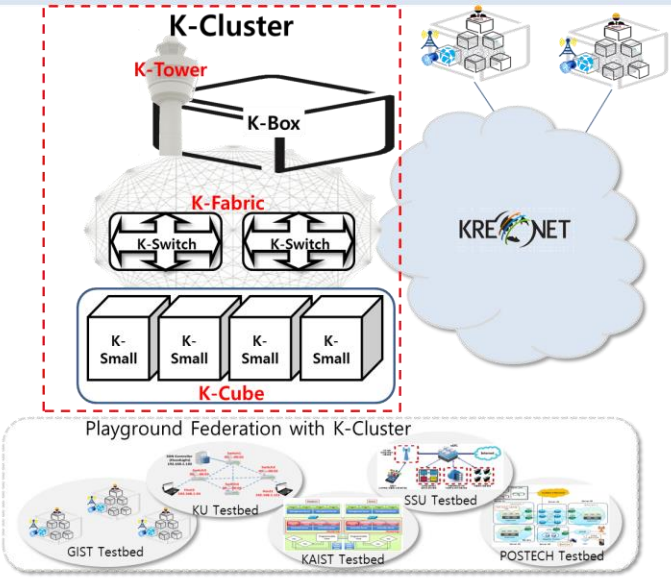
Network-aware Service Mesh for across Multi-site K-ONE Playground

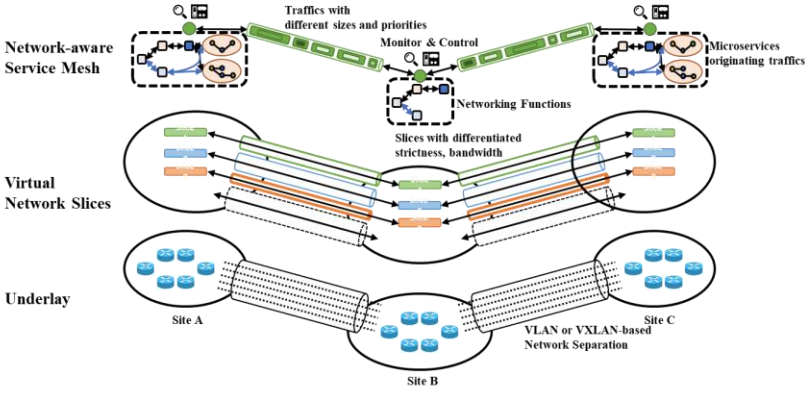
NetCS Lab. (Networked Computing Systems Laboratory), GIST
Moonjoong Kang, Junshik Shin and JongWon Kim
{mjkang, jsshin, jongwon}@nm.gist.ac.kr

K-ONE Open Playground: K-Cluster-centric Playgrounds Federation



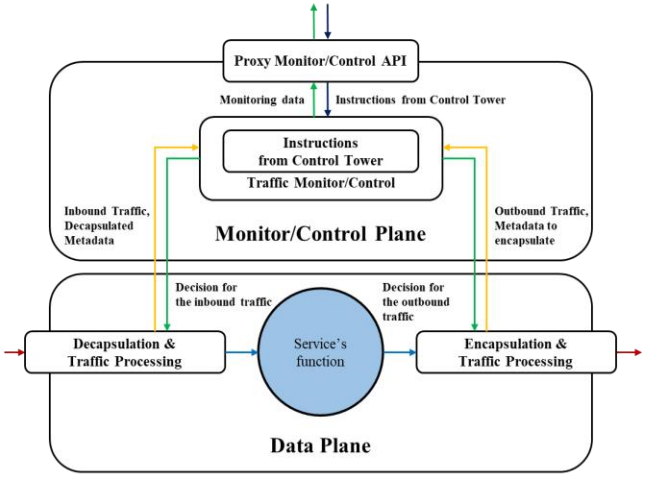
- K-Cluster
  1) Small-sized cluster testbed for SDN/NFV/Cloud
     - Flexible, economic logical testbed model which correspond to Edge-Cloud model, not physical configuration with fixed definition of HW, specification, model
  2) Characteristics
     - Software-based monitor & control automation
     - No vender-specific open hardware boxes
     - Networking that guarantees high-level stability/flexibility/bandwidth interconnect
     - One hardware bundle that handle various SDI verification
     - Economic Small testbed environment for researchers and developers who hard to obtain such environment
- K-ONE Playground
  1) Single K-Cluster has its limits for Multi-site/Domain-related verification
  2) K-Cluster prototypes are distributed to multiple K-ONE Consortium sites, including GIST, KU, SSU, POSTECH, KAIST, and interconnected over KOREN/KREONET to form K-ONE Playground

Network-aware Service Mesh



- Traffic network slice interchange or processing at intermediate node
  - Intermediate nodes keep interchanging neighbor node's network status info and monitoring inter-node network status
  - It evaluates how the traffic's QoS is satisfied and select the next-hop network slice for it and send the traffic through it
- Security Enforcer
  - From Intermediate nodes, Security Enforcer will check the traffic's encryption and ACL filtering
  - Plaintext traffics will be encrypted by Security Enforcer and re-transmit it, and the recipient's Security Enforcer will decrypt it back to plaintext, offloading the service's need for encryption

Network-aware Service Mesh Proxy



- Encapsulation/Decapsulation
  - Encapsulation/Decapsulation to provide separation between Monitor/Control Plane and Data Plane
  - During Encapsulating traffic, the metadata used by Network-aware Service Mesh is embedded into the traffic
  - Decapsulation detaches the metadata and send it to the proxy's Monitor/Control Plane part and sends the original traffic to function. Therefore no Monitor/Control traffic reaches the function at any form, resulting complete separation of planes
- Point of Monitor/Control of traffic
  - The policy for inbound/outbound traffic is downloaded from centralized control tower and the proxy processes the traffic by it
  - Traffic Monitoring data like request rate, success rate, delay time, response size are collected and sent to the control tower