Introduction to APN

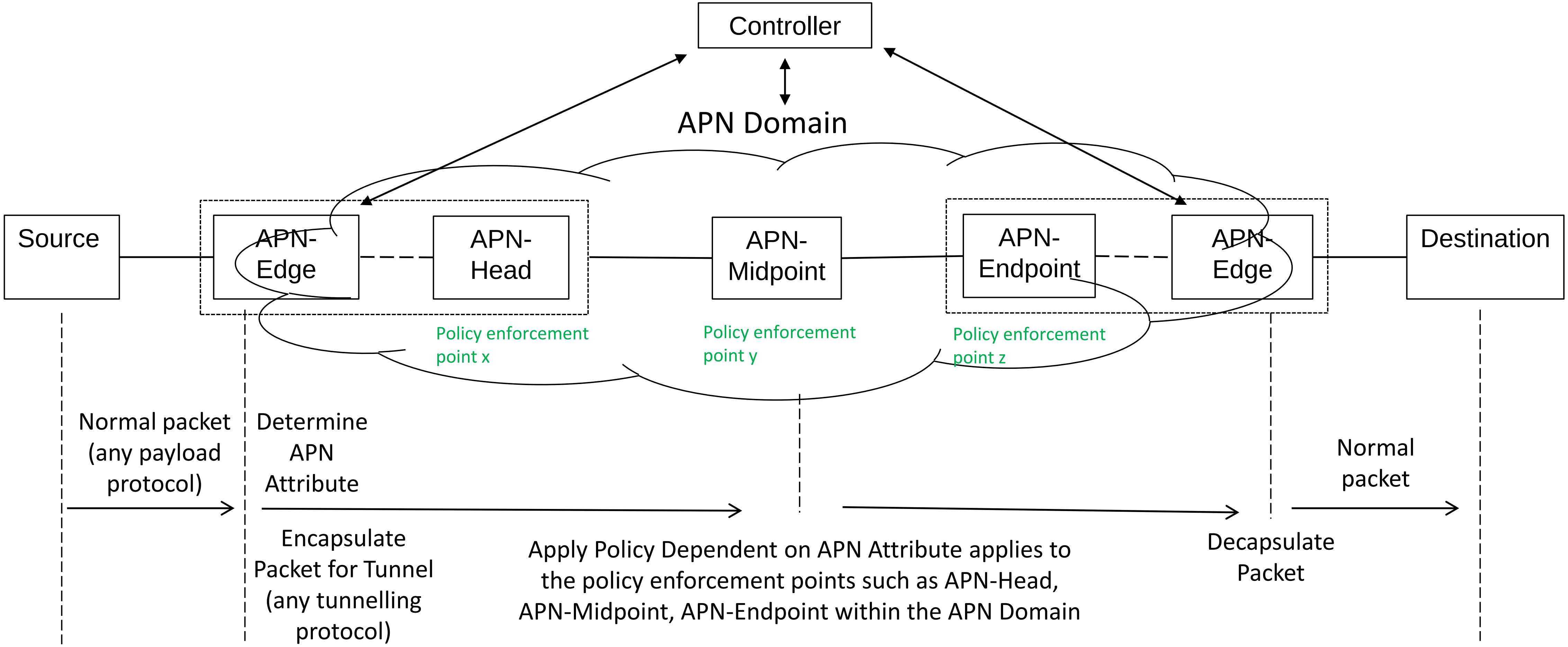
Zhenbin Li

10 mins + 5 mins questions (30/120)

What is APN?

- Application-aware Networking (APN) is a framework, where
  - an APN attribute is introduced at network edge devices
  - the APN attribute is structured with fields
  - the APN attribute is carried along with the tunnel encapsulation for policy enforcement on the nodes within an APN domain
- In short, APN:
  - classifies a packet at ingress to the APN domain (5-tuples, QinQ, ...)
  - encapsulates the packet into a tunnel header with an APN attribute
  - routes, processes, and forwards the packet within the network using policies dependent on the APN attribute
  - decapsulates the packet on egress (i.e. remove outer tunnel encapsulation)
- Privacy is important!
  - The APN will not depend upon being able to determine users' identities or which applications they are running by inspection of packet headers
  - The working group must not publish any specifications that risk violating user privacy

A simple reference diagram



An APN Domain may span multiple network domains controlled by the same operator

How does the edge node set the APN Attribute fields?

- The edge node must be configured/programmed to map from packet fields to a structured APN Attribute

- The edge node may look at all of the usual fields
  - 5-tuple, QinQ (S-VLAN, C-VLAN), port, etc.

- This is a one-off cost at the edge and does not need to be repeated at transit nodes
  - They just look at the APN Attribute

- If the packet is already encrypted some fields may not be accessible
  - The edge node may be configured to use only the fields available
    - APN function may be reduced since only 2-tuple (S/D IP address) are available
    - But still other information such as access ports or QinQ (S-VLAN, C-VLAN) can be used for APN based on configurations

How do the network nodes know what to do?

- The policy enforcement nodes within the APN domain apply policies to packets based on the APN attribute

- The operator of the APN domain configures the mapping from APN attribute to polices at each policy enforcement nodes

- Methods could include:
  - Configuration at each node (such as CLI)
  - Programming from a central management station (YANG or SDN)
  - Distribution using control plane protocols

The Goal of APN

1. The APN attribute allows the network devices to only look at one easily-accessible field in the tunnel header
   - 5 tuples vs. 1 tuple
   - Not having to resolve the 5 tuples of the original packets that are deeply encapsulated in the tunnel encapsulation

2. The APN attribute allows to simplify the policy control at every policy enforcement point within the network
   - The APN attribute allows to reducing each matching entry of policy filter since it is only one field and hardware resources are saved
   - Since APN attribute is relatively stable it introduces the possibilities of eliminating the “stale” policy filter entries
   - In most cases, the APN attribute is centralized configured and distributed to all the policy enforcement points, which saves the policy filter configurations per node and simplifies the O&M

3. The structured APN attribute allows to express fine granular service requirements
   - e.g. MKT-user-group/app-group, R&D-user-group/app-group, latency

4. The structured APN attribute allows to match to the evolving fine granular differentiated network capabilities
   - e.g. SR policy with low latency and high reliability guaranteed

Thank you!