Service Function Chaining Interface for Cloud Network Collaboration(CNC)

draft-sfc-interface-of-cnc-00

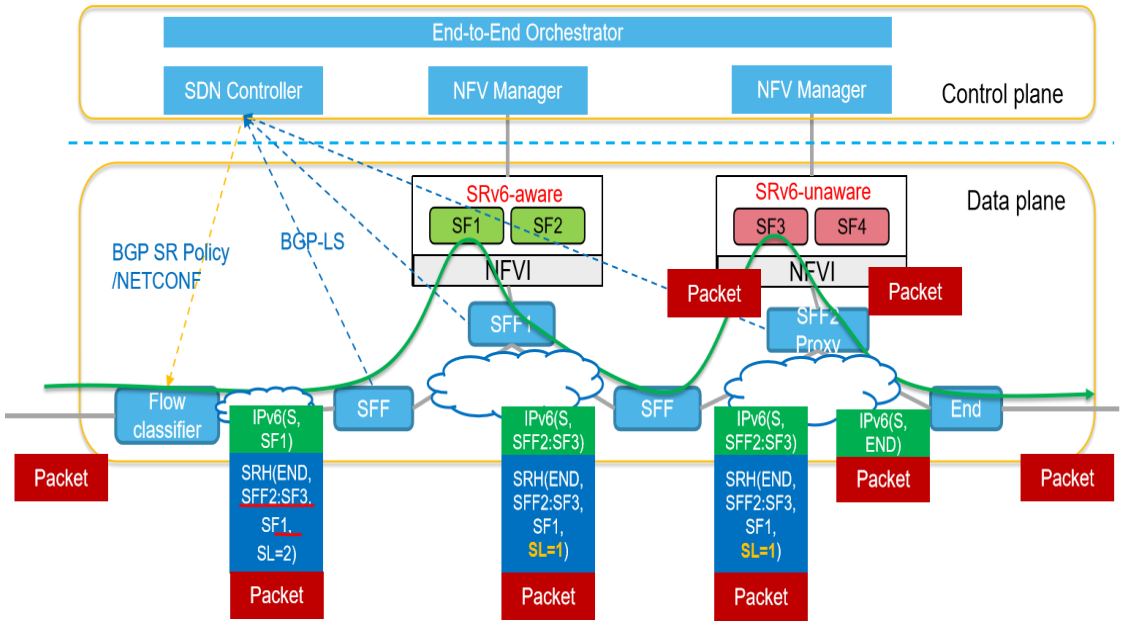
Pang Ran (China Unicom)

Yi Xinxin (China Unicom)

NeoTec@IETF-121

SRv6/SFC Utilization in CNC

RFC 7665 proposes the Service Function Chaining (SFC) architecture, and RFC 8300 proposes the Network Service Header (NSH) as the encapsulation to implement the SFC architecture.



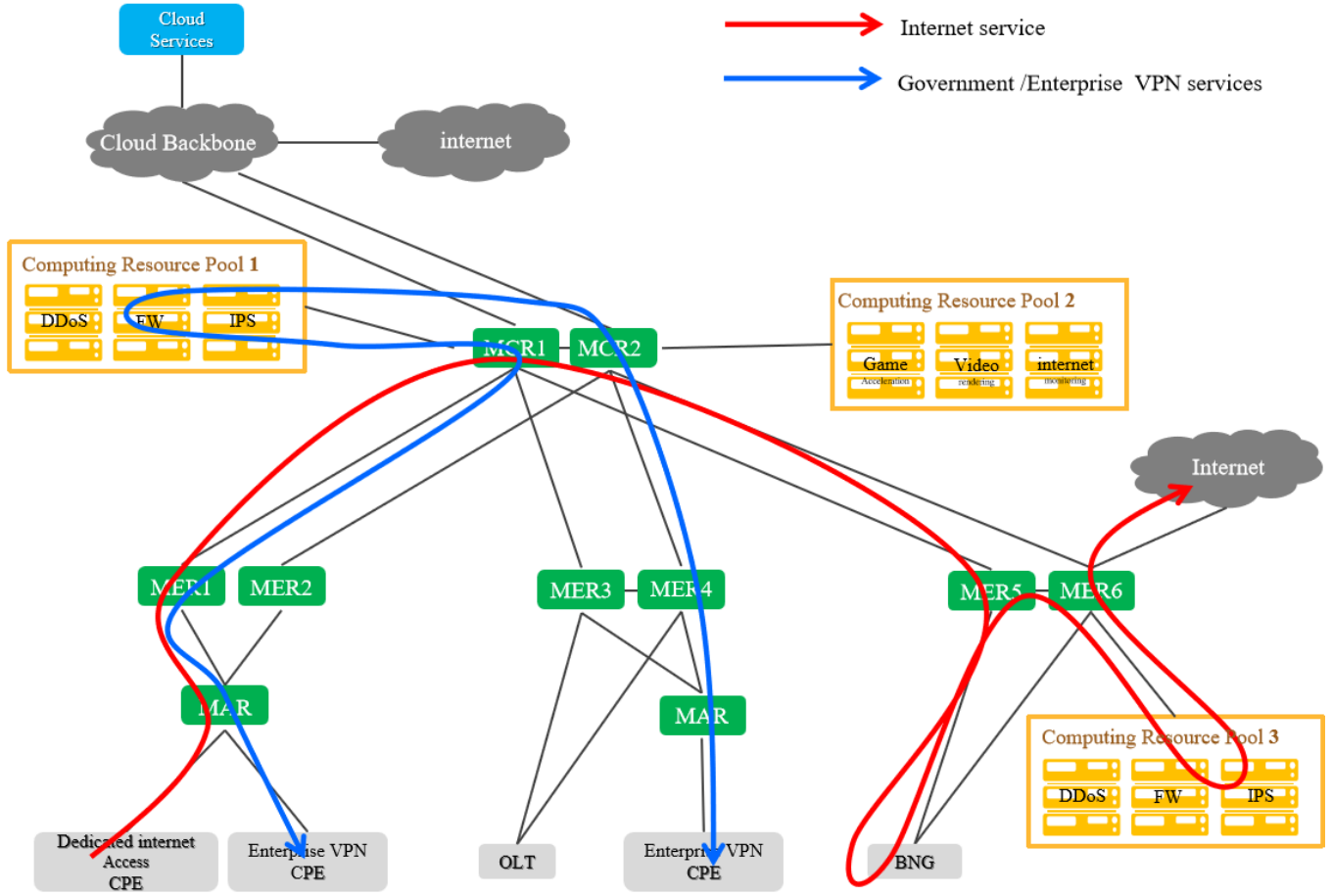
Why SRv6 is naturally suitable for SFC?

- The programmable path characteristics of SRv6 highly match the service sequence requirements of SFC.
- SRv6 can embed network functions into segments, which means that service function calls and path forwarding can be closely integrated.
- SRv6 has excellent cross domain support capability, which can support the construction of service chains between different network regions.

Enhanced Leased Line Service

☐ Main features

- **Quick and on-demand:** Providing on-demand and fast security services on the basis of the existing leased line. Factors such as security resource, pool load and service delay need to be taken into account when selecting security services.
- **Flexible Adjustment:** Users service can be adjusted without awareness of when the security service requires type change/capability change.
- **Low cost:** The upgrade of private line services does not require the replacement of security services/equipment in cloud centers.



Use Case

- With the SRv6+SFC service chain, TSP(Telecom Service Provider) can flexibly forward attack traffic between provincial cleaning cloud centers **(31 provinces)** and high-defense centers **(5 regions)**, achieving comprehensive defense against DDoS attacks.

➢ **D1 Router Traffic Steering:**

Router D announces detailed routes to the metro CR via BGP, which then sends LSPs to D1.

➢ **Traffic Cleansing:**

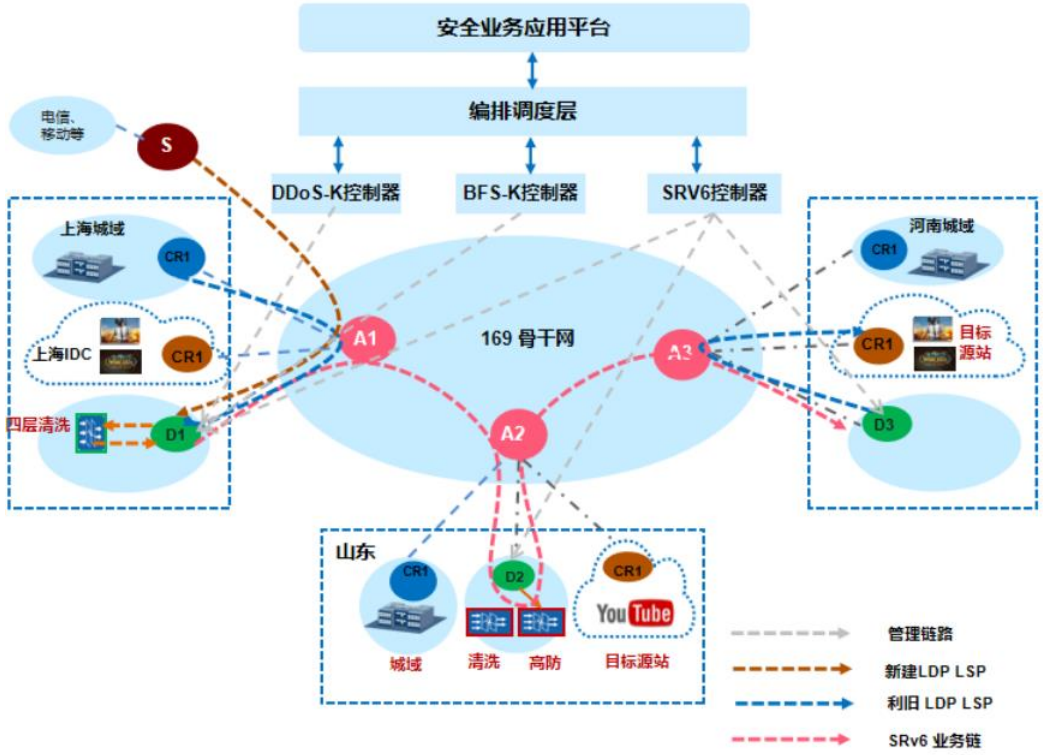
Router D directs traffic to cleaning functions in cloud centers, which return cleansed traffic to D via a local VPN re-injection.

➢ **Attack Source D--->Target Defense--->Target Source D:**

Establish service tunnels to steer traffic intended for the target source (within VPN) to the SRv6 service chain tunnel using BGP FS, then deliver it to the target source D.

➢ **Target Source D--->Target Source:**

Reuse existing public LSPs to forward traffic to the target source.

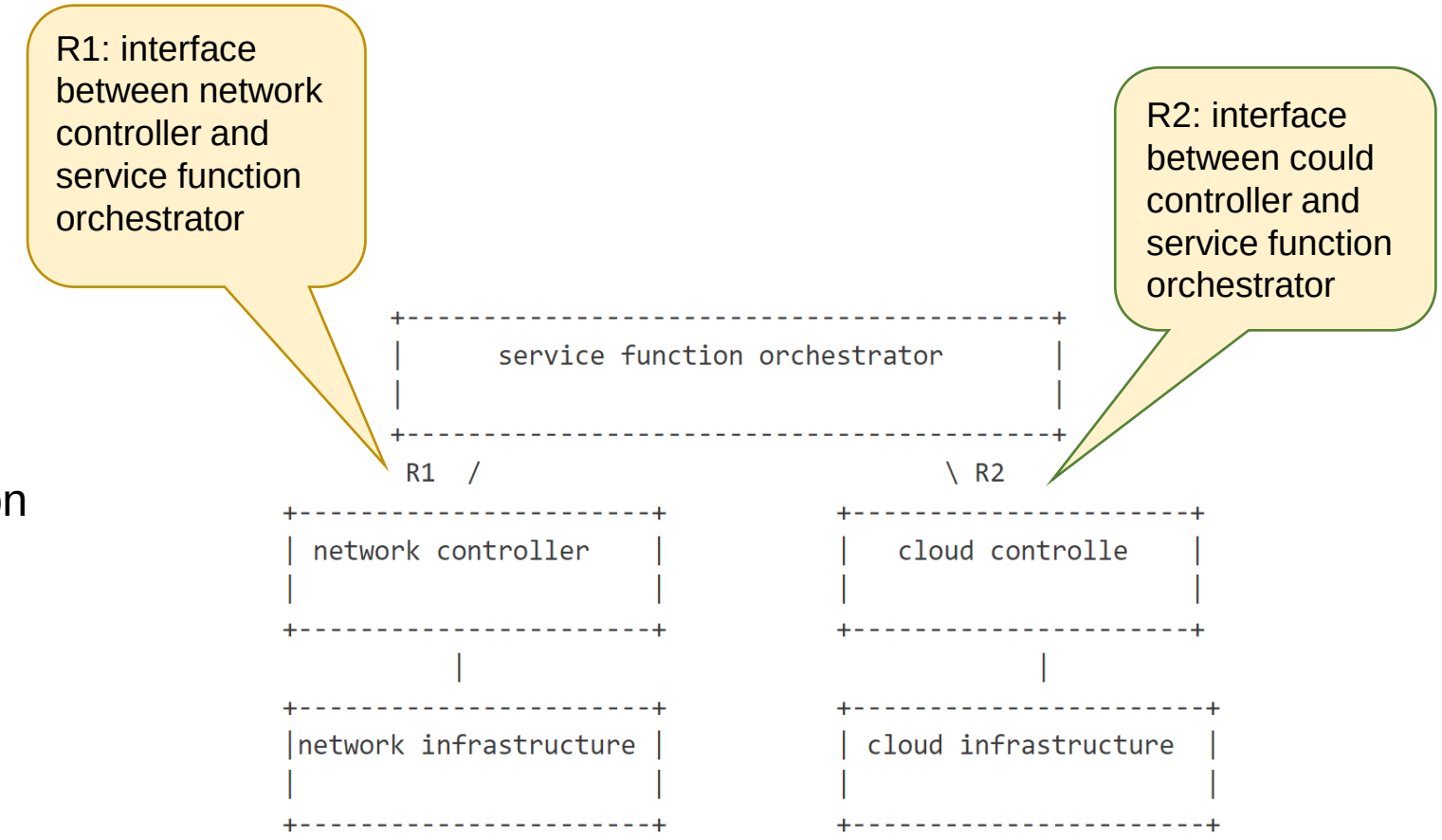


Challenges and Suggestions

- **High Demand:** Stringent requirements for cloud-network orchestration highlight the necessities of the standardization on key interfaces and resource models.
- **Fault Localization:** Challenges in fault localization arise from a dearth of diagnostic tools for cross-cloud networks.
- **SRv6 Support Limitations:** Limited SRv6 support at the cloud-side necessitates the use of SFC proxy methods, which introduces efficiency and other challenges.
- **SFC Adjustment Limitations:** The inadequacy of SFC’s dynamic adjustment capabilities leads to a reliance on static proxy methods in the current network, which can not fully meet the demand of security services in clouds.

Interface Requirements for SFC in CNC

- R1 interface requirements
  - Network resources information
  - Network path information
  - Network path adjustment
  - ……
- R1 interface requirements
  - Computing resources information
  - Scaling service funtoin information
  - Computing resource change
  - ……



Comments and suggestion are welcome

Thank you!