Integration of EVPN in Kubernetes

Frank Potter
Security and Network Engineering
University of Amsterdam

30 September 2019
Introduction

1. Multi-tenancy

2. Optimize resource utilization

3. Network policies
Figure 2: Kubernetes multi-tenancy. Source: A. Gerrard, 2019
Figure 2: Kubernetes multi-tenancy. Source: A. Gerrard, 2019
EVPN-VXLAN in the data center

- Ethernet Virtual Private Network (EVPN)
- Virtual Extensible Local Area Network (VXLAN)
- VTEP (Virtual Tunnel End Point)
- VNI (Virtual Network Identifier)
- MP-BGP (Multi-Protocol BGP)

Figure 6: EVPN-VXLAN architecture. Source: D. G. Dutt, 2018
MAC/IP advertisement
EVPN Route Type 2 (RT-2)

<table>
<thead>
<tr>
<th>MAC</th>
<th>IP</th>
<th>VNI</th>
<th>VTEP</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM11</td>
<td>VM11</td>
<td>100</td>
<td>1</td>
</tr>
<tr>
<td>VM12</td>
<td>VM12</td>
<td>200</td>
<td>1</td>
</tr>
<tr>
<td>VMn1</td>
<td>VMn1</td>
<td>200</td>
<td>n</td>
</tr>
<tr>
<td>VMn2</td>
<td>VMn2</td>
<td>300</td>
<td>n</td>
</tr>
<tr>
<td>VM22</td>
<td>VM22</td>
<td>300</td>
<td>2</td>
</tr>
</tbody>
</table>
● EVPN on the host
  ○ Free Range Routing (FRR) version 4.0, released in March 2018

● L3 Multi-tenancy

● EVPN-VXLAN in the data center
Research question

How can **EVPN** provide for **L3 multi-tenancy** in a **Kubernetes containerized environment**?

1. What advantages does EVPN have as a solution to allow for L3 multi-tenancy in a Kubernetes orchestrated container environment?

2. How can the recent improvements in FRR allow for EVPN to be integrated into the Kubernetes container orchestration platform?
RFC 7364 described that the network is not being able to support the increasing demand for server virtualization in data centers

- Gave insight in Network Virtualization Overlays (NVOs) that provide multi-tenancy to overcome this

Makowski and Grosso conducted an evaluation of virtualization and traffic filtering methods for container networking

- Compared EVPN and Identifier Locator Addressing (ILA) as NVO
Background - Calico

BIRD (BIRD Internet Routing Daemon)

Figure 3: Calico multi-tenancy. Source: N. van Noort, 2018
Figure 4: Cilium identities and labels. Source: N. van Noort, 2018
Cilium
Cilium

VXLAN overlay

Leaf

VNI 1000

VNI 2000

VTEP 1

L2 Overlay

VTEP 3

Server 1

Server 2

Server 3

Container 1
VLAN10

eBPF

Container 2
VLAN20

eBPF

Container 3
VLAN10

eBPF

VLAN

VLAN

VLAN

Figure 5: Cilium multi-tenancy. N. van Noort, 2018

eBPF (extended Berkley Packet Filter)
Methodology

- Requirements of multi-tenancy
- EVPN L3 multi-tenancy
- Architecture
- Integration of EVPN in Kubernetes
Evaluation - Requirements of multi-tenancy

  - Traffic isolation and address space isolation
  - Multiple different virtual networks
  - Scalability
  - Mobility
  - Optimal forwarding
Evaluation - EVPN L3 multi-tenancy

VRF (Virtual Routing and Forwarding)

- Traffic isolation and address space isolation (VRF)
- Multiple different virtual networks (VRF)
- Scalability (255 VRFs, 100 pods)
- Mobility (EVPN RT-2)
- Optimal forwarding (EVPN)

Figure 7: EVPN L3 multi-tenancy on the host
Evaluation - EVPN L3 multi-tenancy

FRRouting Release 7.1 Available for Download
July 30, 2019

bgpd:

- EVPN can now be configured in non-default VRFs.

Figure 7: EVPN L3 multi-tenancy on the host
No Network Policies!!

SVI (Switched Virtual Interface)

Figure 8: Architecture of EVPN L3 multi-tenancy
Results - Integration of EVPN in Kubernetes

CRoHDAd (Cumulus Routing on the Host Docker Advertisement daemon)

1. Schedule container
2. Create/delete container
3. Event container added/deleted
4. Host route added/deleted
5. Redistribute VRF table

Figure 9: Proof of Concept flow chart
Discussion

- **Security**
  - VRFs
  - Containers

Figure 10: Hypernetes. Source: H. Zhang and P. Ni, 2019
Conclusion

How can **EVPN** provide for **L3 multi-tenancy** in a Kubernetes containerized environment?

- **VRFs**
  - Tenant network isolation
  - Without network policies

- Importing Container IP addresses into FRR and advertising host routes with EVPN
Future work

- Performance comparison of EVPN
- Adding eBPF to EVPN
- CNI plugin (GO)
- Security of Hypernetes
- Maximum VRFs on the host
References


- D. G. Dutt, EVPN in the Data Center. O'Reilly Media, Inc., 2018.


Questions?