An Architecture for Network Function Interconnect

draft-bookham-rtgwg-nfix-arch-01

C. Bookham, A. Stone, J. Tantsura, M. Durrani, B. Decraene
Presenter: W. Henderickx

An Architecture for Network Function Interconnect

Introduction

- With the introduction of 5G, IoT, and Industry 4.0, service requirements are changing.
  - Besides ever-increasing demand for more capacity, there is demand for ultra-reliable and/or low-latency communication.
- Dealing with SW based workloads/Network Functions – NFV (network virtualization)
  - Besides Physical network functions (PNF), we have to interconnect VNF(s), that are deployed through DC infrastructure
- Service edge boundary is changing – functions that were reasonably centralized are being distributed
  - i.e. to deal with low latency requirements, or to reduce costs

This draft introduces an architecture framework that deals with all of this

NFIX: Network Function InterConnection (INFORMATIONAL)

An Architecture for Network Function Interconnect

Terminology

- PNF: A physical network function (PNF) refers to a network device such as a Provider Edge (PE) router that connects physically to the wide-area network
- VNF: A virtualized network function (VNF) refers to a network device such as a provider edge (PE) router that is hosted on an application server. The VNF may be bare-metal in that it consumes the entire resources of the server, or it may be one of numerous virtual functions instantiated as a VM or number of containers on a given server that is controlled by a hypervisor or container management platform.
- A Data Center Border (DCB) router refers to the network function that spans the border between the wide-area and the data center networks, typically interworking the different encapsulation techniques employed within each domain.
- An Interconnect controller is the controller responsible for managing the NFIX fabric and services.
- A DC controller is the term used for a controller that resides within an SDN-enabled data center and is responsible for the DC network(s)

An Architecture for Network Function Interconnect

Motivation

- As VNFs become part of the service landscape, the data-path must be extended across the WAN and into the DC.
- Historically these have been architected independently with some form of service-interworking at the DC border, which has limitations:
  - DC uses (i.e.) VXLAN/NVGRE while WAN uses (i.e.) MPLS – requires service interworking and decap/encap.
  - Requires heavy-touch service provisioning on the DC border.
  - Automation is difficult due to above, but with other contributing factors. Automation is a must have in a virtualization world!
  - Some or all of the above make service-interworking cumbersome with questionable scaling attributes.
- Need an open, scalable, and unified network architecture to bring together DC and WAN in an evolutionary way.

An Architecture for Network Function Interconnect

Proposal

- Allow for seamless connectivity between VNF to VNF, VNF to PNF, and PNF to PNF.
- Use seamless-MPLS as a baseline and build on that.
- Uses Segment Routing for construction of end-to-end LSPs (version 00 uses SR-MPLS dataplane, but does not preclude SRv6).
- Uses a centralized controller (Interconnect Controller)
  - Path computation and placement (SR policy).
  - Interfaces to other controllers that may reside in an SDN-enabled DC.
  - Logic is extended to be service-aware to correlate appropriate paths are used for the appropriate services.
  - Uses BGP-LS or BGP-LU to learn the topologies of DCs and WAN.
  - Understand real-time state using IPFIX, Netconf/YANG, telemetry, BGP-LS, BMP...

An Architecture for Network Function Interconnect

Routing and LSP Underlay

- Wide-Area Network Domain
  - Default forwarding path is shortest path SR and BGP-LU (seamless MPLS) if WAN is constructed from multiple domains.
- Data Center Domain
  - Uses RFC 8663 or native SR-MPLS/SRv6. Allows for good entropy and allows for a lightweight interworking function at DC border.
- Inter-Domain
  - Default forwarding path is BGP-LU resolved to SR/SRoUDP (DC) and IGP/SR (WAN).
  - TE path is SR Policy computed and advertised by Interconnect Controller (color is important!).
  - For SR-TE LSP, DC border is always BSID anchor – reduces number of segments/labels, but also allows for removal of heavy midpoint provisioning at DC border.

```
 +---------------+  +----------------+  +---------------+
 | Data Center 1 |  |   Wide-Area    |  | Data Center 2 |
 | +----+       +----+      3       +----+       +----+ |
 | |VNF1|       |DCB1|-1   / \   5--|DCB2|       |VNF2| |
 | +----+       +----+ \ /   \ /   +----+       +----+ |
 |               |  |    2     4     |  |               |
 +---------------+  +----------------+  +---------------+
 SR Policy      SR Policy
 BSID m         BSID n
{DCB1,n,VNF2} {1,2,3,4,5,DCB2}
```

An Architecture for Network Function Interconnect

Service Overlay

- Service layer uses EVPN and VPN-IPv4/IPv6 Address Families
  - BGP Next-Hop passed end-to-end and not modified by transit routers (including domain borders).
  - Complements the gateway-less architecture and requirement for midpoint provisioning.
- Interconnect controller computes end-to-end TE paths for each [headend, color, endpoint] as part of routing and LSP underlay.
- The collection of [headend, endpoint] pairs for the same color constitutes a logical network topology, where each topology satisfies a given SLA requirement.
- Interconnect controller discovers endpoints associated to a given topology (color) when receiving EVPN and IPVPN routes advertised by the endpoint.
  - TE topology can be coarse (i.e. per-VPN) or granular (VNF1=blue, VNF2=green).
- Mechanism allows for automated service activation.

An Architecture for Network Function Interconnect
Status

- draft-bookham-rtgwg-nfix-arch-01 (Informational)
- Open framework, build upon various work done in IETF
- Interworking of various vendors in live deployments
- Authors welcome feedback.