Application-aware Networking (APN) Solution Discussions

Shuping Peng/Zhenbin Li

Progress summary

- APN Side Meetings @IETF105 & IETF108
- APN Hackathons @IETF108 & IETF109 & IETF110
- APN Demos @INFOCOM2020 & 2021
- APN Mailing List: apn@ietf.org
- APN Wiki: https://datatracker.ietf.org/wg/apn/about/

- The use cases have been discussed extensively in previous IETF meetings
  - SD-WAN, FBB, MBB, etc.

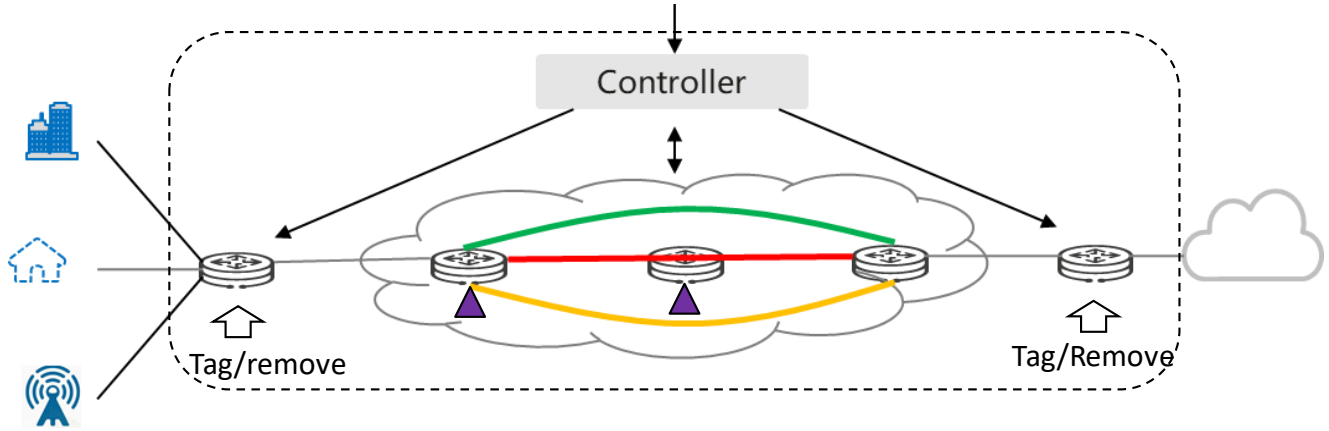
- RTG people would like to start working on the solutions of APN.

Scope & Scenario of APN

- APN works within a service operator's network domain.
  - Typically, an APN domain is defined as a service provider's network domain where MPLS, SR/SRv6, VXLAN and other tunnel technologies are adopted.
  - APN attribute is tagged/removed at the edge of the network domain.
- APN is not about identifying a particular application or user within the network.
- APN is about telling the network what policies to apply to traffic.

☐ **APN attribute is constructed based on the existing information such as 5-tuple presented in the packet header.**

☐ According to the APN attribute, various policies can be flexibly applied to the traffic flow on various nodes along the network path, without the need of resolving the 5-tuple at every policy enforcement point in the network.



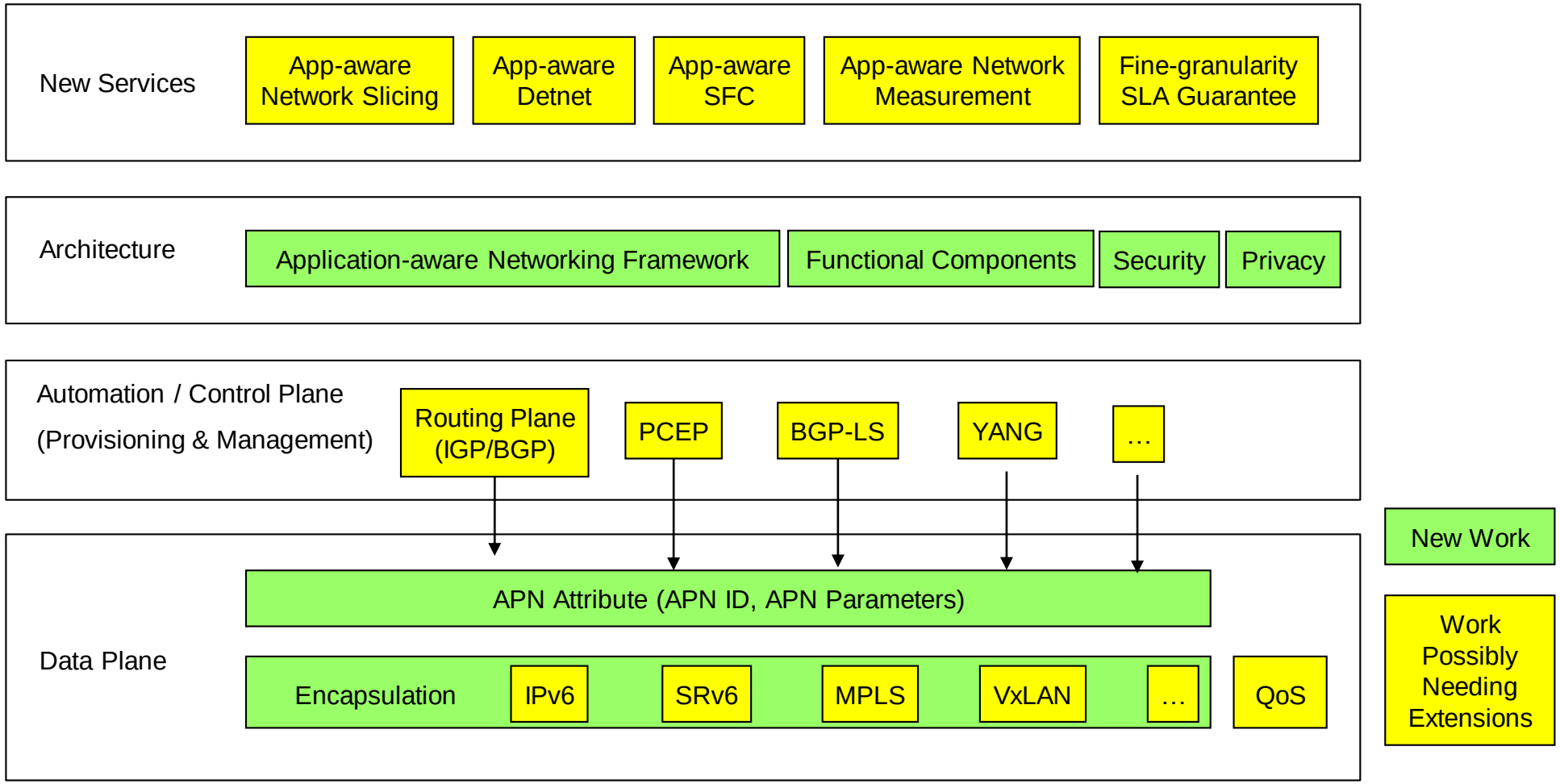
Updates

- Changes we have made to the drafts according to feedback received from the presentations @IETF110
  - Removed the application-side solution, only keep the network-side solution
  - The APN attribute is acquired based on the existing information in the packet header such as 5-tuple and QinQ (S-VLAN and C-VLAN) at the edge devices of the APN domain, added to the data packets along with the tunnel encapsulation.
  - When the packets leave the APN domain, the attribute will be removed together with the tunnel encapsulation header.
  - APN aims to apply various policies in different nodes along a network path onto a traffic flow altogether, for example, at the headend to steer into corresponding path, at the midpoint to collect corresponding performance measurement data, and at the service function to execute particular policies.

- Drafts have been updated accordingly to reflect the presented contents and concepts
  - Framework
    - https://tools.ietf.org/html/draft-li-apn-framework
  - Problem Statement
    - https://tools.ietf.org/html/draft-li-apn-problem-statement-usecases
  - Scope & Gap analysis
    - https://tools.ietf.org/html/draft-peng-apn-scope-gap-analysis
  - Security & Privacy consideration
    - https://tools.ietf.org/html/draft-peng-apn-security-privacy-consideration

Supporters would like to form a working group

- The potential work items as below,



APN: Application-aware Networking

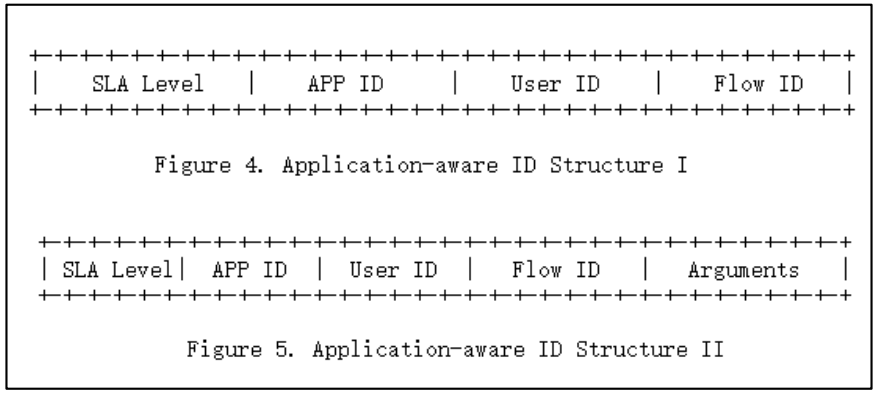
Solutions that need to look into

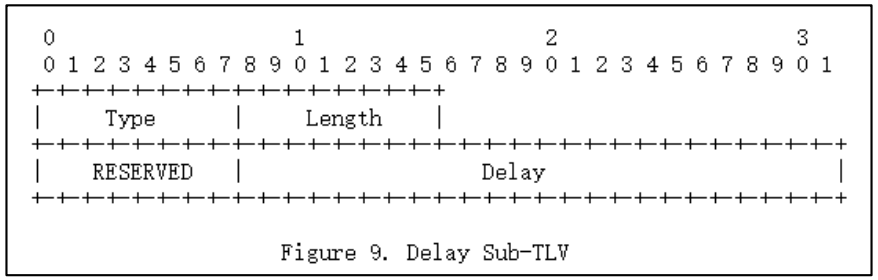
1. Design of the APN attribute
2. Encapsulation of the APN attribute on the various data planes
3. Delivery of the APN attribute through the control plane protocols
4. Management of the APN attribute via NETCONF/YANG

Design of the APN attribute I

- APN header design
  - Do we need a dedicated header for APN?
  - How about the encapsulations of different types of tunnels?
- APN attribute structure design, In which format? – hardware friendly
  - TLV?
- APN attribute design, including
  - APN ID
  - APN Parameters
  - ?
- APN ID design, including
  - APP Group ID (Mandatory/Optional?)
    - The identifier of the application type/group
  - USER Group ID (Mandatory/Optional?)
    - The identifier of the user type/group
  - SLA (Mandatory/Optional?)
    - The SLA level of the service requirements
  - Session/FLOW ID (Mandatory/Optional?)
    - The identifier of the key session/flow of the traffic flow
- APN Parameters, including network performance parameters
  - Bandwidth, Latency, Jitter, Packet loss?
- Length design
  - APN ID: Flexible/Fixed?
  - APN Parameters: Flexible/Fixed?
  - Total length: Flexible/Fixed?

Example of the APN attribute structure





https://tools.ietf.org/html/draft-li-6man-app-aware-ipv6-network-03

Encapsulation of the APN attribute on the various data planes

- MPLS
  - Anything from the ongoing DT?
- IPv6/SRv6
  - Location? - Extension header
    - HBH, DOH, SRH
  - Fixed location or multiple choices?
- Overlay tunnels
  - VxLAN-GPE
  - GENEVE
- GTP-u
- Priority?
  - IPv6-based
  - MPLS-based
  - …

Example of the encapsulation of the APN attribute on the IPv6 data plane

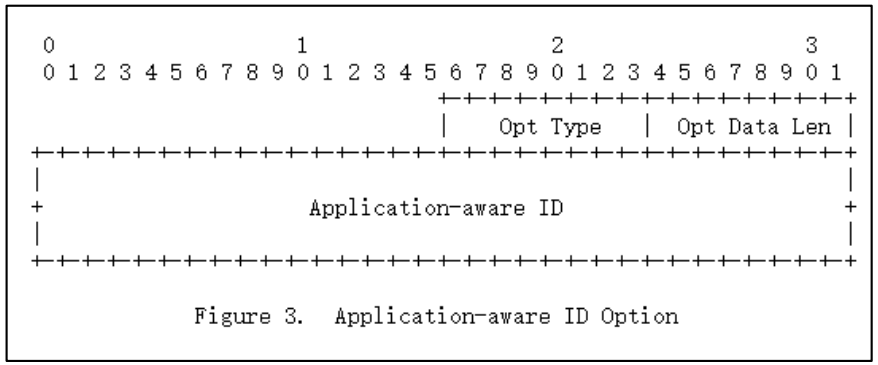


Figure 3. Application-aware ID Option

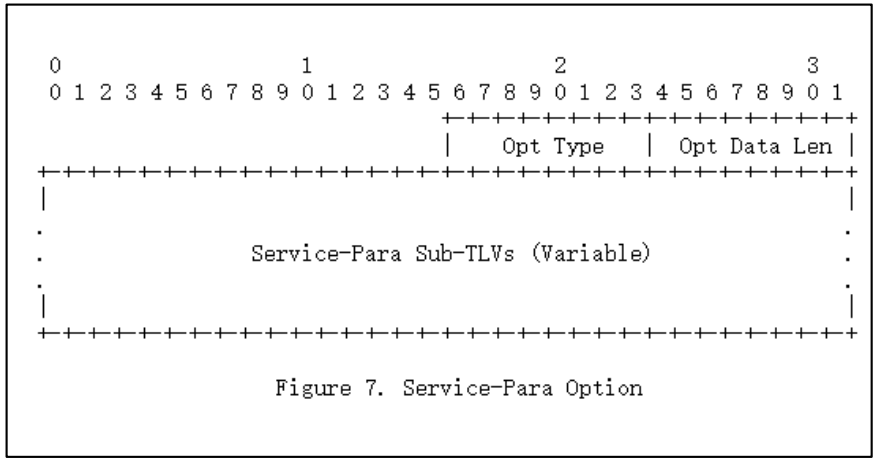
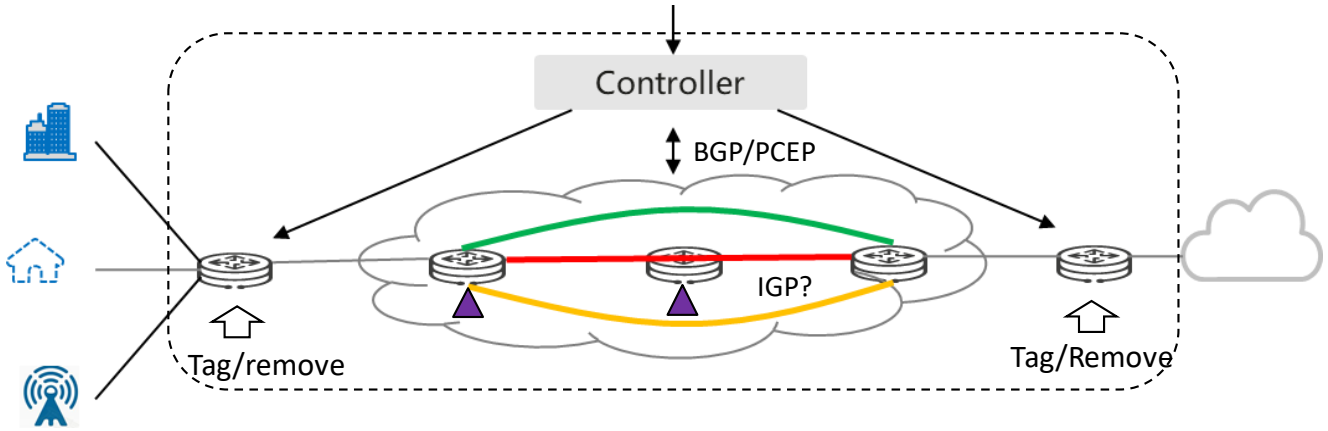


Figure 7. Service-Para Option

https://tools.ietf.org/html/draft-li-6man-app-aware-ipv6-network-03

Delivery of the APN attribute through the control plane protocols

- BGP
  - Between the Controller and network devices including
    - APN-Edge: existing information in the packet header and the APN attribute
    - APN-Headend: the APN attribute and the policies (for traffic steering)
    - APN-Midpoint/APN-Endpoint
- PCEP
  - Between the Controller and network devices, for policy enforcement, etc.
    - APN-Edge/APN-Headend/APN-Midpoint/APN-Endpoint
- BGP-LS
  - Is it needed?
- IGP?
  - Is it needed?



Management of the APN attribute via NETCONF/YANG

- Configurations for
  - the existing information in the packet header to the APN Attribute
  - the APN attribute to the policies
- YANG model for the NBI of the controller
  - Service models defined
  - Refer to the SD-WAN draft
  - https://datatracker.ietf.org/doc/html/draft-sun-opsawg-sdwan-service-model-04
- YANG model for the SBI of the controller
  - Device models
  - Refer to the FlowSpec draft
  - https://tools.ietf.org/html/draft-wu-idr-flowspec-yang-cfg-01
- Other key YANG models to consider?
  - Global configuration
  - For particular device such as APN-Edge/APN-Headend/APN-Midpoint/APN-Endpoint

https://datatracker.ietf.org/doc/html/draft-sun-opsawg-sdwan-service-model-04

```
+--rw application* [app-id]
|  +--rw app-id    svc-id
|  +--rw ac* [name] =application criteria
|     +--rw name                          string
|     +--rw (match-type)?
|        +--:(match-flow)                                   Match
|        |  +--rw match-flow
|        |     +--rw ethertype?          uint16
|        |     +--rw cvlan?              uint8
|        |     +--rw ipv4-src-prefix?    inet:ipv4-prefix
|        |     +--rw ipv4-dst-prefix?    inet:ipv4-prefix
|        |     +--rw l4-src-port?        inet:port-number
|        |     +--rw l4-dst-port?        inet:port-number
|        |     +--rw ipv6-src-prefix?    inet:ipv6-prefix
|        |     +--rw ipv6-dst-prefix?    inet:ipv6-prefix
|        |     +--rw protocol-field?     union
|        +--:(match-application)
|           +--rw match-application?   identityref
+--rw application-group* [app-group-id]
|  +--rw app-group-id    svc-id
|  +--rw app-id*         -> ../../application/app-id
+--rw policy* [policy-id]
|  +--rw policy-id          svc-id
|  +--rw policy-package
|     +--rw encryption?        enumeration
|     +--rw public-private?    enumeration
|     +--rw local-breakout?    boolean
|     +--rw billing-method?    enumeration
|     +--rw backup-path?       enumeration
|     +--rw bandwidth
|        +--rw commit?   uint32                              Policy
|        +--rw max?      uint32
+--rw endpoints* [endpoint-id]
   +--rw endpoint-id             svc-id
   +--rw site-role?              identityref
   +--rw site-attachment
   |  +--rw site-id?   -> /sdwan-svc/sites/site/site-id
   +--rw endpoint-policy-map
      +--rw app-group-policy* [app-group-id]
      |  +--rw app-group-id    leafref
      |  +--rw policy-id?      leafref
      +--rw app-policy* [app-id]
         +--rw app-id       leafref
         +--rw policy-id?   leafref                        Policy
```

https://tools.ietf.org/html/draft-wu-idr-flowspec-yang-cfg-01

```
+--rw flowspec-cfg
|  +--rw flowspec-policy* [policy-name]
|     +--rw policy-name       string
|     +--rw vrf-name?         string
|     +--rw address-family?   identityref
|     +--rw flowspec-rule* [rule-name]
|        +--rw rule-name                string
|        +--rw flowspec-component* [component-type]
|        |  +--rw component-type        component-enum
|        |  +--rw (component)?
|        |     +--:(destination-prefix)                                  Match
|        |     |  +--rw destination-prefix?   inet:ip-address
|        |     +--:(source-prefix)
|        |     |  +--rw source-prefix?        inet:ip-address
|        |     +--:(ip-protocol)
|        |     |  +--rw ip-protocol* [op value]
|        |     |     +--rw op       numeric-operator
|        |     |     +--rw value    uint16
|        |     +--:(port)
|        |     |  +--rw port* [op value]
|        |     |     +--rw op       numeric-operator
|        |     |     +--rw value    uint16
|        |     +--:(destination-port)
|        |     |  +--rw destination-port* [op value]
|        |     |     +--rw op       numeric-operator
|        |     |     +--rw value    uint16
|        |     +--:(source-port)
|        |     |  +--rw source-port* [op value]
|        |     |     +--rw op       numeric-operator
|        |     |     +--rw value    uint16
|        |     +--:(icmp-type)
|        |     |  +--rw icmp-type* [op value]
|        |     |     +--rw op       numeric-operator
|        |     |     +--rw value    uint8
|        |     +--:(icmp-code)
|        |     |  +--rw icmp-code* [op value]
|        |     |     +--rw op       numeric-operator
|        |     |     +--rw value    uint8
|        |     +--:(tcp-flags)
|        |     |  +--rw tcp-flag* [op value]
|        |     |     +--rw op       bitmask-operator
|        |     |     +--rw value    uint16
|        |     +--:(packet-length)
|        |     |  +--rw packet-length* [op value]
|        |     |     +--rw op       numeric-operator
|        |     |     +--rw value    uint16
|        |     +--:(dscp)
|        |     |  +--rw dscp* [op value]
|        |     |     +--rw op       numeric-operator
|        |     |     +--rw value    dscp-type
|        |     +--:(fragment)
|        |        +--rw fragment* [op value]
|        |           +--rw op       numeric-operator
|        |           +--rw value    fragment-type
|        +--rw flowspec-action* [action-type]
|           +--rw action-type     action-type
|           +--rw (action)?
|              +--:(traffic-rate)                                       Action
|              |  +--rw rate?           float
|              +--:(redirect)
|              |  +--rw route-target?   string
|              +--:(traffic-marking)
|                 +--rw remark-dscp?    dscp-type
```

Security Consideration

In the APN work, in order to reduce the privacy and security issues, the following specifications are defined:

[S1]. The APN attribute MUST be conveyed along with the tunnel information in the APN domain. The APN attribute is encapsulated and removed at the APN-Edge.

[S2]. The APN ID (including the Application Group ID and the User Group ID) MUST be acquired from the existing available information in the packet header without interference into the payload.

According to the above specifications, the APN attribute is only produced and used locally within the APN domain without the involvement of the host/application side.

In order to prevent the malicious attack through the APN attribute, the following policies can be configured at the network devices of the APN domain:

[P1]. If the APN attribute is conveyed without the tunnel information, the packet MUST be dropped.

[P2]. If the APN attribute is not known to the APN domain, it should trigger the alarm information. The packet can be forwarded without being processed or dropped depending on the local policy.

[P3]. If the network service requirements exceed the specification for the specific Application Group ID and/or User Group ID, it should trigger the alarm information. The packet should be discarded to prevent abusing of the resources.

[P4]. There should be rate-limiting policy at the APN-Edge to prevent the traffic belonging to a specific Application Group ID and/ or User Group ID from exceeding the preset limit.

Next step

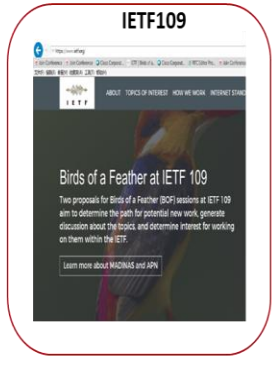
- Work on the Charter of the APN working group, who wants to get involved?

- Work on the drafts on solutions, who wants to get involved?

Thank you!

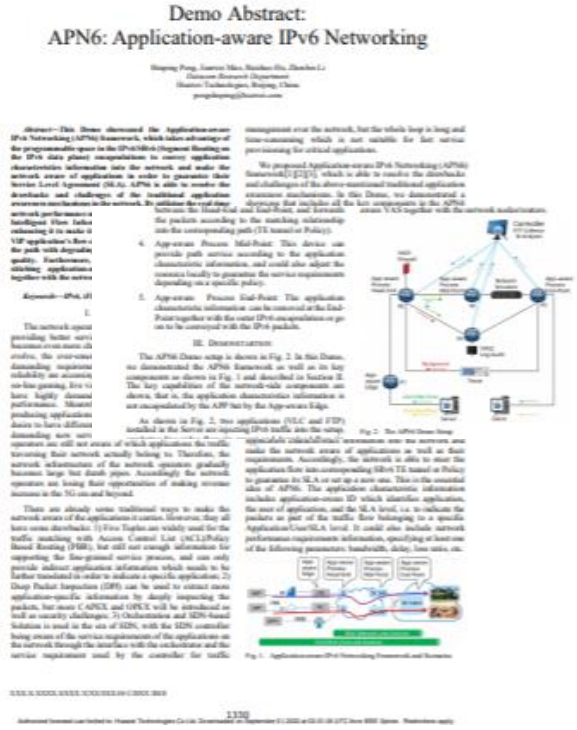
APN Activities

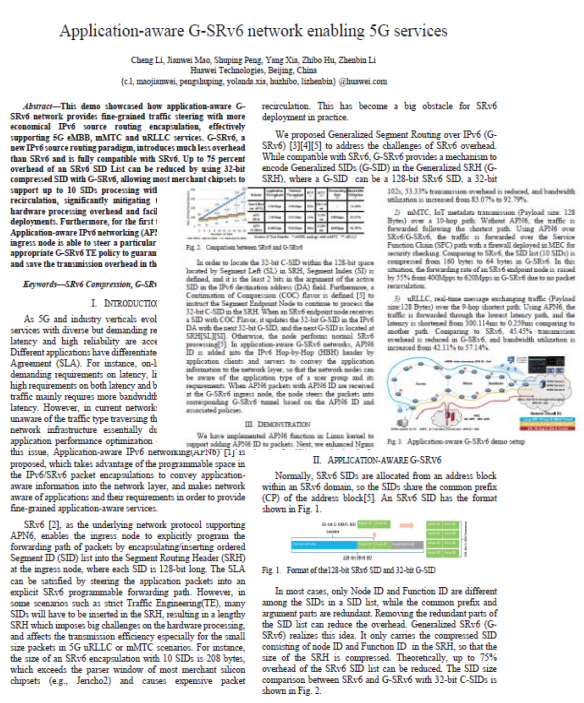
- **Side Meetings** @IETF105 & IETF108
- **Hackathons** @IETF108 & IETF109 & IETF110
- **Demos** @INFOCOM2020 & 2021
- **APN Mailing List** Discussions - apn@ietf.org



https://github.com/APN-Community

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



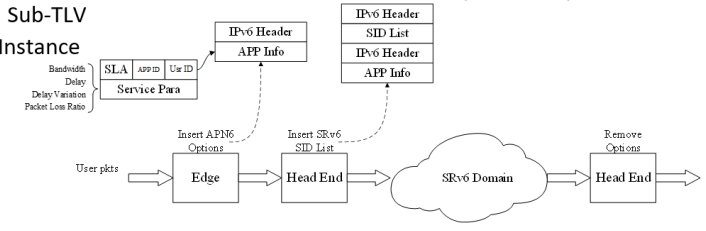


https://ieeexplore.ieee.org/abstract/document/9162934
https://www.youtube.com/watch?v=ONqwxKVmPp0

Application-aware G-SRv6 network

- Champions
  - Jianwei Mao (maojianwei@...)
  - Cheng Li (c.l@...)
  - Shuping Peng (pengshuping@...)
- Projects
  - Develop functions of Generalized SRv6 (G-SRv6
  - Combine G-SRv6 with APN6, to achieve Applica
- Specifications
  - draft-lc-6man-generalized-srh
  - draft-cl-spring-generalized-srv6-np
  - draft-cl-spring-generalized-srv6-for-cmpr
  - draft-li-6man-app-aware-ipv6-network
  - draft-li-apn-framework

- Application-aware traffic control.
  - Make use of the IPv6 extensions header to convey the service requirements, in the form of APN6 options and optional Sub-TLV.
  - Determine the SRv6 SID List based on the encapsulated options and Sub-TLV
- An Instance

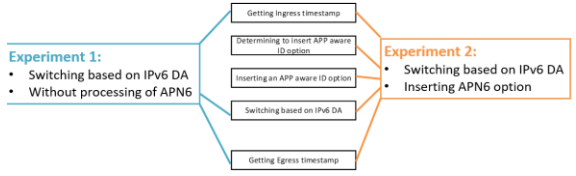


Implemented Functions

- 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
    2. The encapsulation of the SRv6 SID List according to IPv6 DA and APN6 options
    3. Basic SRv6 END SID processing

Performance Evaluation

- **Processing Latency**



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

Experiment	Mean	STDEV	MAX	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	

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

References – Drafts have been updated

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

- https://trac.tools.ietf.org/bof/trac/wiki/WikiStart

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

- https://mailarchive.ietf.org/arch/browse/apn/

To subscribe the APN Mailing list,

- https://www.ietf.org/mailman/listinfo/apn

Here are some relevant drafts and materials for your reference.

Scope & Gap analysis

- https://tools.ietf.org/html/draft-peng-apn-scope-gap-analysis

Problem statement & Use cases

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

Framework

- https://datatracker.ietf.org/doc/draft-li-apn-framework/

Security & Privacy

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

APN Community

- https://github.com/APN-Community

APN: Application-aware Networking