draft-li-apn-framework/</u>

Security & Privacy

<u>https://datatracker.ietf.org/doc/draft-peng-apn-security-privacy-consideration</u>

APN Community

<u>https://github.com/APN-Community</u>

APN: Application-aware Networking

Thank you!