#### APN

Long name: Application-aware Networking

Abbreviation: APN

**Summary:**

APN is focused on developing a framework and set of mechanisms to derive, convey and use an identifier to allow for implementing fine-grain user (group)-, application (group)-, and service-level requirements at the network layer.

The identifier is acquired, constructed in a structured value, and then encapsulated in the packets. Such structured value is treated as an opaque object in the network, to which the network operator applies policies in various nodes/service functions along the path and provide corresponding services. The identifier may represent the application traffic of a particular user group but does not identify the actual user nor the actual application for the network operator.

The use-case presented below further expands on the rationale for such identifier and how it can be derived and used in that specific context.

APN works within a limited trusted domain. Typically, an APN domain is defined as the service providers’ limited domains in which MPLS, VXLAN, SR/SRv6 and other tunnel technologies are adopted to provide services.

**Use case example**

To be more specific and more concrete, here we use SD-WAN as an example use case to present more detailed explanations.

In the case of SD-WAN, an enterprise usually buys WAN services from an SD-WAN provider for its employees to access the applications in the Cloud, and then the SD-WAN provider may buy WAN lines from a network operator. The enterprise may know what applications will use the SD-WAN services but it will only provide the 5 tuples of those applications to the SD-WAN provider. So the SD-WAN provider does not know what applications it is actually serving. And then, the SD-WAN provider would usually buy WAN services from Network Operator. It will only provide 5 tuples to the Network Operator and the service-level requirements for steering their customer’s traffic. In this way, the Network Operator does not know anything else about the traffic except the 5 tuples and requirements. Nowadays, SD-WAN is usually using 5-tuple to steer the traffic into corresponding WAN lines across the Network Operator’s network.

However, there are two main issues in the current SD-WAN deployments.

1. It is complicated and hard to resolve the 5 tuples. Even worse, with the traffic being all encrypted, it becomes impossible to obtain any transport layer information. Moreover, 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.
2. Currently there is still no way to apply various policies in different nodes along the network path onto a traffic flow altogether, that is, 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. Maybe we can stack those various policies in a list of TLVs at the headend. However, it is going to introduce great complexities and impose big challenges on the hardware processing and forwarding.

With APN, at the edge node, i.e. CPE, of the SD-WAN, the 5-tuple, plus information related to user or application requirements is constructed into a structured value. Please note, here the structured value is just a bit string respectively and do not indicate actual application/user identification. This information is only meaningful for the network operators to apply various policies in different nodes/service functions.

With such identifier in the network, we can easily solve the two issues above-mentioned.

1. We will not need to resolve the 5-tuple and perform the deep inspection any more. This structured value is encapsulated in the IP layer and can be easily read by the router and service function. If the data plane is SRv6, for example, such identifier can be encapsulated in an SRH TLV.
2. Since this identifier is taken as an object to the network, the network operators will simply place the policies in the nodes/service functions where this indicated traffic will go through, and the corresponding node/service function will just apply policies for this object. This can be easily done by utilizing this structured value, which is not possible with any current existing mechanism.

Such structured value will also bring other benefits, for example,

1. 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.
2. Very flexible policy enforcement in various nodes and service functions along the network path.

Furthermore, with such structured value, more new services could be enabled, for example,

1. 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;
2. The policy execution on the service function can be only based on this value and not based on 5-tuple, which can eliminate the need of deep packet inspection;
3. 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.

The BoF plans on covering:

* A discussion on the use-case
* A discussion on the possible means to achieve that use-case
* A discussion on which other use-cases would benefit from a similar set of functionalities as well as on the identification of commonalities amongst them, if any
* A discussion on the security and privacy aspects of identifier based solutions

The overall goal of the BoF is to gather wider consensus in the IETF community on the way forward for APN, in particular, whether protocol extensions are necessary and whether existing operational procedures will need to be changed, and what the potential work items would be in order to construct the APN.

Status: Non-WG Forming

Responsible Area Director (AD): Martin Vigoureux

BoF chairs:  AD to assign

BoF Proponents: Zhenbin Li <lizhenbin@huawei.com>, Shuping PENG <pengshuping@huawei.com>, James N Guichard < jguichar@futurewei.com>, Zafar Ali <zali@cisco.com>, Daniel Voyer <daniel.voyer@bell.ca>, Luis M. Contreras <luismiguel.contrerasmurillo@telefonica.com>, Chongfeng Xie <xiechf.bri@chinatelecom.cn>, Feng Yang < yangfeng@chinamobile.com >, Chang Cao < caoc15@chinaunicom.cn>, Kentaro EBISAWA <ebisawa@toyota-tokyo.tech>, Stefano Previdi <stefano@previdi.net>

Number of people expected to attend: 100

Length of session (1, 1.5, 2, or 2.5 hours): 2 hours

Conflicts to avoid (whole Areas and/or WGs): 6man, v6ops, spring, opsawg, intarea, dmm, rtgwg, sfc, detnet, ippm, mpls, pce, teas

Tentative Draft Agenda

1. Introduction and problem statement (15 mins)
2. Scope (30 mins)
   * Discussion of problem statement and scope
3. Use cases (20 mins)
   * Discussion of use cases
4. Gap analysis and potential work items (40 mins)
   * Discussion of gap analysis and possible work items
5. Conclusions and hums (15 mins)

Links to the mailing list, draft charter if any, relevant Internet-Drafts, etc.

* Mailing List: apn@ietf.org
* Relevant drafts and materials:
* 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

Appendix:

During IETF-105, the Application-aware IPv6 Networking (APN6) proposal was discussed in the APN6 side meeting, where there was some support as reported in the minutes of this meeting and the related materials are available here:

[​](https://mailarchive.ietf.org/arch/browse/ggie/) <https://github.com/APN-Community/IETF105-Side-Meeting-APN6>

Since then, it has become clear that the APN concept should apply more widely than just IPv6 networking, it should also fully embrace other technology advancements such as SRv6, as well as include MPLS.

During IETF-108, the Application-aware Networking (APN) proposal was again discussed in a side meeting, the results of which are reported in the minutes of this meeting and the related materials are available here:

<https://github.com/APN-Community/IETF108-Side-Meeting-APN>

The APN side meeting @IETF108 clarified the differences between APN and SPUD/PLUS, and it was made clear that APN focuses on the network layer within a limited domain. Four Network Operators introduced the problems faced by network operations in providing diverse levels of service, outlined various use cases that could benefit from the APN effort, and believed that the awareness of applications and their requirements could improve how networks are operated and how services are delivered. Furthermore, whether the security and privacy issues would be introduced by the APN work was analyzed and discussed case by case for each of the possible deployment scenarios. It was clarified that in the limited domains the security and privacy issues introduced by the APN can be under control [draft-peng-apn-security-privacy-consideration].

During IETF-109, the Application-aware Networking (APN) BoF was conditionally approved:

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