Application-aware Networking (APN) Problem Statement

draft-li-apn-problem-statement-usecases-03

Zhenbin Li (Huawei), Shuping Peng (Huawei), Dani Voyer (Bell Canada), Chongfeng Xie (China Telecom), Peng Liu (CMCC), Zhuangzhuang Qin (China Unicom), Gyan Mishra (Verizon), Kentaro Ebisawa (Toyota), Stefano Previdi (Huawei), Jim Guichard (Futurewei)

Problem statement

- The challenges faced by network operators when attempting to provide fine-grained traffic operations.
  - Challenges of lack of fine-granularity service information
  - Challenges of Traditional Differentiated Service Provisioning
    - ✓ Existing solutions in IETF
  - Challenges of Supporting New 5G and Edge Computing Technologies

Challenges of lack of fine-granularity service information

- In today's networks, the infrastructure through which the traffic is forwarded is not able to obtain the fine-granularity service information. It is therefore difficult for network operators to provide fine-grained traffic operations for various performance-demanding applications.
  - In order to satisfy the SLA requirements network operators continue to increase the network bandwidth but only carrying very light traffic load (in general, around 30%-40% of its capacity).

- As network technologies keep evolving, the network capability has been greatly enhanced and is able to provide fine-granularity service provisioning. For example,
  - H-QoS: provides hierarchical fine-grained QoS services.
  - SR Policy: provides the ability to handle a large number of explicit and flexible SR paths in order for services to select to satisfy their SLA requirements.
  - Network Slicing: provides the ability to define a number of network slices with guaranteed resources to satisfy highly demanding service requirements.
  - IOAM: provides more accurate performance measurement of the traffic flow.

- In summary, driven by the ever-emerging diverse demanding services, the lack of the fine-granularity information about the services in the network will cause the following issues:
  - the service information is not clearly described and known by the network
  - the fine-granularity service provisioning capability is not fully utilized
  - a fine-granularity service scheduling and measurement cannot be achieved

Challenges of Traditional Differentiated Service Provisioning

- The traditional ways used to provide fine-grained service provisioning face some challenges. The network devices mainly rely on the 5-tuple of the packets or DPI.
- However, there are some challenges for these traditional methods in differentiated service provisioning:
  - Five Tuples used for ACL/PBR:
    - ✓ cannot provide enough information for the fine-grained service process, and can only provide indirect application-level information which needs to be translated
    - ✓ involve high overhead on the forwarding process
    - ✓ impossible to resolve the 5 tuples due to the transport layer information being pushed very deep in the packet in tunnel encapsulation
  - Deep Packet Inspection (DPI):
    - ✓ introduce more CAPEX and OPEX for the network operator and impose security and privacy challenges
  - Orchestration and SDN-based Solution:
    - ✓ The whole loop is long and time-consuming which is not suitable for fast service provisioning for critical applications
    - ✓ Too many interfaces are involved in the loop, which introduce challenges of standardization and inter-operability

Effort in History - Gap Analysis

- Some mechanisms have been specified in IETF using attribute/identifier to perform traffic steering and service provisioning.
- The existing solutions are specific to a particular scenario or data plane, and a generalized method used for fine-grained service provisioning is still missing.

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 [RFC6438].
   - [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) [RFC8300] Context Header.
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.
5. Binding SID [RFC8402]
   - BSID is bound to an SR Policy, instantiation of which may involve a list of SIDs.
6. FlowSpec Label [RFC5575], [I-D.ietf-idr-flowspec-mpls-match], [I-D.ietf-idr-bgp-flowspec-label], [I-D.liang-idr-bgp-flowspec-route]
   - 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).
7. Group Policy ID
   - The capabilities of the VXLAN-GPE protocol can be extended by defining next protocol "shim" headers that are used to implement new data plane functions.
   - Group Policy ID is carried in the Group-Based Policy (GBP) Shim header [I-D.lemon-vxlan-lisp-gpe-gbp].
   - GENEVE has similar ability as VXLAN-GPE to carry metadata.

APN: Application-aware Networking

Challenges of Supporting New 5G and Edge Computing Technologies

- New technologies such as 5G, IoT, and edge computing, are continuously developing leading to more and more new types of services accessing the network.

- Large volumes of network traffic with diverse requirements such as low latency and high reliability are therefore rapidly increasing.

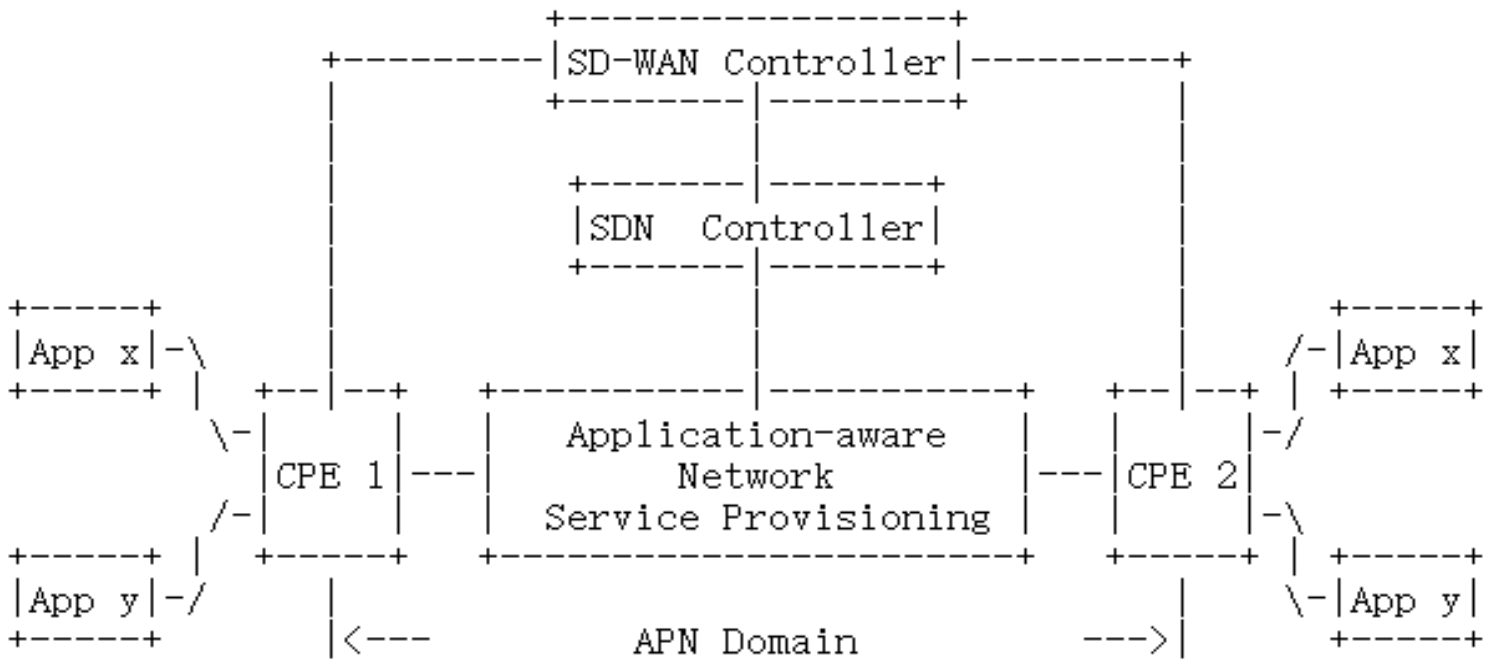
- If traditional methods for differentiation of traffic continue to be utilized, it will cause much higher CAPEX and OPEX to satisfy the ever-developing applications' diverse requirements.

Scenarios of APN Domains

- SD-WAN scenario
- Home broadband scenario
- Mobile broadband scenario

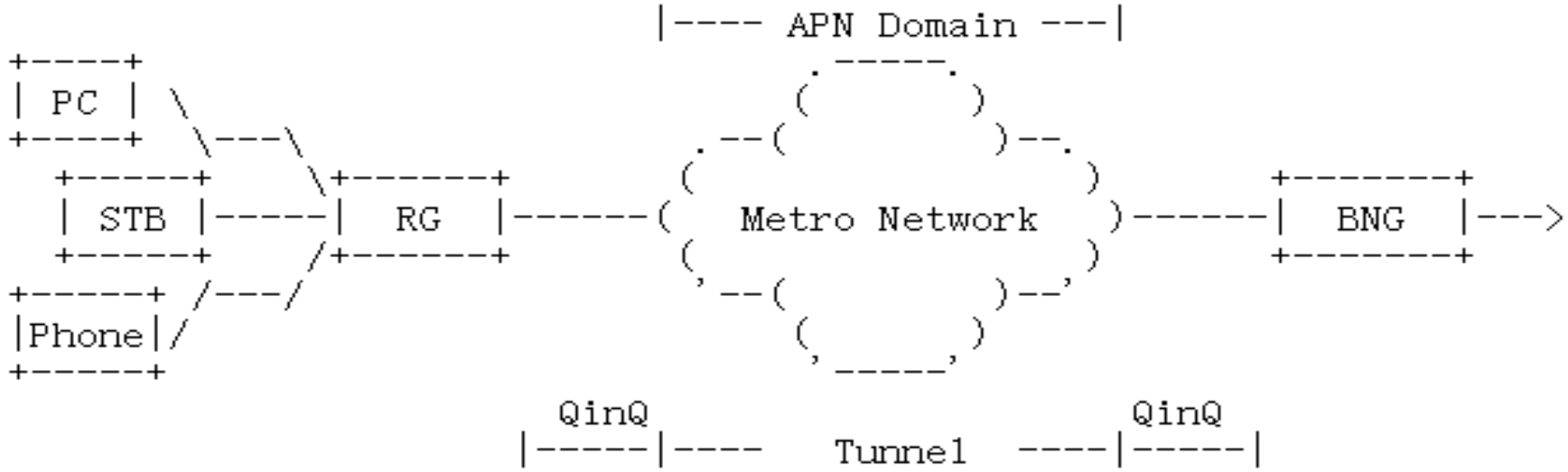
SD-WAN scenario

- With APN, at the edge node, i.e. CPE, of the SD-WAN, the 5-tuple, plus information related to user or application group-level requirements is constructed into the APN attribute.
- When the packet is sent from the CPE, the attribute is added along with the tunnel encapsulation.
- This attribute is only meaningful for the network operators to apply various policies in different nodes/service functions, which can be enforced from the Controllers.



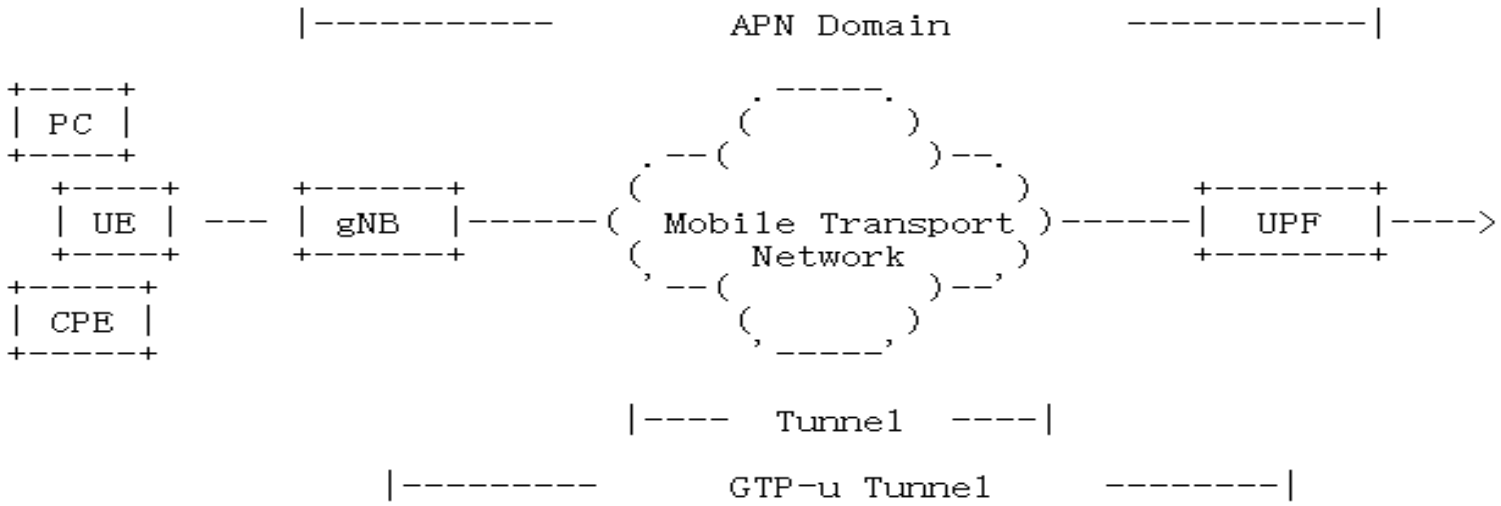
Home broadband scenario

- In the home broadband scenario, generally a home broadband user is authorized by the BNG. If the validation is passed and the access control is released, so the user group can start enjoying the value-added service.
- With APN, when the traffic traverses the metro network, the traffic flow can be indicated by the APN attribute that is added/removed at the edge devices of the Metro Network (APN domain) based on the mapping from the existing information (e.g. the QinQ which is composed of C-VLAN and S-VLAN) in the packet header and then carried in the tunnel encapsulation header.
- The APN attribute will facilitate the fine-granular service in the APN domain.
- Once the packets leave the APN domain, the APN attribute will be removed together with the tunnel encapsulation header.



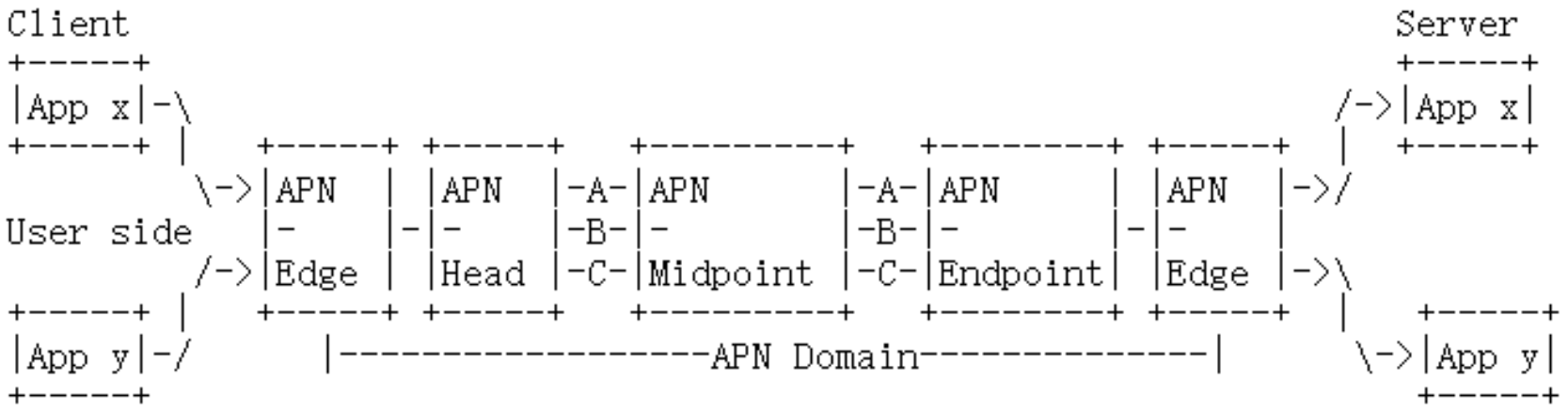
Mobile broadband scenario

- In the mobile broadband scenario, a UE is authorized by the 5GC function, and the traffic steering and QoS policy are enforced by the UPF (User Plane Function) node. If the validation is passed and the access control is released, so the user can start enjoying the value- added service.
- With APN, when the traffic traverses the mobile transport network, the traffic flow can be indicated by the APN attribute that is added at the edge devices of the mobile transport network (APN domain) based on mapping from the existing information (e.g. GTP-u tunnel encapsulation information) in the packet header and then carried in the tunnel encapsulation header.
- The APN attribute will facilitate the fine-granular service in the APN domain.
- Once the packets leave the APN domain, the APN attribute will be removed together with the tunnel encapsulation header.
- In fact, the APN attribute can also be acquired at the gNB based on the mapping of the existing information of the packet header (e.g. 5-tuple information) and carried along with the GTP-u tunnel encapsulation.



APN Framework

- Application-aware Networking (APN) is a new framework, where
  - application-aware information (i.e. APN attribute) including APN identification (ID) and/or APN parameters (e.g. network performance requirements) is encapsulated at network edge devices and carried along with the tunnel encapsulation for the packet traversing an APN domain
  - to facilitate service provisioning, perform fine-granularity traffic steering and network resource adjustment



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

APN: Application-aware Networking

Usecases (Network services) based on APN

- App-aware SLA Guarantee
- App-aware network slicing
- App-aware deterministic networking
- App-aware service function chaining
- App-aware network measurement

APN: Application-aware Networking

Thank you!