APN @IETF110 Report

Thanks to the ADs and Chairs of the following areas and working groups, in this IETF110, we have made presentations in the four areas which triggered a lot of active discussions and through which we collected very valuable comments and feedback. Especially those information collected from the experts in ART and SAAG made us obtain the views and concerns from new angles. Although most of the concerns were because of the walls between different areas, we did find that these feedback really helped us to focus on addressing the confusions in our presentations of the work.

The summary of each presentation is reported as below.

Before IETF, an advertisement email was sent to the APN mailing list to introduce presentation plan.

1. Dispatch - 13:00-15:00 Monday

Before the session started, an email was sent to the DISPATCH mailing list to introduce the coming presentation expressing the goal that we would like to achieve through this presentation, i.e. "**For the ARTers, we would like to especially know about the new applications' trends and requirements on the network, and how the network can serve these groups/types of applications better.**"

Zhenbin Li made the presentation.

There were a lot of discussions in the Jabber room. When going through them, we found that some similar questions have been frequently asked, so we summarized a list of FAQs as below to further clarify the confusions and concerns.

The top 5 questions are given as below, and the answers to them are provided at the end of this report.

1) Are there any applications that can benefit from APN?
2) How APN can help resolve the QoE issues?
3) Who is to set the APN attribute?
4) How to set the APN attribute?
5) How the APN attribute is used in the network?

The slides to be presented in the following sessions were also updated with a new slide on FAQ.

2. SAAG - 13:00-15:00 Thursday

The same as the above, before the session started, an email was sent to the DISPATCH mailing list to introduce the coming presentation expressing the goal that we would like to achieve through this presentation, i.e. "**For the SECers, we would like to especially know about what the**

security issues are when the APN attribute is used within a limited operator's controlled domain."

Zhenbin Li made the presentation.

We received a lot of questions and active Jabber room discussions, but they are still very similar to the ones asked in the ART, mainly about the following three key questions. They are answered at the end this document.

1) Who is to set the APN attribute?
2) How to set the APN attribute?
3) How the APN attribute is used in the network?

3. RTGAREA - 17:00-19:00 Thursday

Shuping Peng made presentation.

Probably because APN has been presented a few times and it mainly focuses on the network layer technologies, it is easier for the people in the RTG area to understand. The presentation was received very well and was considered to be concise and clear from the feedback received.

From the comments received during the meeting, people got further clarified on the APN work to be developed in the RTG area.

A use case which might be able to use APN was introduced by Linda, which was also posted and discussed in the APN mailing list. It gives an example on how to classify the different types of application flows. "For a person-to-person messaging Application Flow across the company, a full mesh is useful, but the point-of-sale Application Flow in each store can only forward IP Packets to the POS controller, at the company data center."

The main comment was on the encapsulation of the APN attribute on the IPv6/SRv6, IPv4, and MPLS data planes, more details as below.

The encapsulation on the IPv6 and SRv6 was discussed. It could use IPv6 extensions header such as hop-by-hop options header, destination options header, and segment routing header (SID arguments and SRH TLV) to encapsulate the APN attribute, since it is decoupled from the various data planes.

A clarification is further made that APN is not related with the work currently ongoing in 6man on the processing of the hop-by-hop options header, which mainly aims to make the hop-by-hop options header usable and processed reasonably.

How to encapsulate on the IPv4 and MPLS data planes was also raised. This question is actually related with the solution development, which could be investigated later altogether once we get

this work progressed further. Robin commented that this work could also be related with the discussions to be happened in the Joint session on Friday.

4. INTAREA - 15:30-16:30 Friday

The presentation time was limited in the INTAREA session. The main content was presented but no time for questions.

Tommy presented the “per-application networking” in the INTAREA session, which suggested to categorizing the traffic into user group and application group, so the privacy issues can be mitigated. However, since the app-aware info is directly tagged at the host/application, people seem to be still concerned about the privacy issues.

APN is not about identifying a particular user or application to or within the network, and we followed the suggestion to categorizing the traffic into groups, which can mitigate the privacy. Moreover, APN tags and removes its attribute at the network edge devices. When the packets leave the limited domain, the attribute will be removed and will not impact the rest of the Internet. At the network edge devices, the values in the existing fields in the IP headers (such as N-tuples as defined in MEF70) are used to construct the APN attribute, which is used by the operators to perform policies in the various nodes and/or service functions along the path. The construction of the APN attribute should obey the regulation of the area where the technology is used.

Within the network, the operators only need an opaque value or a bit string against which to perform a policy enforcement. The network does not need to know who the user is and what application is sending traffic. These information is not useful for the policy enforcement either.

==========

When going through the discussions, we found that some similar questions have been frequently asked, so we summarized a list of FAQs as below to further clarify the confusions and concerns. This list has also been sent to the DISPATCH, SAAG, and INTAREA as well as the APN mailing lists.

Frequently Asked Questions (FAQ):

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. To further clarify, this is a type of video conferencing application.

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

2. How APN can help resolve the QoE issues?

As shown in the APN demonstrations, we can see the differences/improvements which APN can make in the network. QoE is complex and has many impacting factors including the terminal, access, and 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 as 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