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
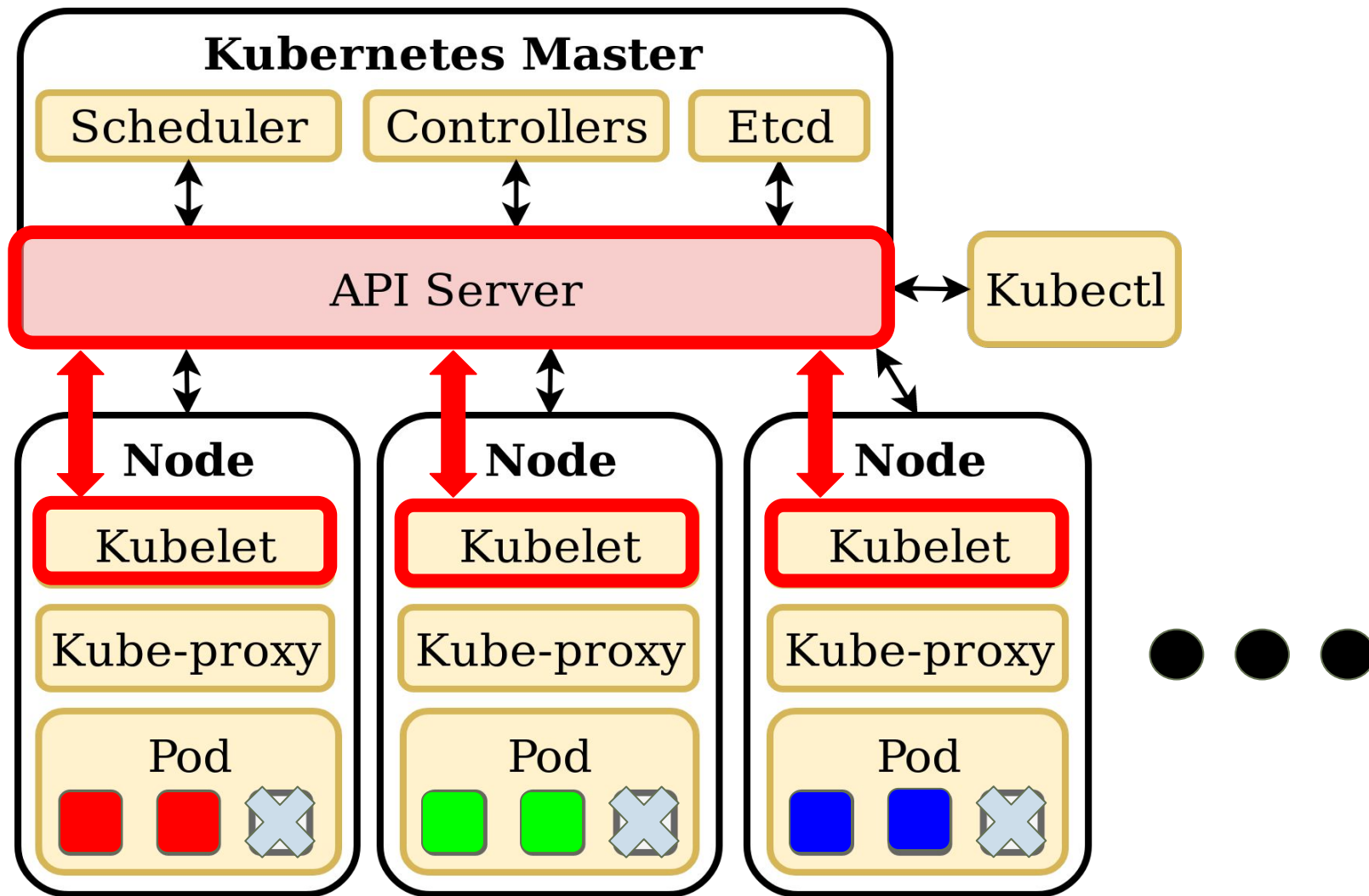
3. Network policies

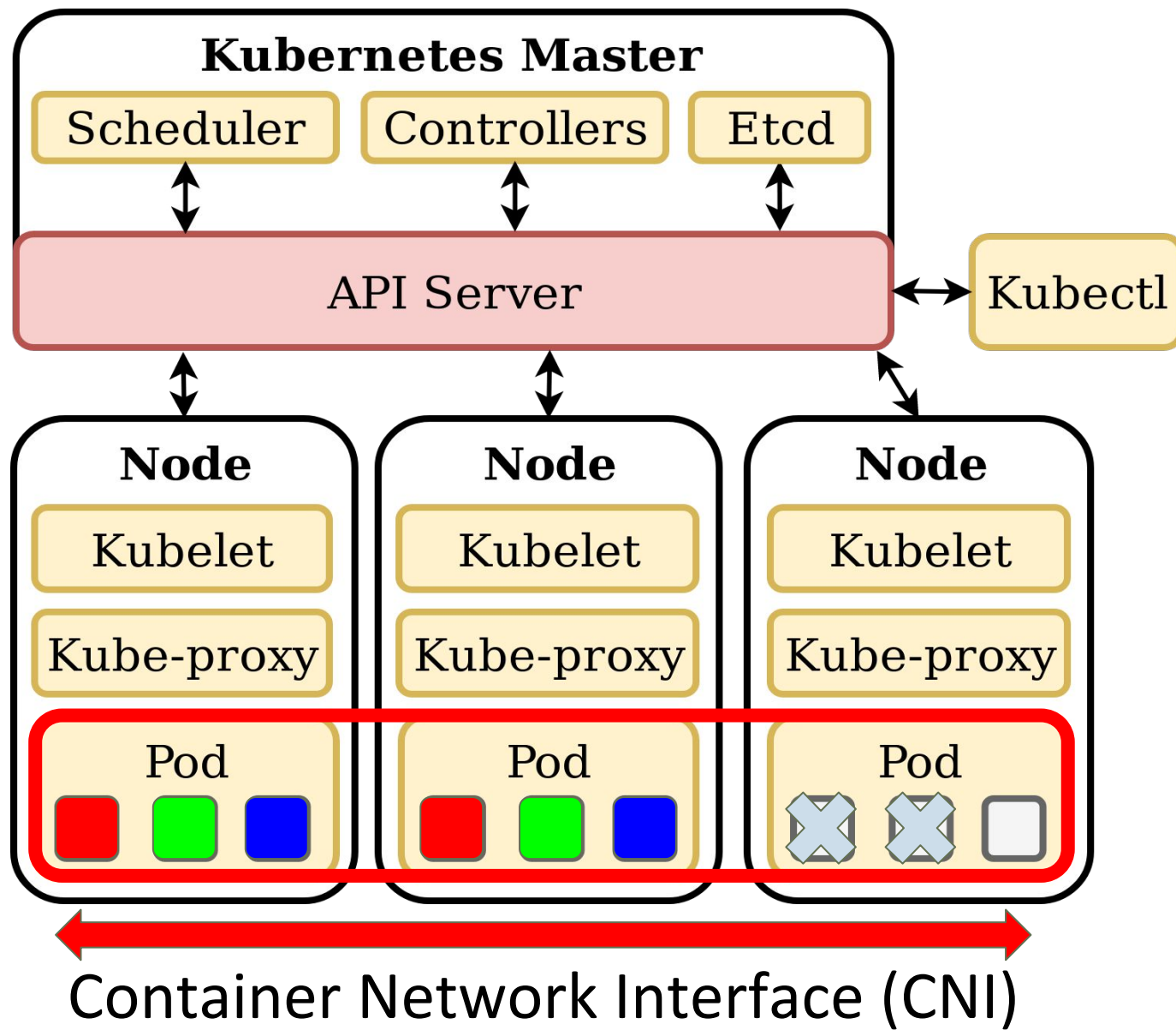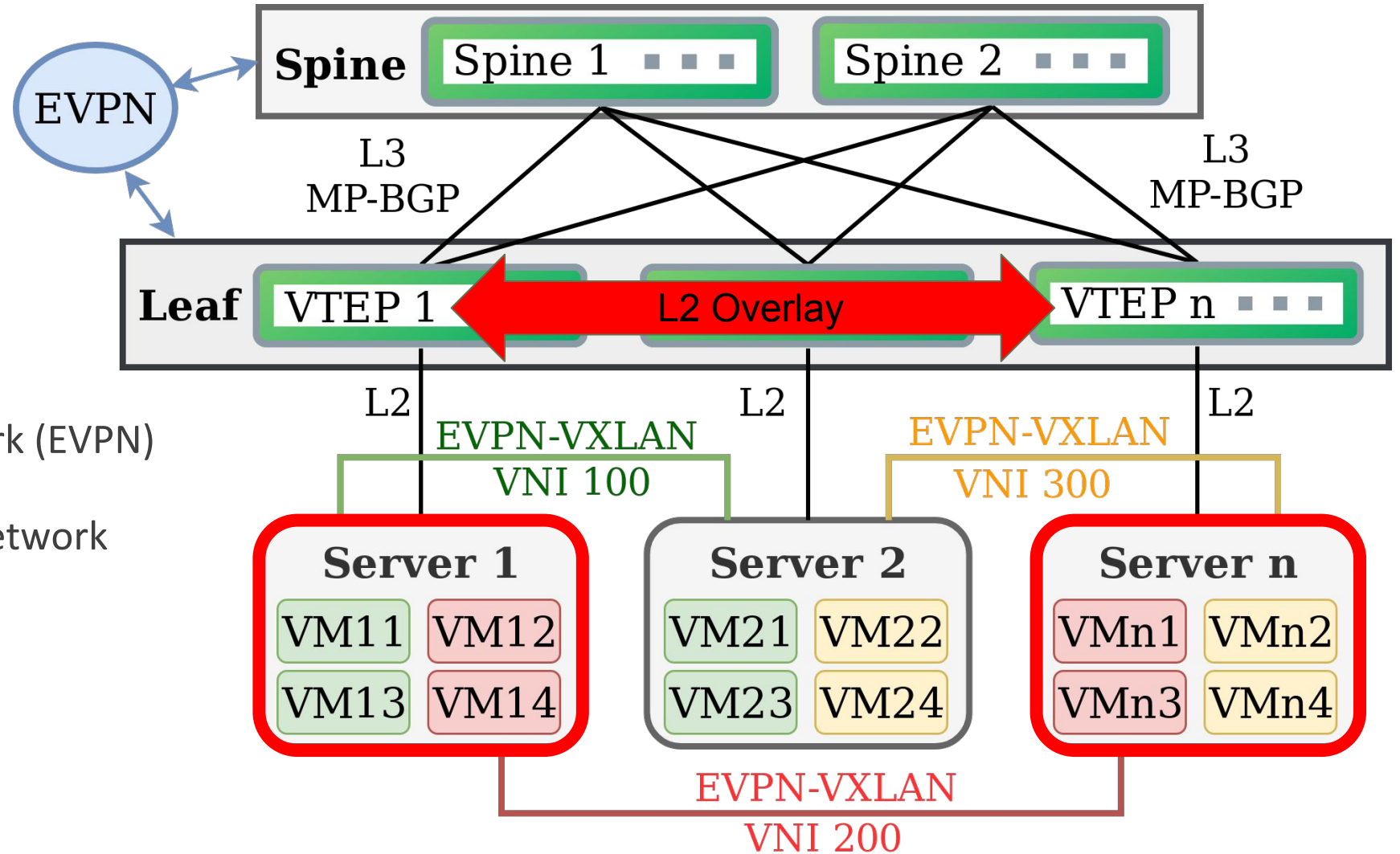Figure 2: Kubernetes multi-tenancy. Source: A. Gerrard, 2019

Figure 2: Kubernetes multi-tenancy. Source: A. Gerrard, 2019

EVPN-VXLAN in the data center

EVPN

Spine | Spine 1 ▪ ▪ ▪ | Spine 2 ▪ ▪ ▪

L3 MP-BGP

L3 MP-BGP

Leaf | VTEP 1 ← L2 Overlay → VTEP n ▪ ▪ ▪

L2

L2

L2

EVPN-VXLAN
VNI 100

EVPN-VXLAN
VNI 300

Server 1

| VM11 | VM12 |
| VM13 | VM14 |

Server 2

| VM21 | VM22 |
| VM23 | VM24 |

Server n

| VMn1 | VMn2 |
| VMn3 | VMn4 |

EVPN-VXLAN
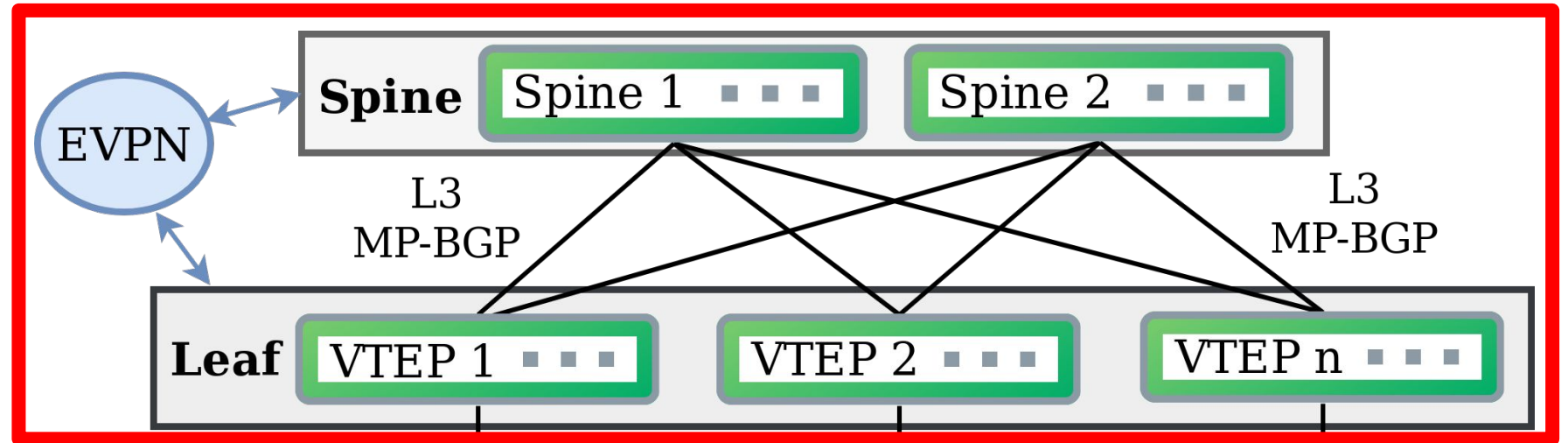VNI 200

Ethernet Virtual Private Network (EVPN)

Virtual Extensible Local Area Network (VXLAN)

VTEP (Virtual Tunnel End Point)
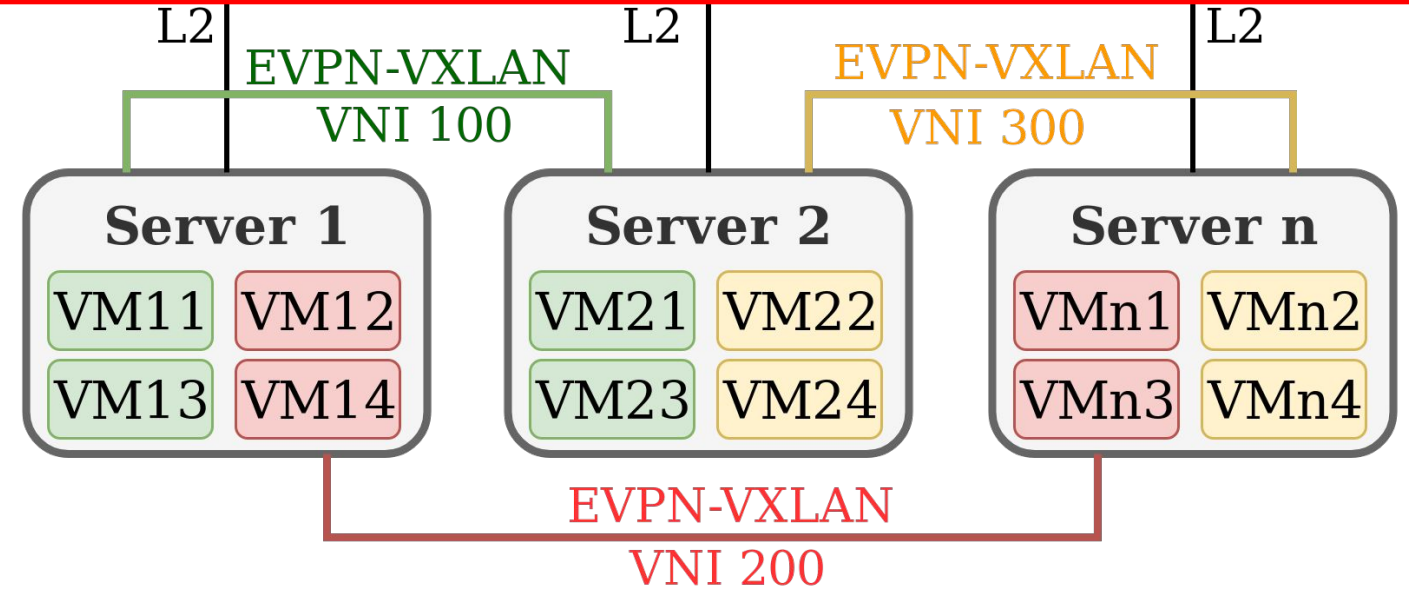
VNI (Virtual Network Identifier)

MP-BGP (Multi-Protocol BGP)

Figure 6: EVPN-VXLAN architecture. Source: D. G. Dutt, 2018

MAC/IP advertisement
EVPN Route Type 2 (RT-2)

MAC	IP	VNI	VTEP
VM11	VM11	100	1
VM12	VM12	200	1
VMn1	VMn1	200	n
VMn2	VMn2	300	n
VM22	VM22	300	2

- 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?

Related work

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
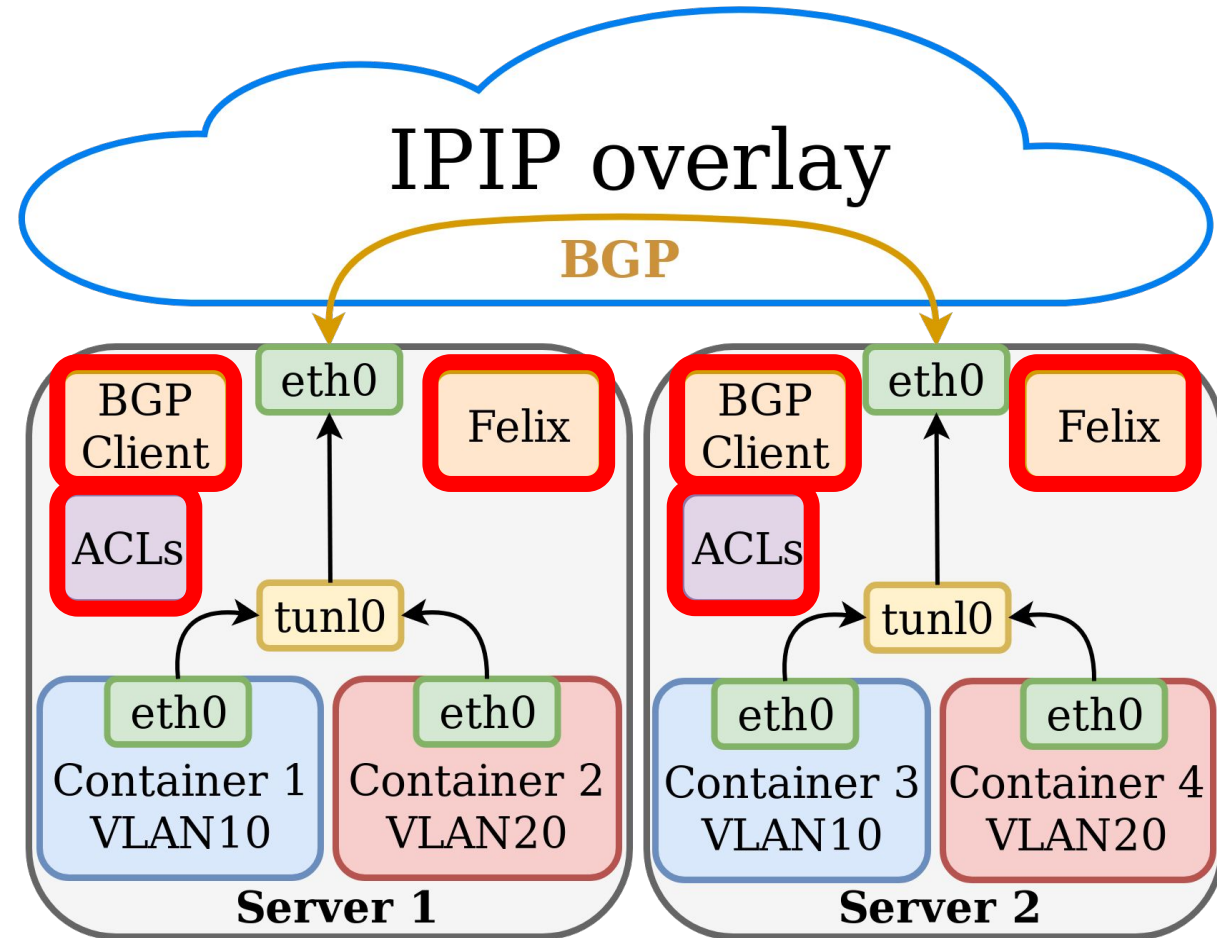
BIRD (BIRD Internet Routing Daemon)

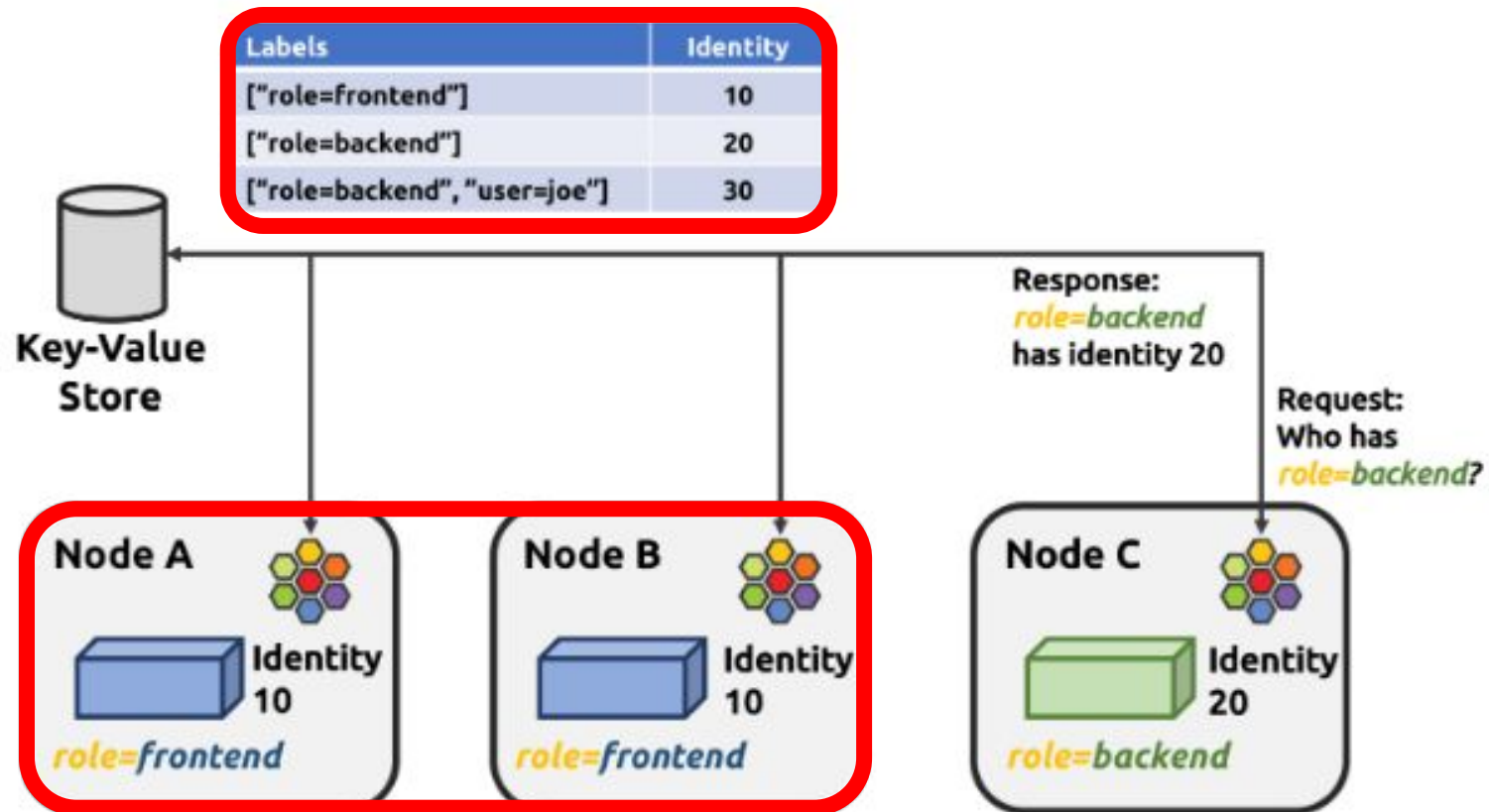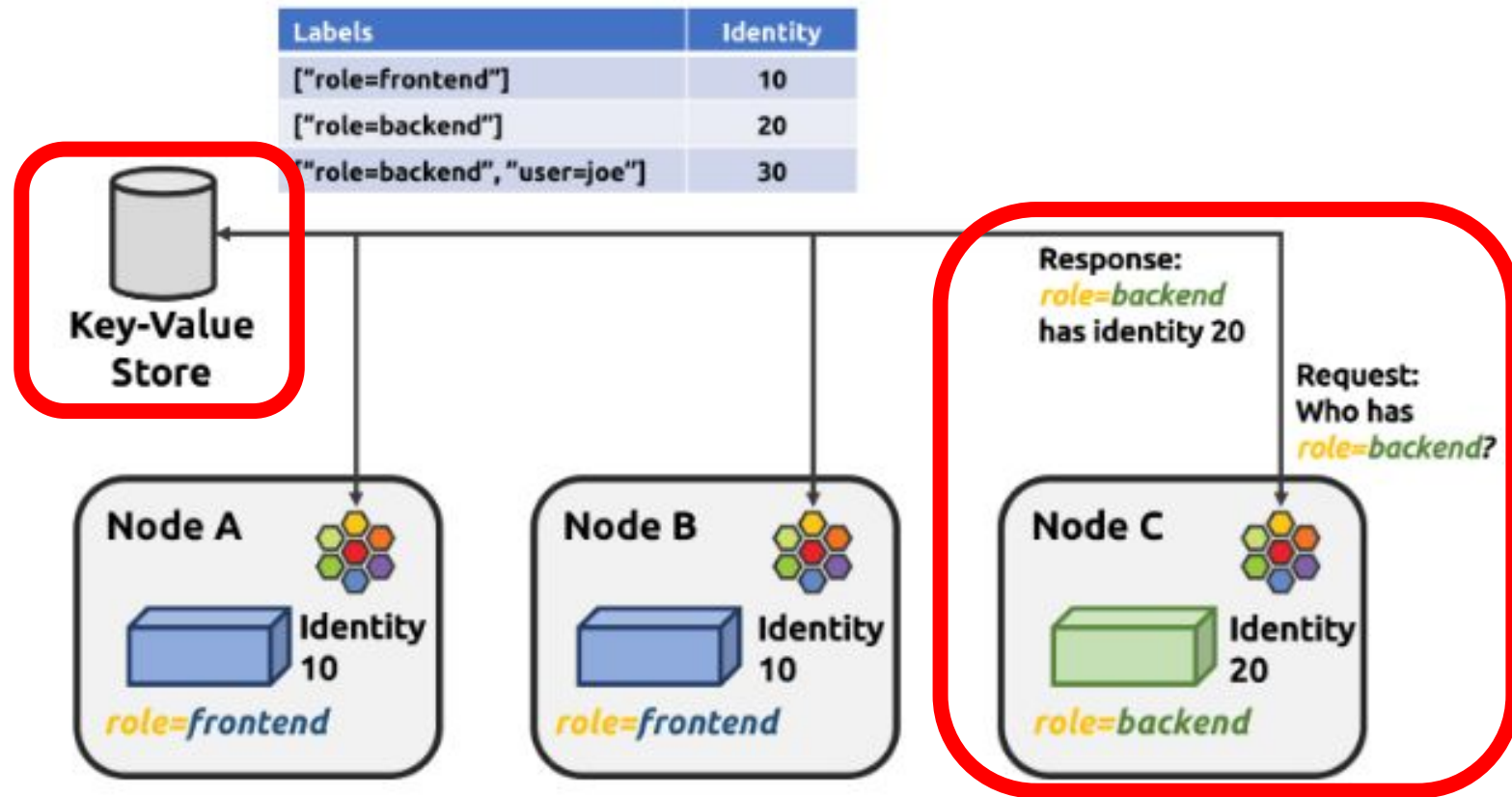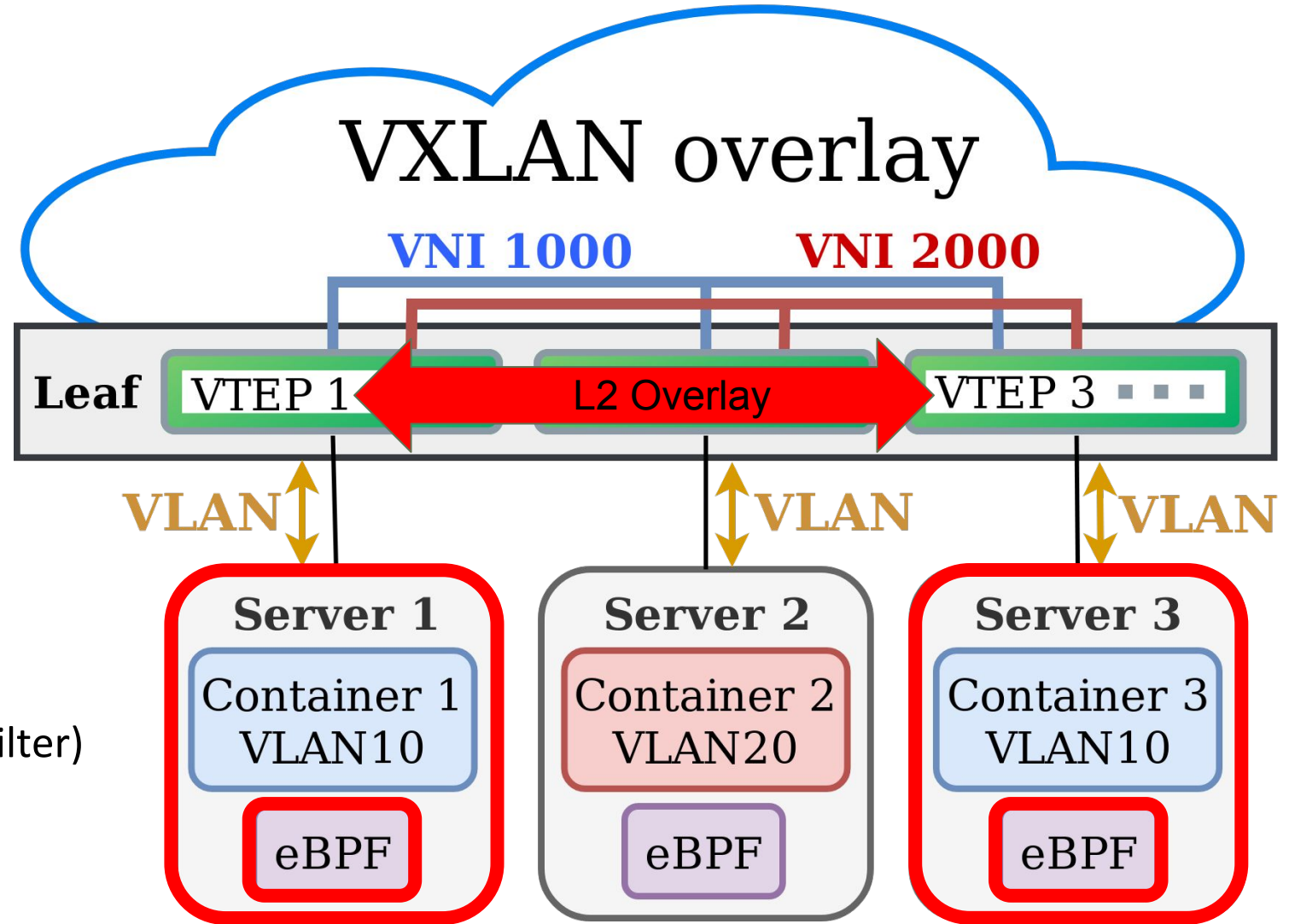Figure 3: Calico multi-tenancy. Source: N. van Noort, 2018

Cilium

Figure 4: Cilium identities and labels. Source: N. van Noort, 2018

Cilium

Cilium

eBPF (extended Berkley Packet Filter)

VXLAN overlay

VNI 1000 **VNI 2000**

Leaf VTEP 1 L2 Overlay VTEP 3 ▪ ▪ ▪

VLAN VLAN VLAN

Server 1
Container 1
VLAN10
eBPF

Server 2
Container 2
VLAN20
eBPF

Server 3
Container 3
VLAN10
eBPF

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

Methodology

- Requirements of multi-tenancy

- EVPN L3 multi-tenancy

- Architecture

- Integration of EVPN in Kubernetes

Evaluation - Requirements of multi-tenancy

- **RFC 7364 Problem statement: Overlays for Network Virtualization (Narten, et al. 2014)**

  - 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)
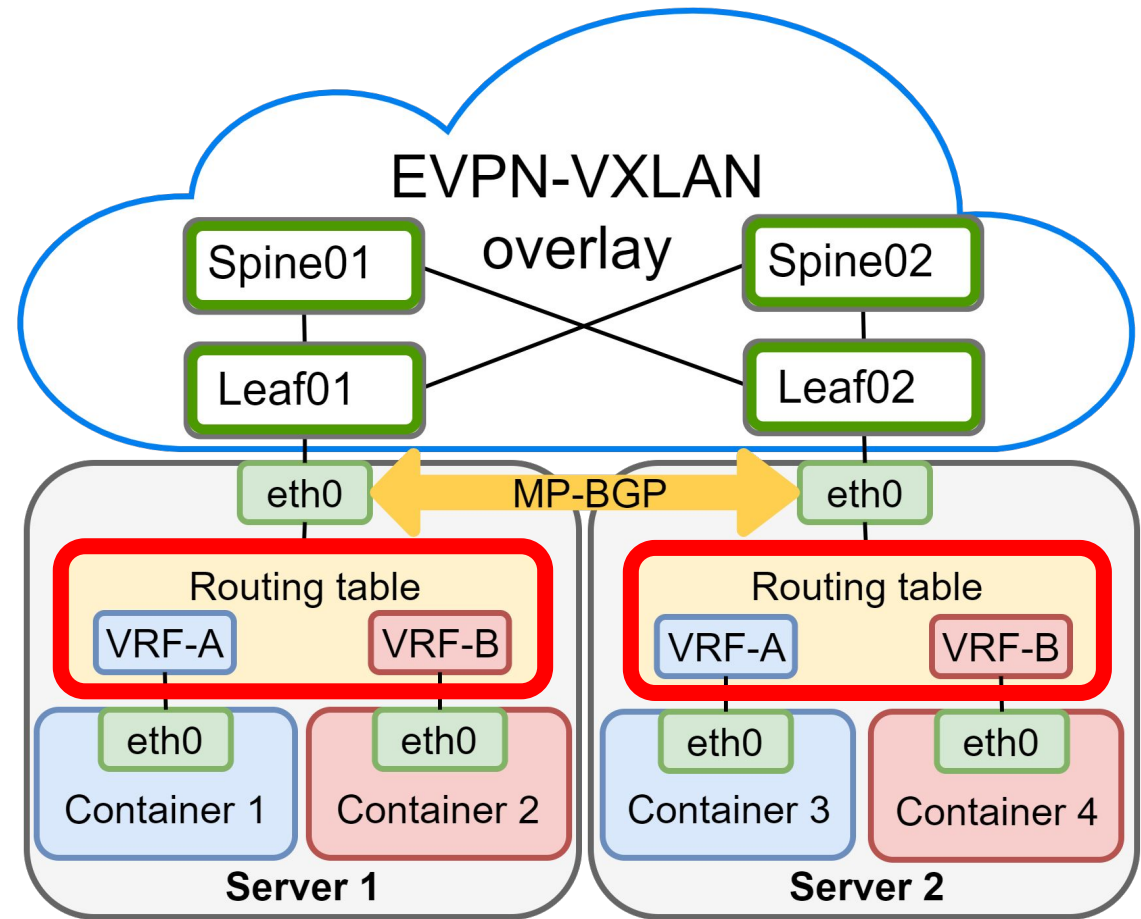
- Optimal forwarding (EVPN)

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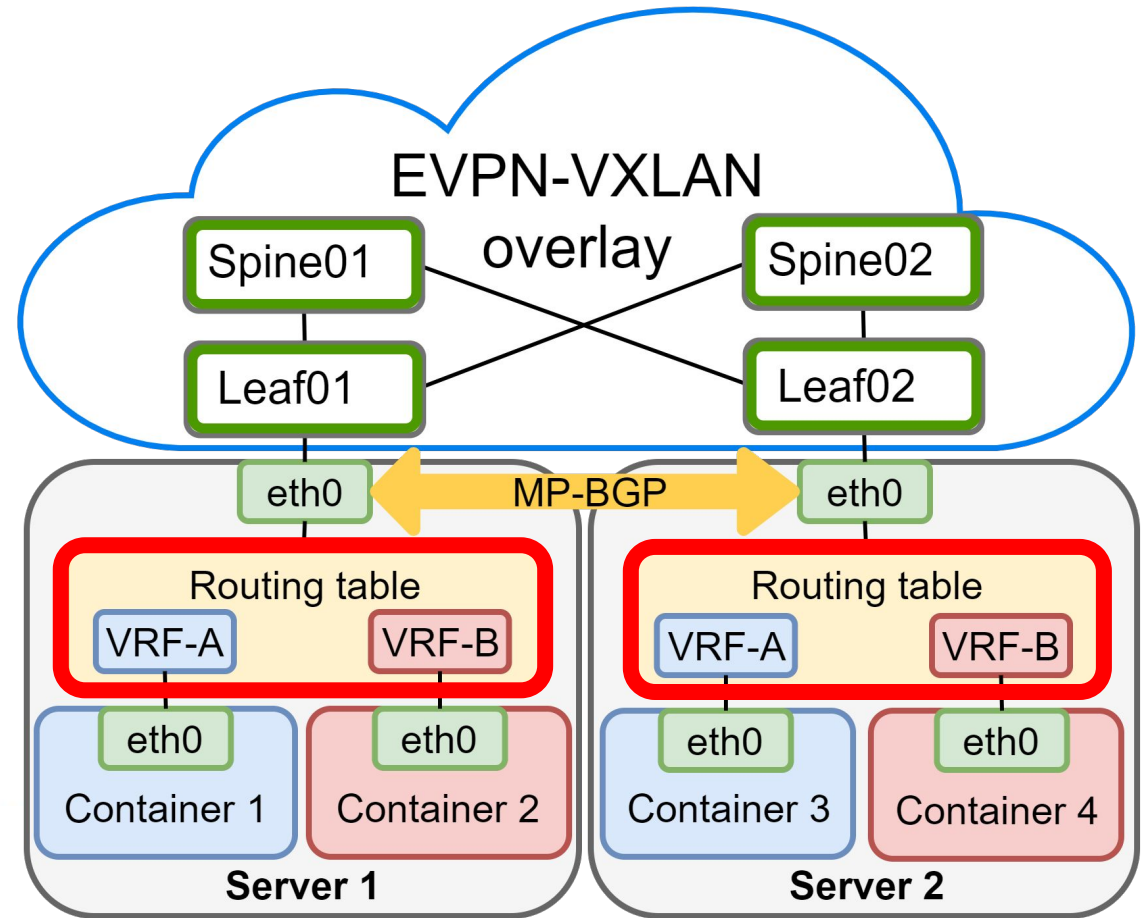
Evaluation - EVPN L3 multi-tenancy

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

Results - Architecture

No Network Policies!!

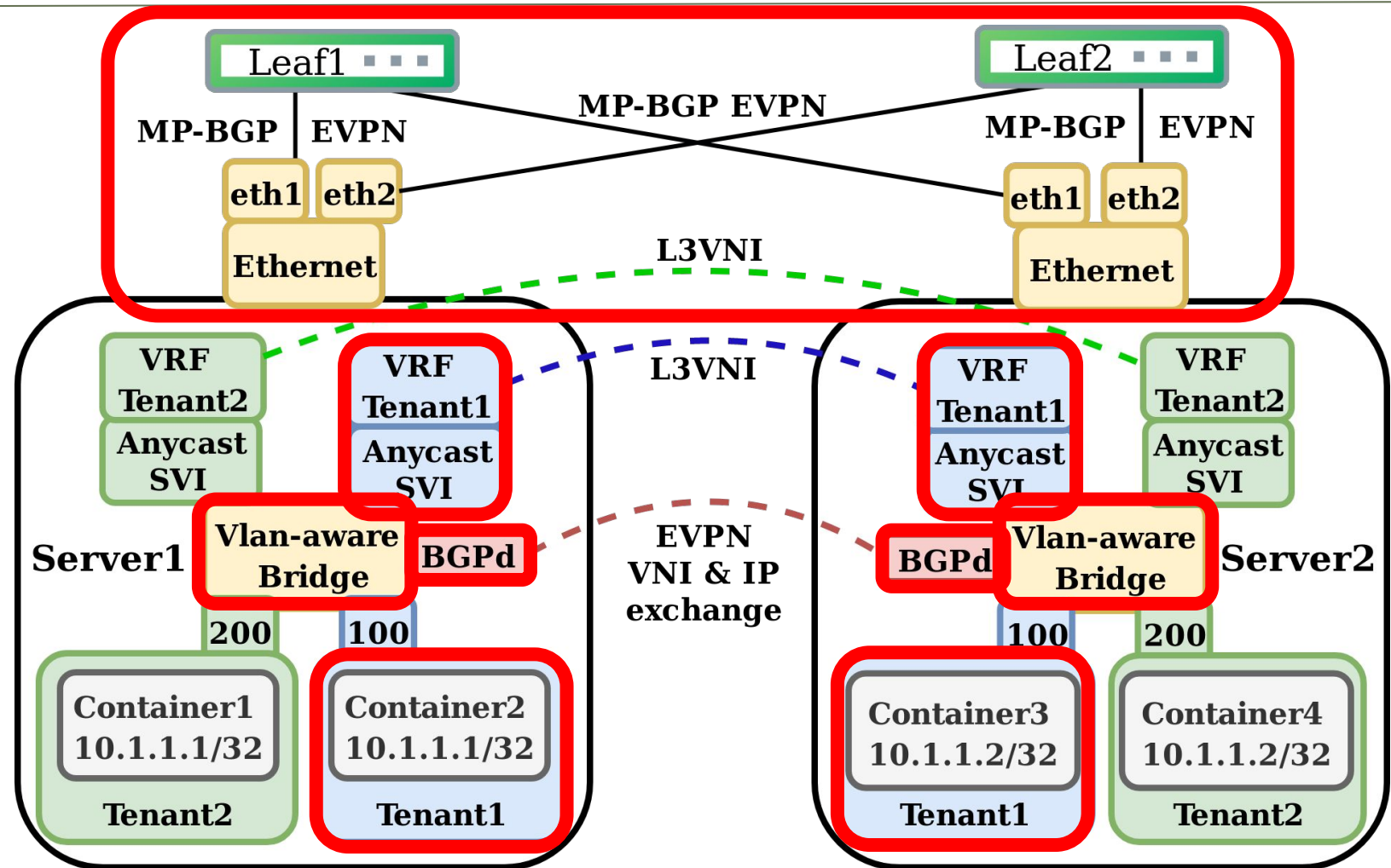SVI (Switched Virtual Interface)

Figure 8: Architecture of EVPN L3 multi-tenancy

Results - Integration of EVPN in Kubernetes

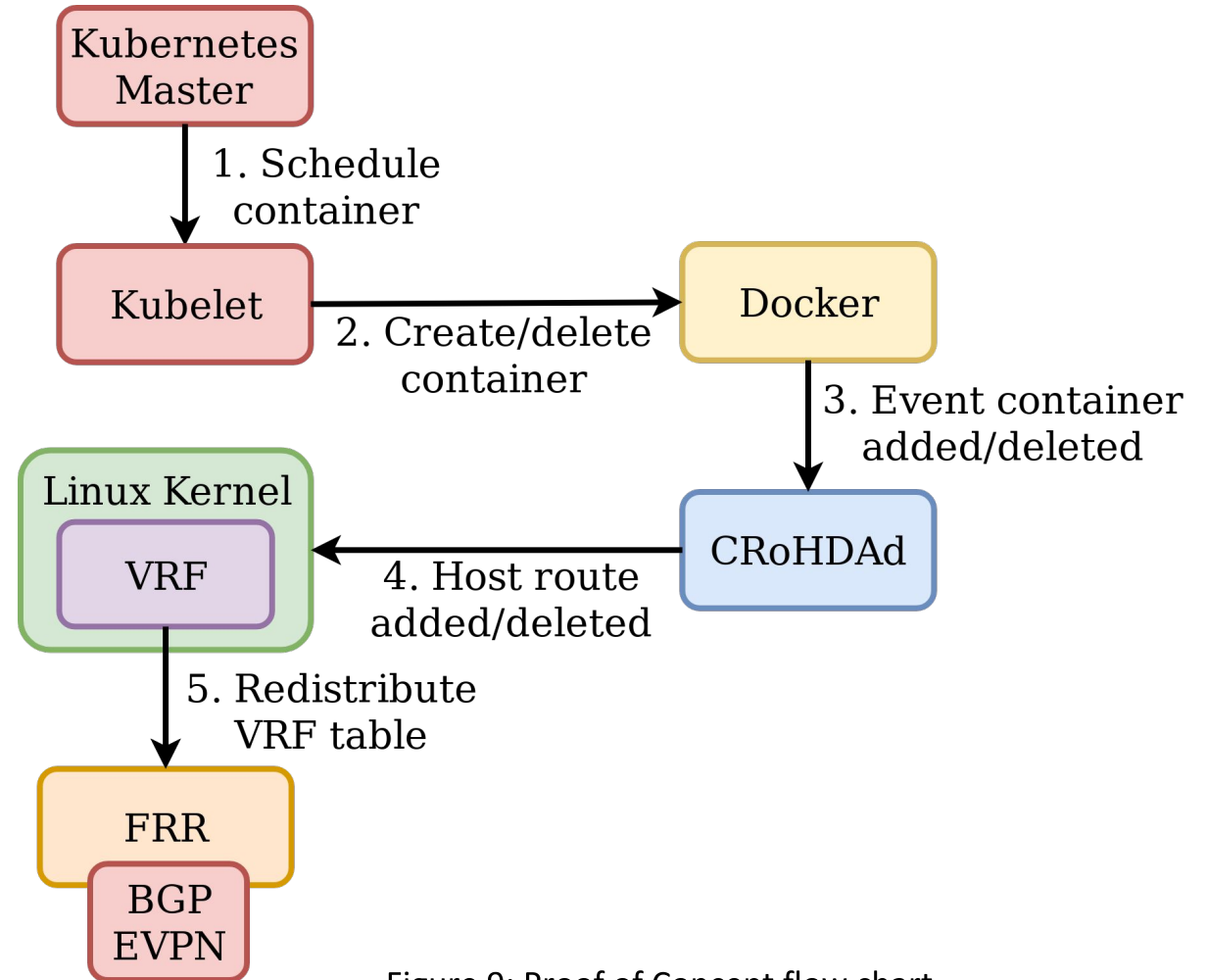CRoHDAd (Cumulus Routing on the Host Docker Advertisement daemon

Figure 9: Proof of Concept flow chart

Discussion
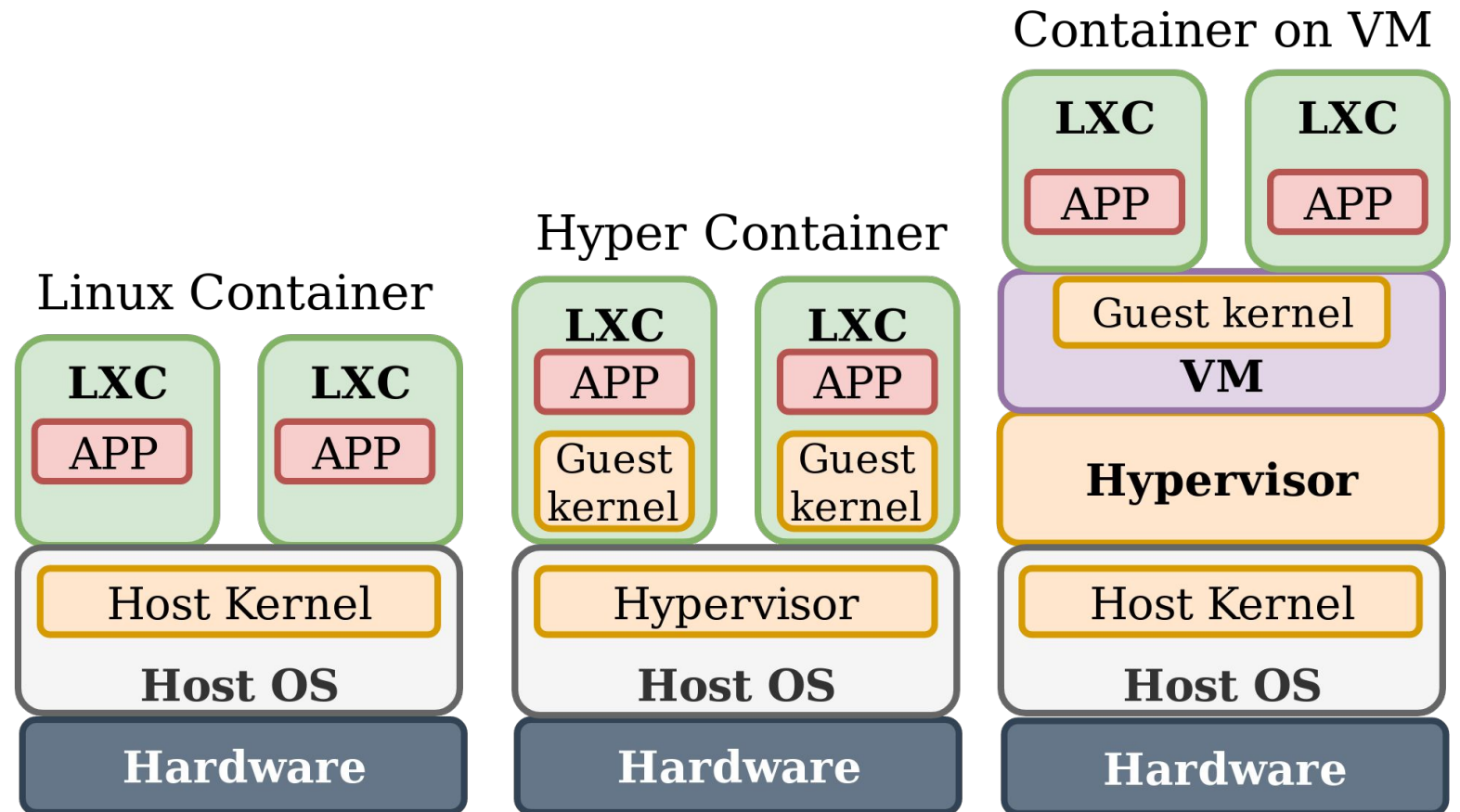
- Security
  - VRFs
  - Containers

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

- A. Gerrard, "What Is Kubernetes? An Introduction to the Wildly Popular Container Orchestration Platform." https://blog.newrelic.com/ engineering/what-is-kubernetes/, 2019.

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

- T. Narten, Ed., E. Gray, Ed., D. Black, L. Fang, L. Kreeger and M. Napierala, "Problem Statement: Overlays for Network Virtualization." http://www.hjp.at/doc/rfc/rfc7364.html, 2014.

- L. Makowski and P. Grosso, "Evaluation of virtualization and traffic filtering methods for container networks", Future Generation Computer Systems, vol. 93, pp. 345 – 357, 2019.

- N. van Noort, "Secure data sharing in container networks," 2019.

- H. Zhang and P. Ni, "Hypernetes: Bringing Security and Multi-tenancy to Kubernetes." https://kubernetes.io/blog/2016/05/hypernetes-security-and-multi-tenancy-in-kubernetes/, 2016.

Questions?