Thinking on scenarios where IP networks empower applications

IETF-119
Feng Yang (CMCC)

Background

- Fact:
  - China Mobile's IP networks has already evolved to SRv6/G-SRv6 in last year.
- Question:
  - However, SRv6 is deployed within trusted domain, mainly for L2VPN/L3VPN/EVPN services
  - How to fully leverage SRv6, create new services, then more revenue? Consider our bussiness:
    - 2C/2H products accounts for 70%
    - 2B products accounts for 20%
- Answer:
  - We defined ARN lable, which indicate the network services opened up to customer
    - It is a "contract" between service provider and subscriber that carried inside IP packet header.
      - can be map to service provider's network slice
   - is an unique and random number for each subscriber and service

Use Case 1： 2C/2H services

Case: subscriber wants better gaming experience, and placed an order.

Prerequisites: SDN underlay network with low latency slice, ARN Y is preallocated for that slice

How: Contorller allocates unique ARN X to subscriber, also ARN Y and ARN X mapping on BNG; HGW mngr puts it into HGW, then new SSID_gaming is created and binded with ARN X. BNG maps the packets with ARN X to Y, and then onto low latency slice.

 Note: ARN X represents cotract with subscriber; ARN Y represents network slice
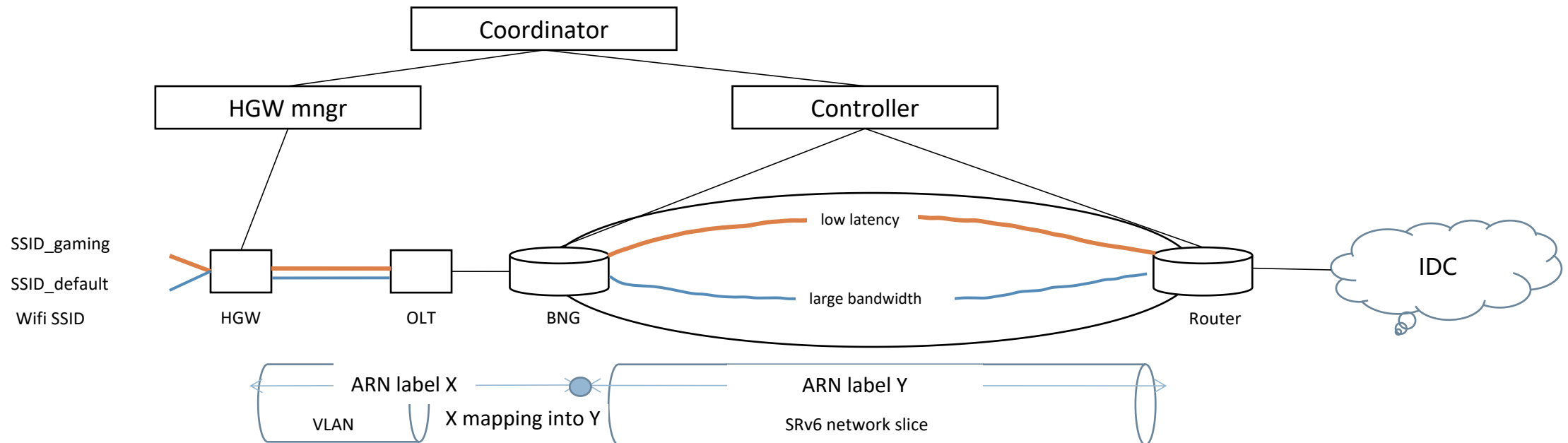
Use Case 2: 2B service

Case: customer wants better quality of service for cloud access with SD-WAN

Prerequisites: SDN underlay network with low latency slice, ARN Y is preallocated for that slice

How: unique ARN X is assocciated with cloud access VPN on CPE; PE1 map the packets with ARN X to Y, and then onto low latency slice.

Note: ARN X represents cotract with subscriber; ARN Y represents network slice
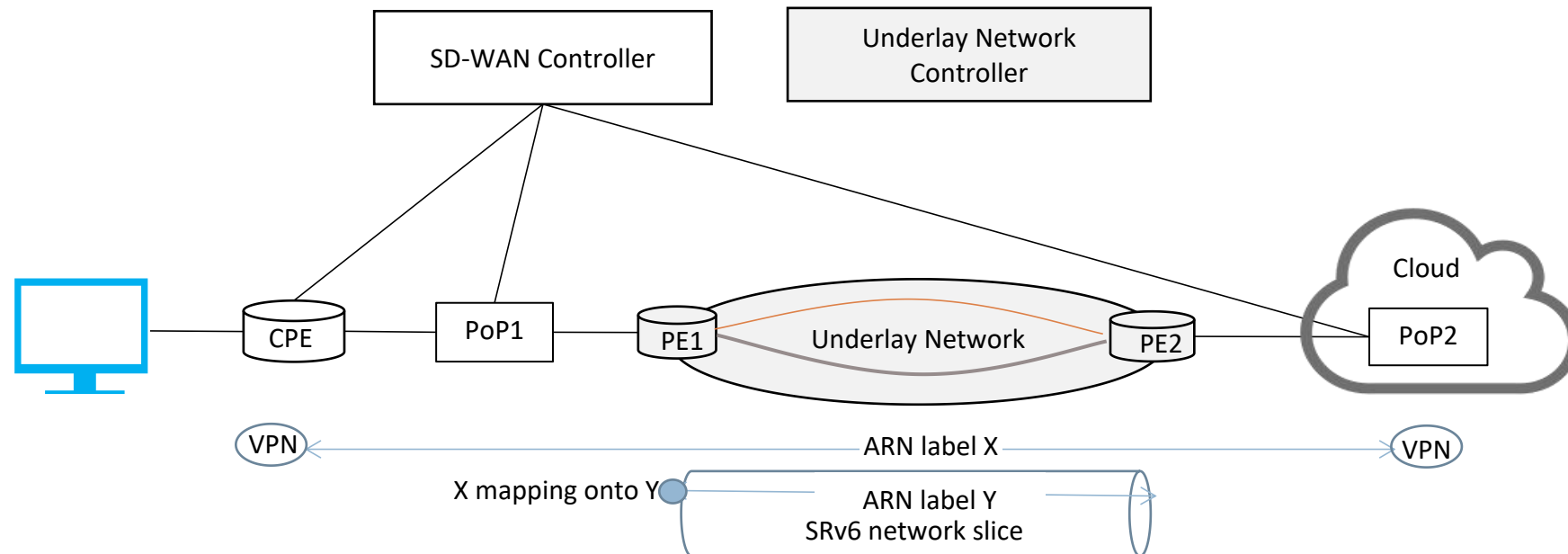
More thoughts

- Privacy:

  - customer privacy (e.g. app infor, personal privacy) is not awared

  - network provider credential information(e.g. topology, slice exposure) is not exposed

- Scalebility

  - Aggregatable, N labels can be mapped to 1 label

- Security

  - Easily to do ARN label access control

Questions?