IETF 97
Seoul, South Korea
ODL SFC, Implementing IETF SFC
November 14, 2016

Brady Johnson
ODL SFC Project Technical Lead
brady.allen.johnson@ericsson.com
OpenDaylight SFC Data Model

Service Function Chain (SFC)
- Abstract, ordered list of Service Function Types
  - ex: [DPI, FW, NAT, QoS]

Service Function Path (SFP)
- Concrete, directional details about an SFC
- Specific transport details (VxLAN-GPE+NSH, Eth+NSH, etc)
- Optionally specify concrete Service Functions and Service Function Forwarders

Rendered Service Path (RSP)
- The actual service chain, combining info from the SFC and SFP
- Includes dynamic runtime representation of SFP resulting from load balancing and/or failover

Service Chaining Classification
- Map subscriber/tenant traffic flows to Service Chains
- Applies Service Chain Encapsulation (NSH)
- Uses IETF ACL matching for traffic flow matching

OpenDaylight SFC Use Case: SF Reclassification and branching

Reclassification:
P2P/BitTorrent ⇒ Blue
HTTP ⇒ Red

ODL-SFC
Re-Classify Feedback
Update/Create Service Chains
Classification Rules
SFF br-int
Classifier
Classifier
Internet
Service Chaining Encapsulation: Network Service Headers (NSH)

NSH encapsulated packets:
NSP: NSH Path, Chain ID
NSI: NSH index, Hop in chain
The shown NSI is after being decremented by the SF

Classify once:
Encapsulate Chain info with every packet

NSH-Aware Service Functions
(decrement NSI on pkt egress)

Original packets

SDN Network
NSH Header and transport details
As supported and implemented in ODL SFC

Example 1:
NSH encapsulated in VXLAN-GPE

Example 2:
NSH encapsulated in Ethernet

Service Path: The Service Chain ID
Index: The hop in the Service Chain
Optional Metadata
OpenDaylight: Just 1 piece of the puzzle

- ODL
- NFV
- OpenStack
- Linux
- OVS
- fd.io

• OPNFV: Integrating it all together
  • https://www.opnfv.org/
  • https://wiki.opnfv.org/display/sfc/Service+Function+Chaining+Home
OPNFV SFC

Legend

- Yellow: VxLAN tunnel SF/SFF
- Green: OpenFlow 1.3/OVSDB
- Blue: Classifier encaps VxLAN-GPE NSH
- Blue and black: Original packets, no encap
IETF SFC RFC: future focus areas

- Terminating SFPs and handling SFP egress
  - rfc7665 - Section 4.3, point 2
  - The specification mentions that the last SFF should remove the SFC encapsulation and send the packets back to the network.
    - This could be done by any “SFC egress boundary node”, and should not be required to be performed only by the last SFF.
  - It's not always feasible for the last SFF to know what to do with the original packet.
  - When using GBP and Netvirt classifiers in OPNFV SFC, the “egress classifier” removes the SFC encapsulation, thus acting as an SFC egress boundary node
    - In OPNFV SFC, if the packet is sent back to the network (OpenStack br-int bridge) without the SFC encapsulation, and it enters the classifier again, then there will be a loop
Proxy Service Functions
  - TCP Proxy
    - How to handle the case when the SF generates traffic?
    - The SF terminates the TCP connection with the client and establishes another with the server
  - Transparent Cache
    - How would this work with reclassification?