

Segment routing in container networks

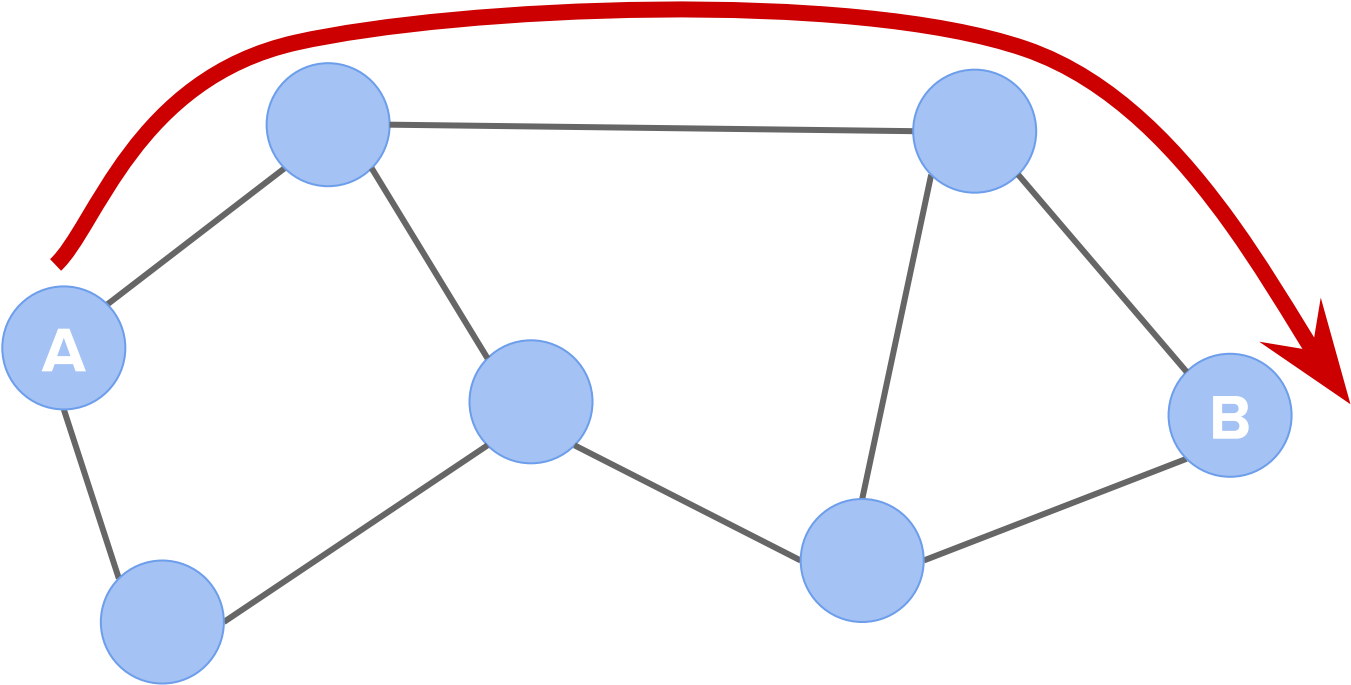
Ben de Graaff

Supervisor: Marijke Kaat (SURFnet/UvA)



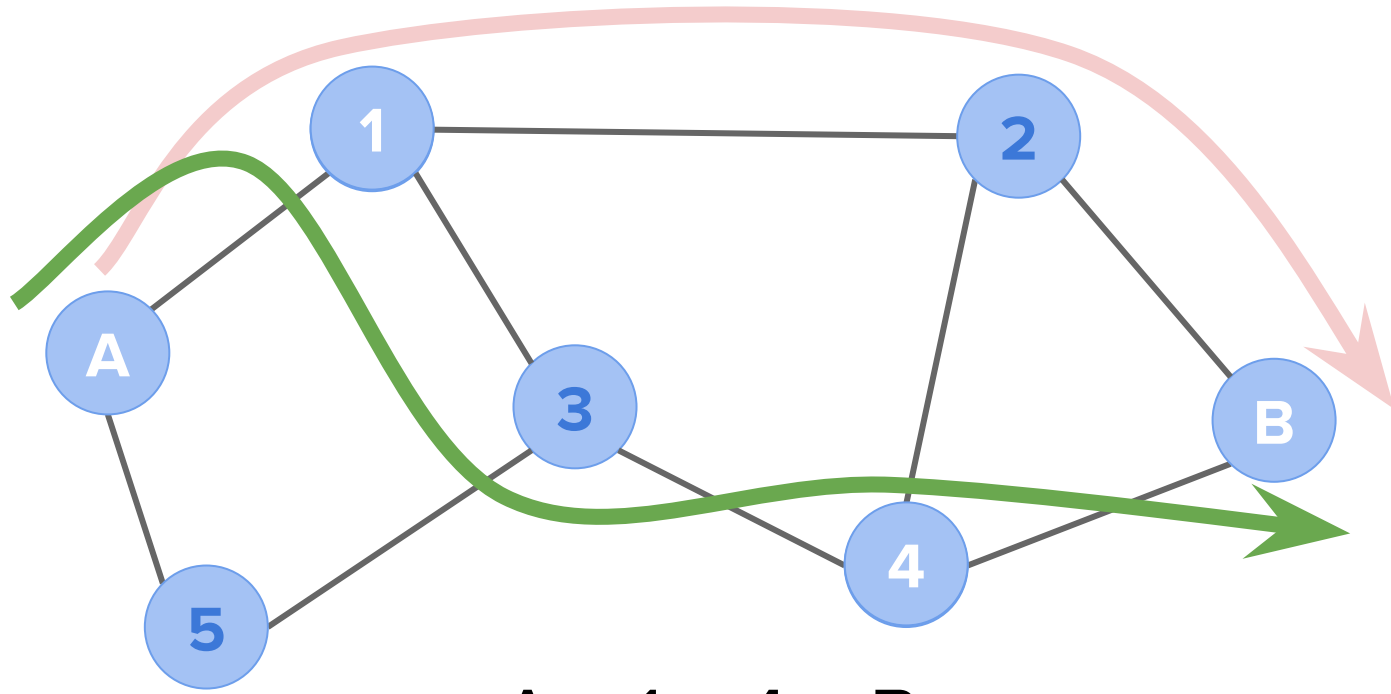
Best path

Background



Arbitrary paths

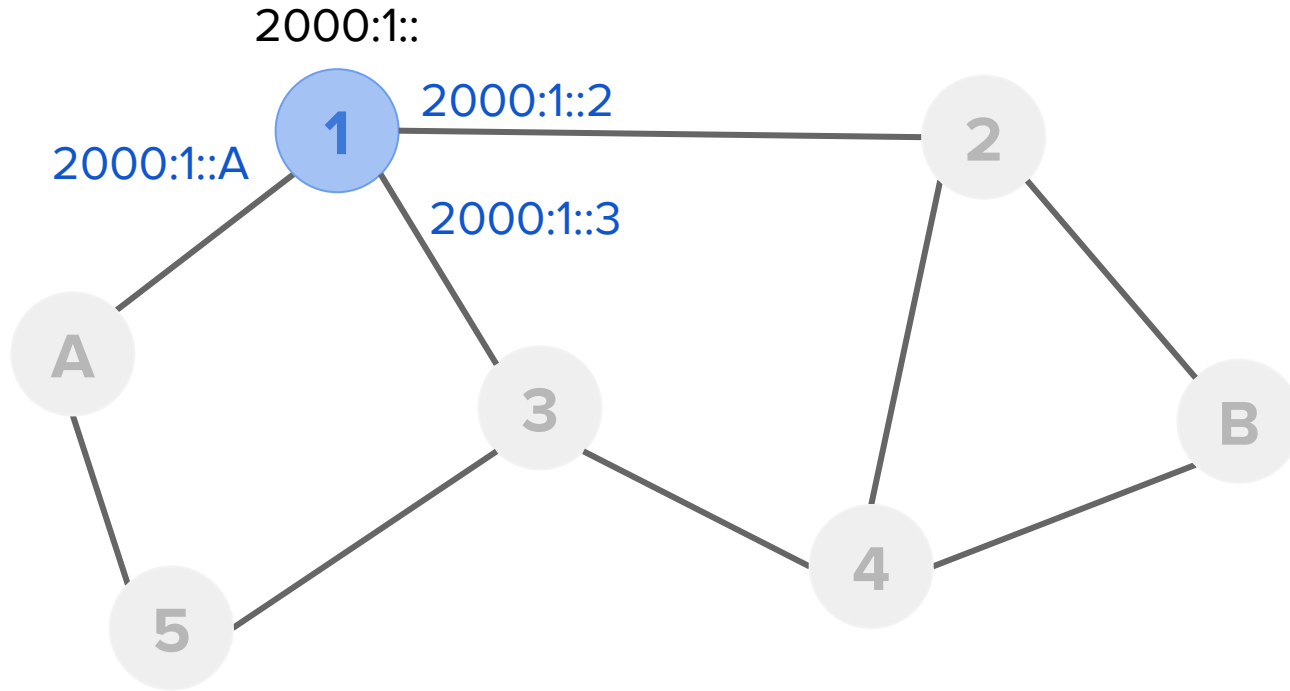
Background



$A > 1 > 4 > B$

Pure IPv6 (SRv6)

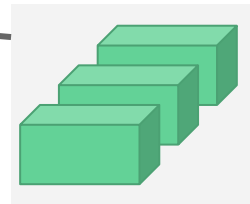
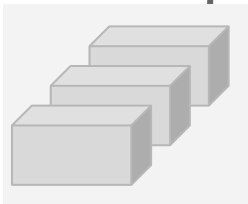
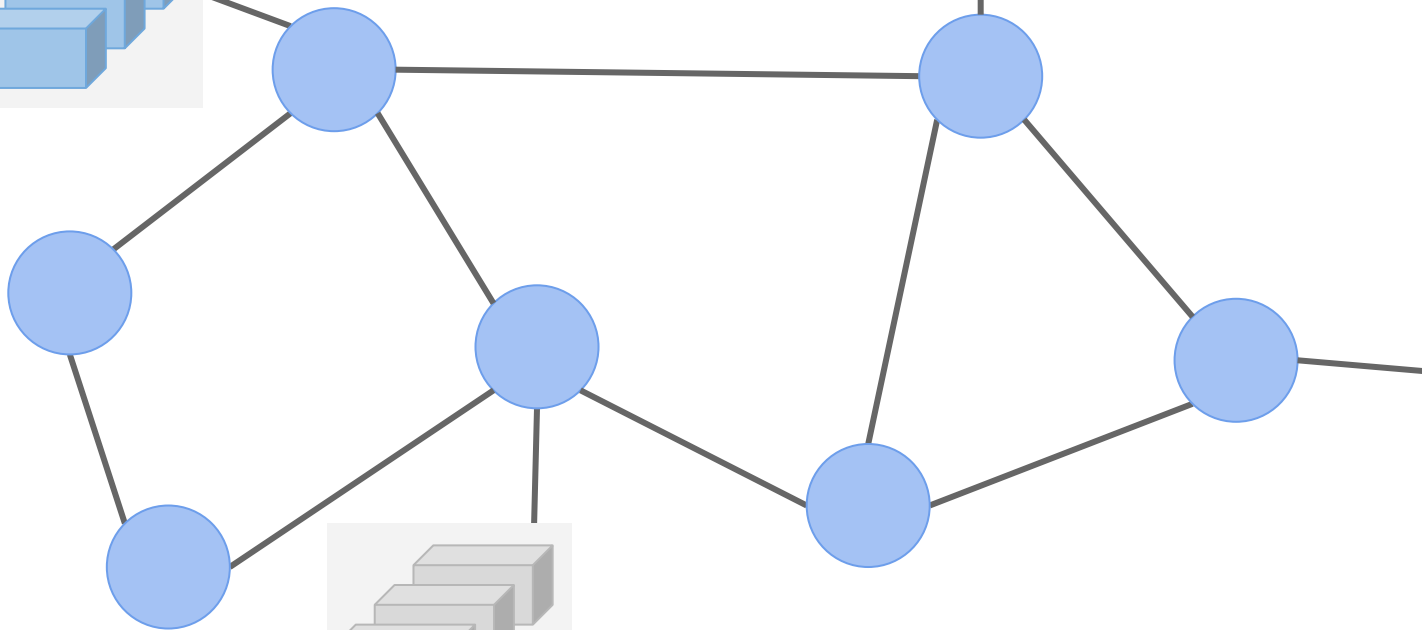
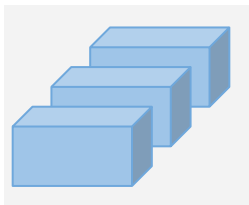
Background



Container networks



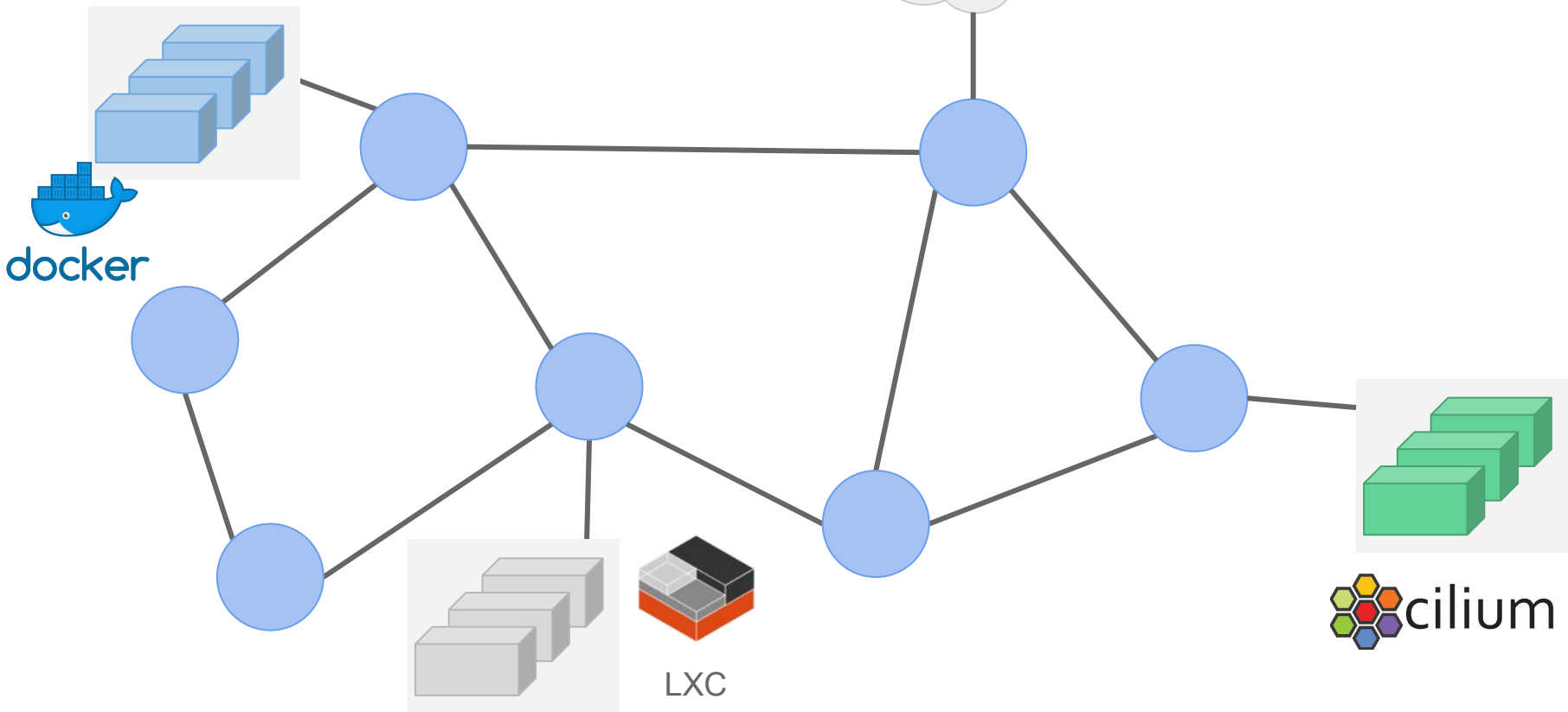
Background



Platform independent



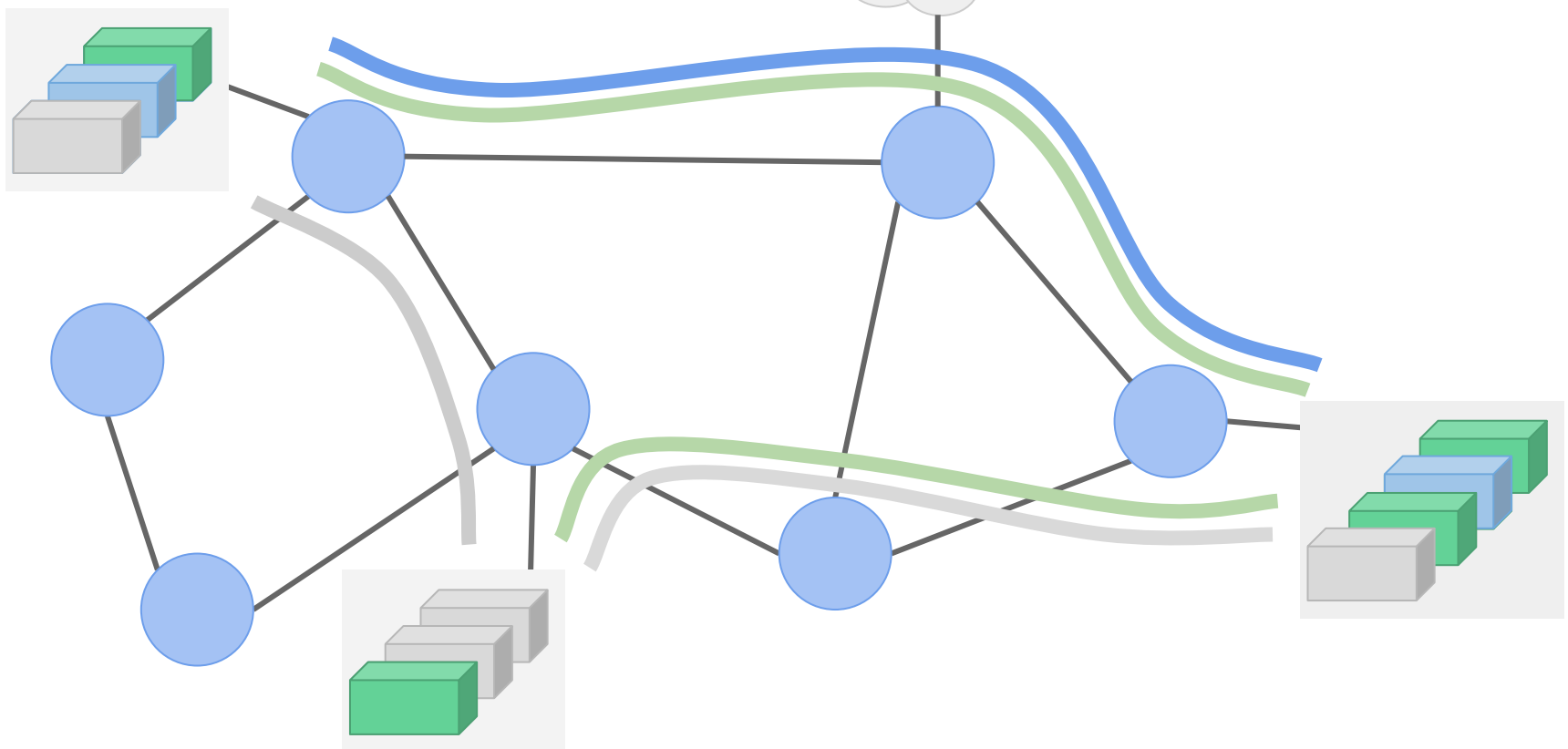
Background



Multi-tenancy



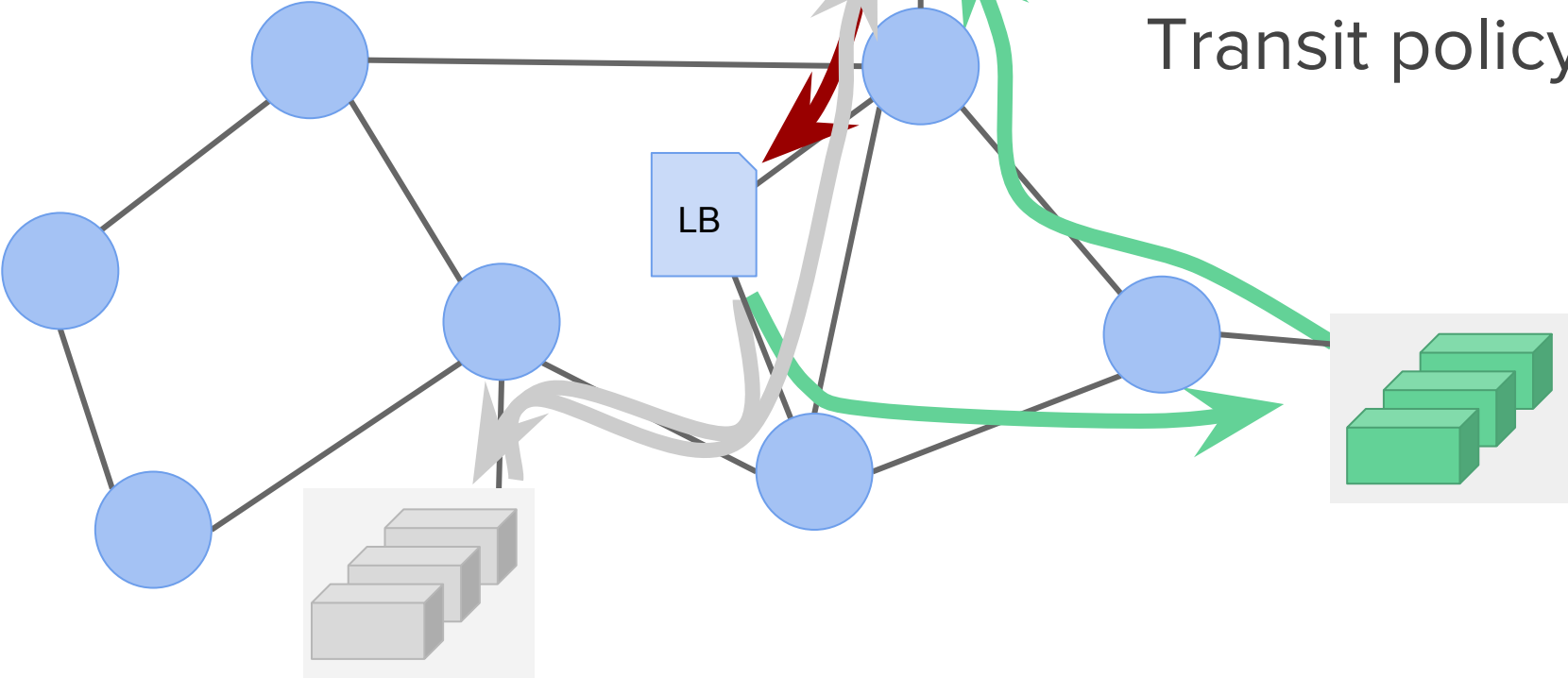
Background



Example: load balancer



Background



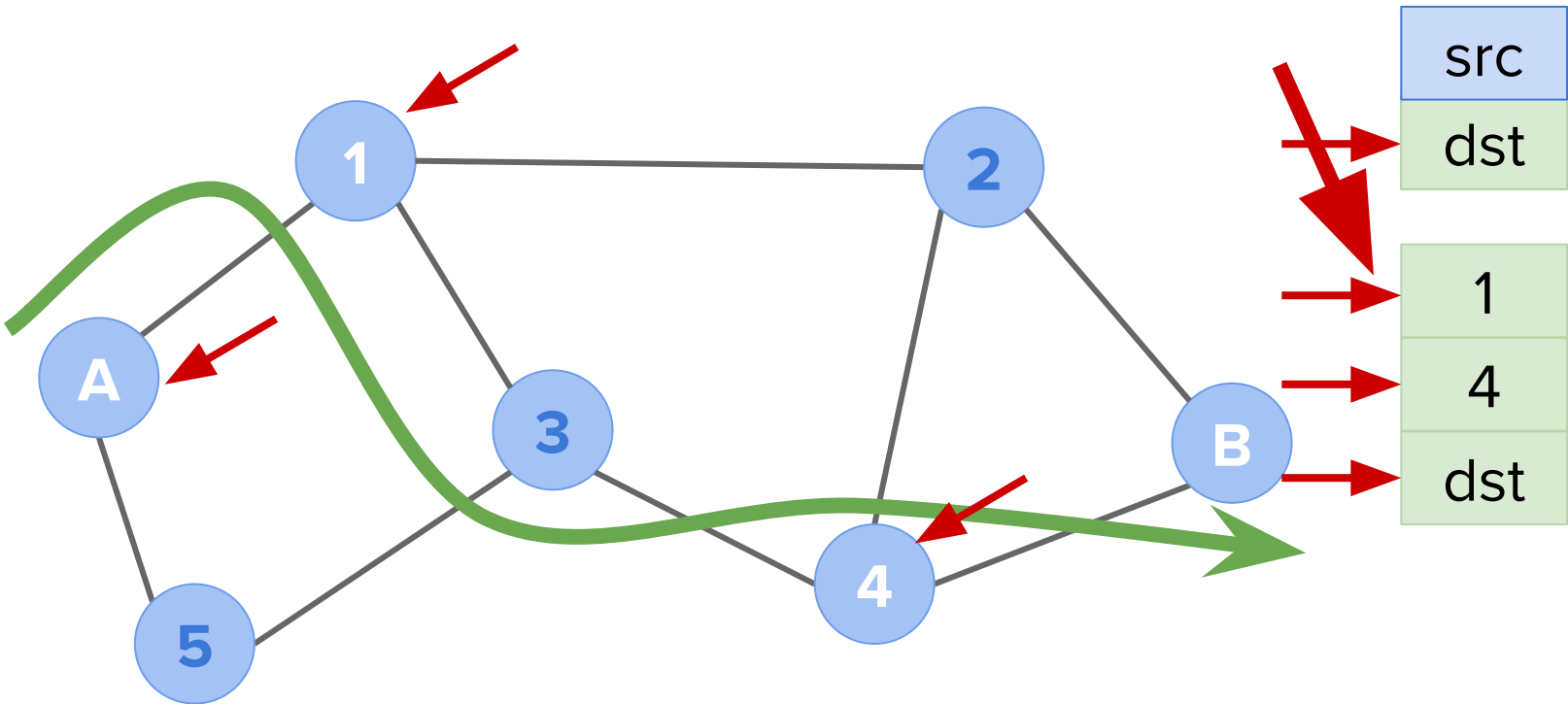
Research

State of segment routing in IPv6

Proof of concept:
Container networking
Network functions



Network programming

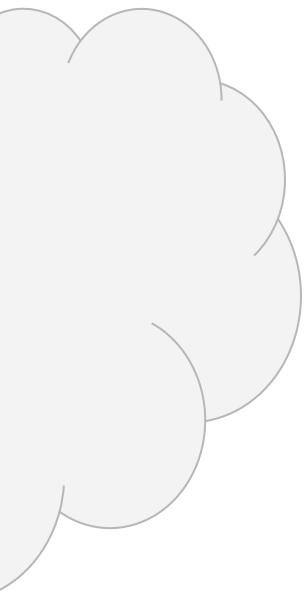


src > 1 > 4 > dst

Segment routing header



Proof of concept



Validate policy

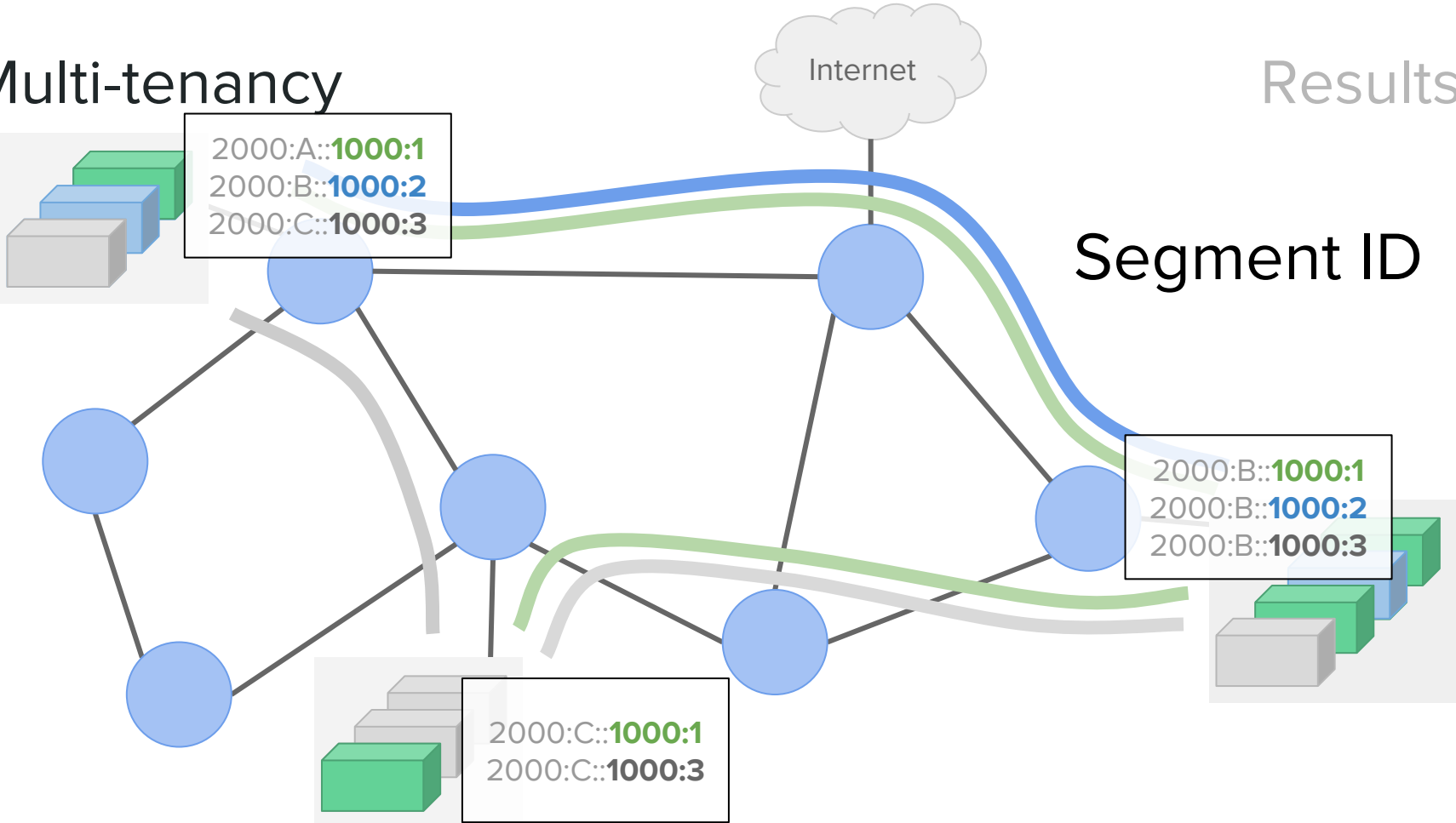


Apply policy

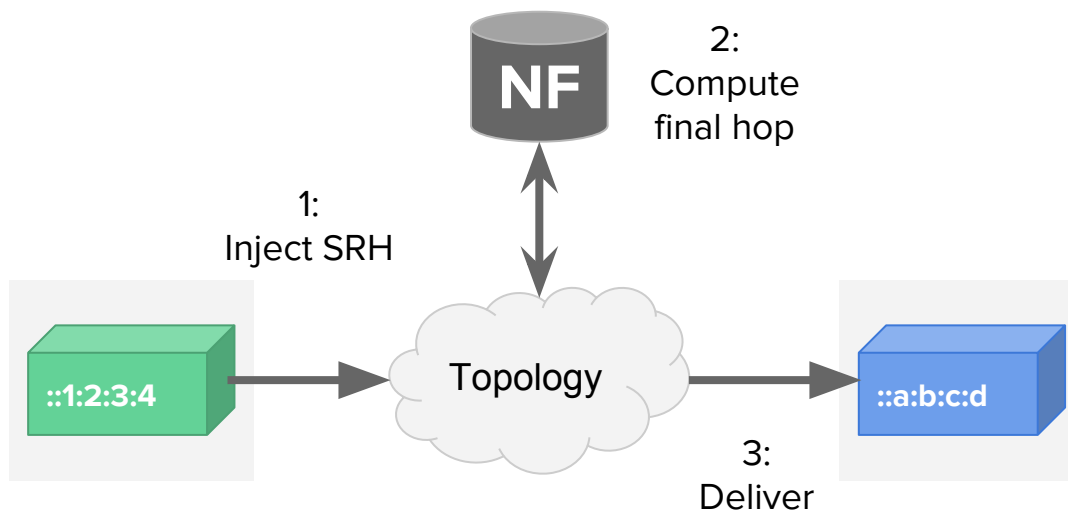


Multi-tenancy

Results



Routing opaque addresses



Implementation

Results

Hardware/software

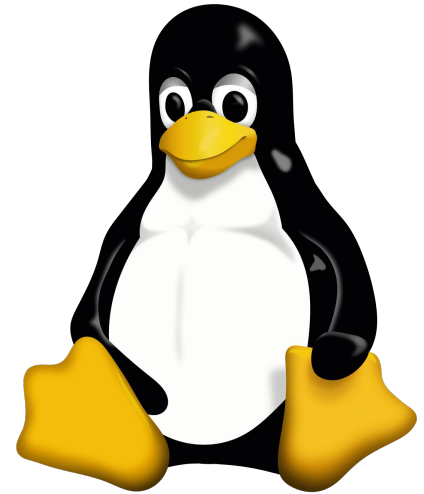
Linux kernel 4.10+

Results

Basic routing/policy

Limited extension support

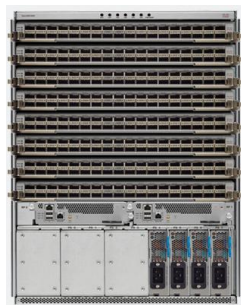
Implementation quirks...



SRv6 availability

Results

Hardware



NCS 5500



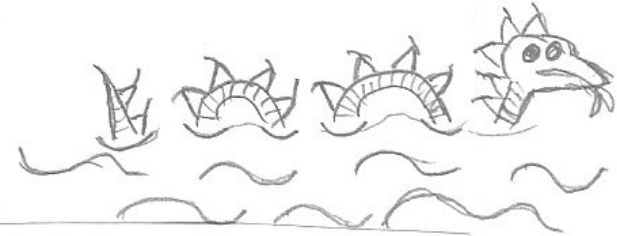
Software

Vector Packet Processing

The Fast Data Project



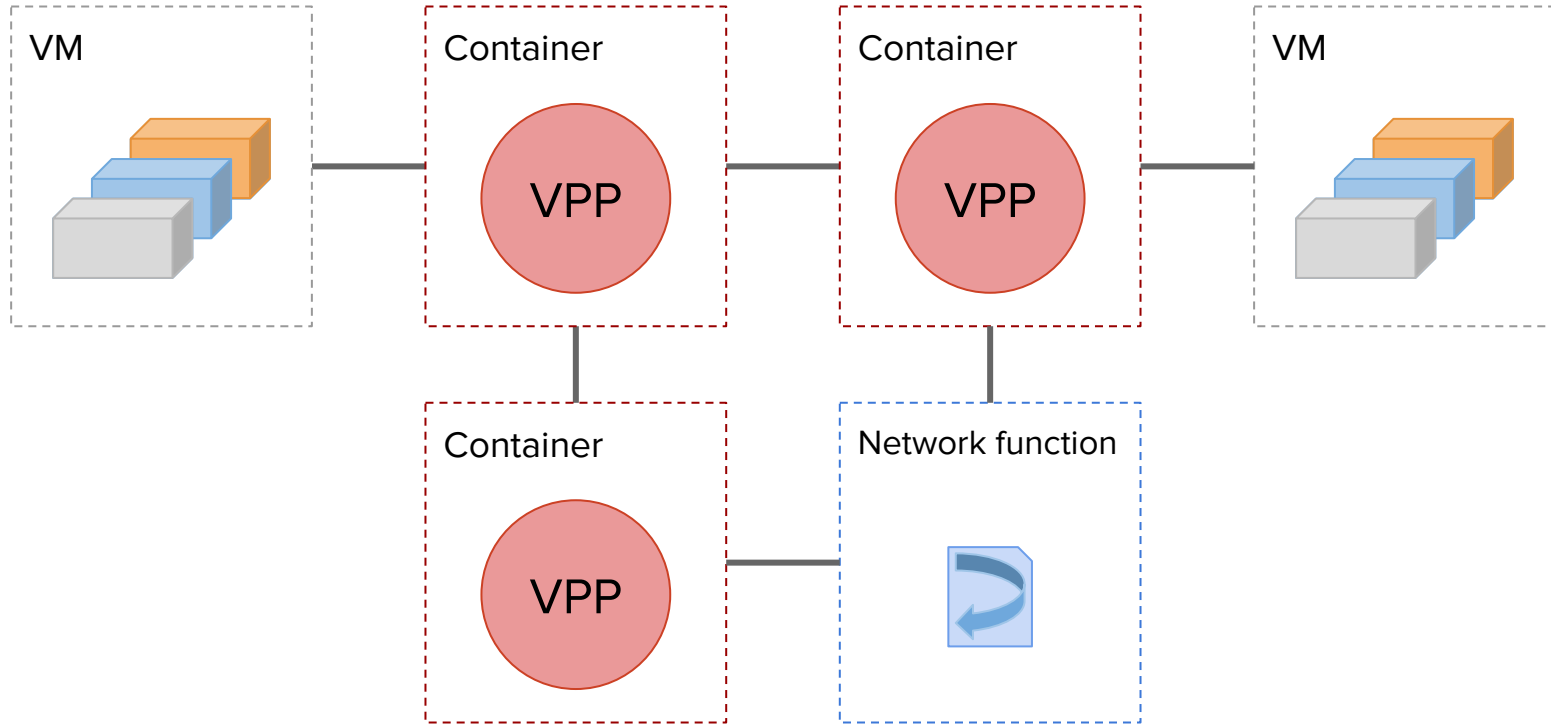
Technical implementation



HERE BE SEA MONSTERS

Virtual topology

Results



eBPF

Results

Latest & greatest

Process directly in kernel

Fast, powerful

myprog.c + LLVM =
bytecode



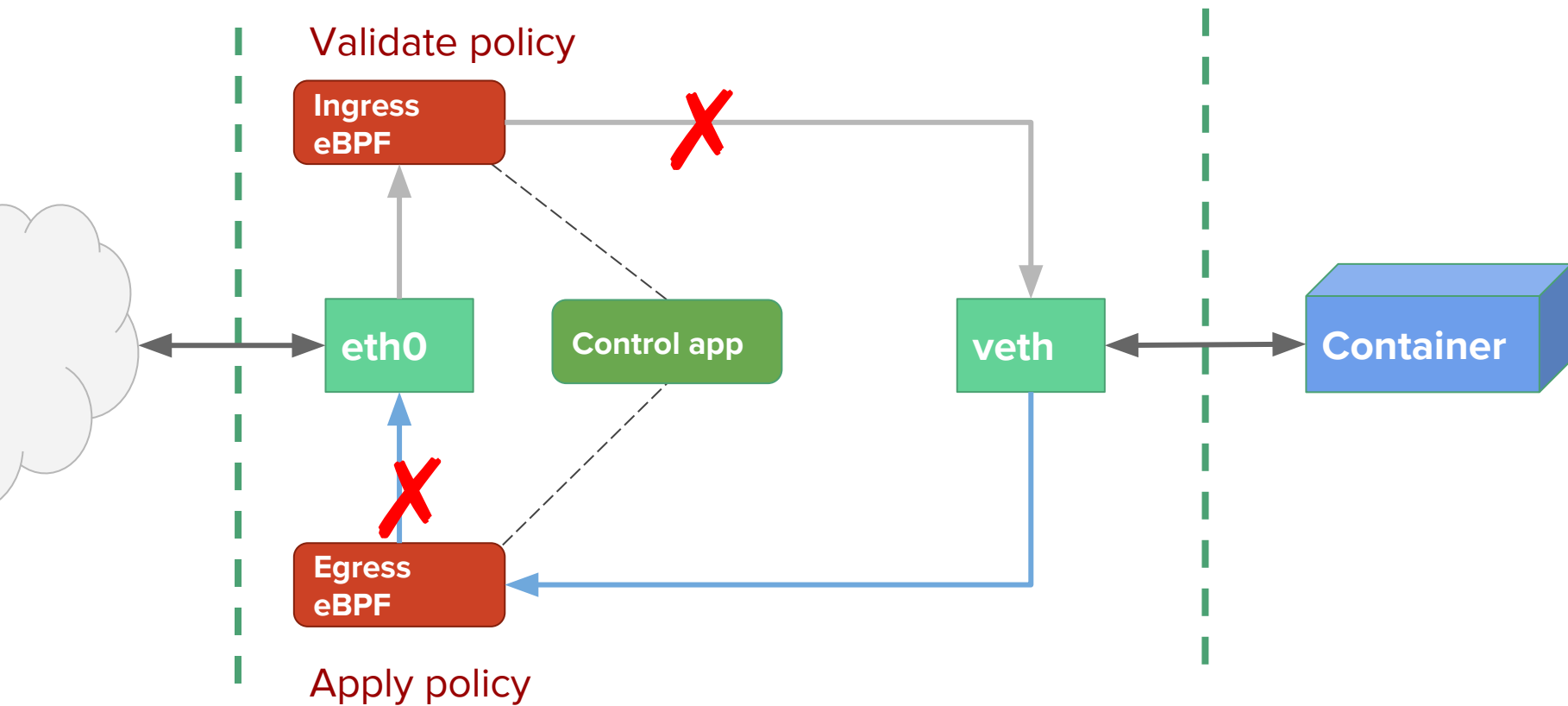
bpf() syscall



Kernel network stack

eBPF

Results



Linux do-it-yourself

Results

Tun/tap

AF_PACKET

ip rule

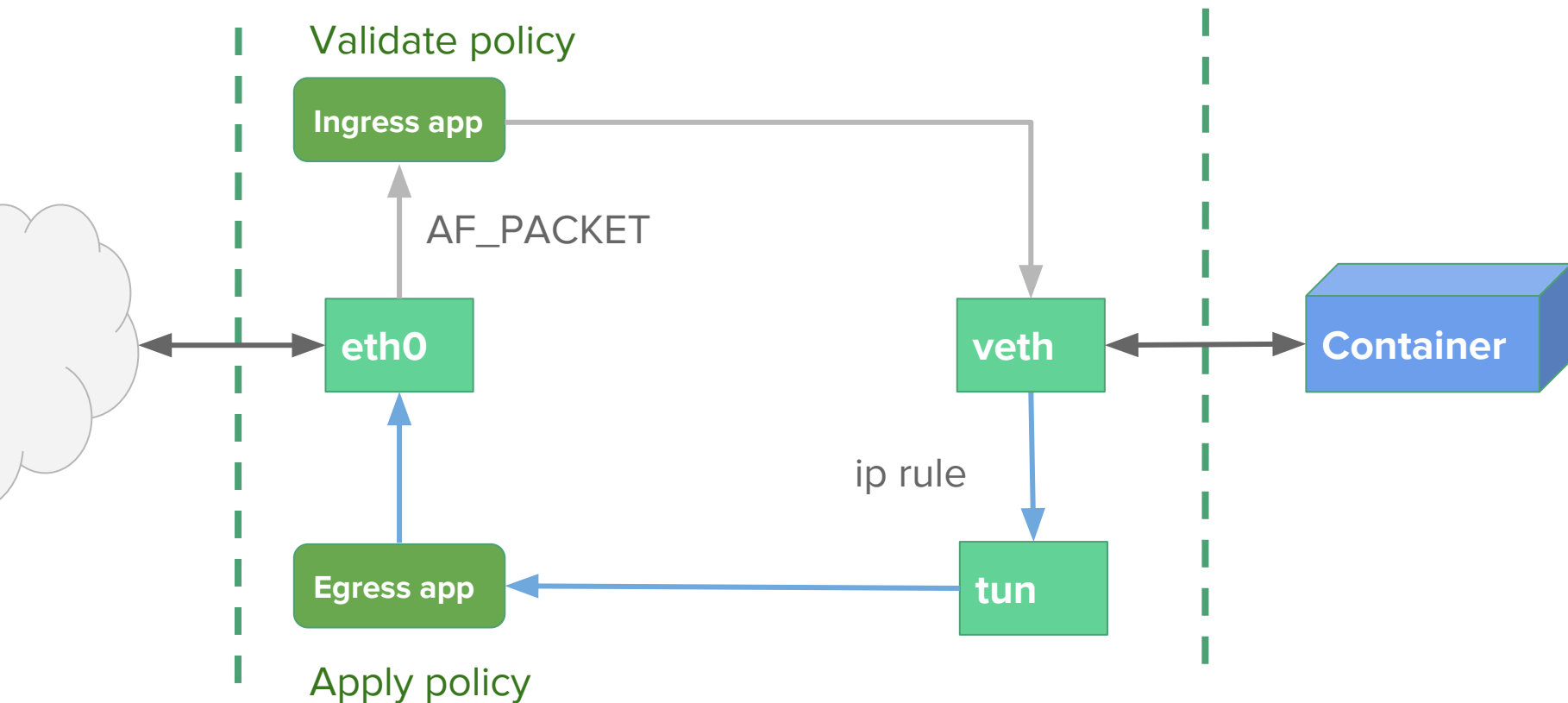
iptables fwmark

PF_RING

...

Linux do-it-yourself

Results



Summary



Validate policy



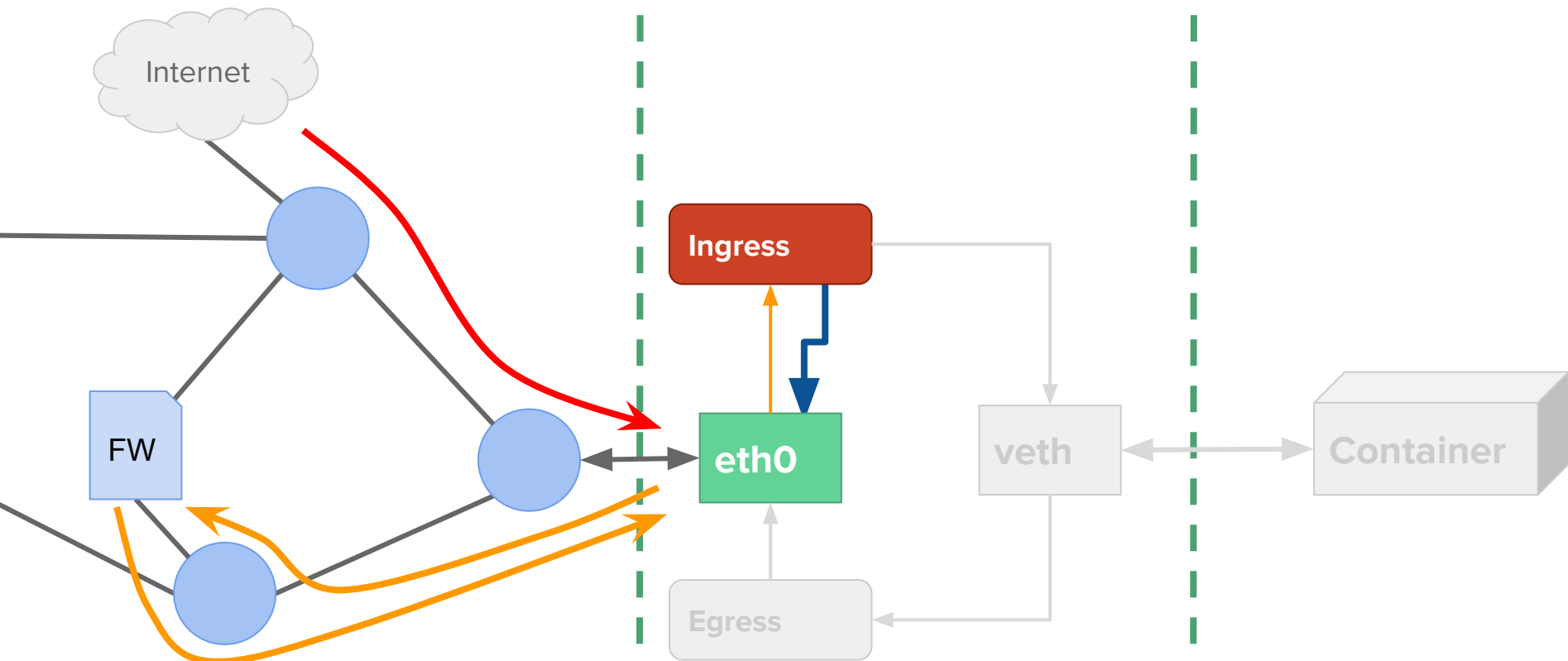
Apply policy

Results



Ingress policy enforcement?

Discussion



Future work

Ingress path control

Linux segment routing Netlink API

Develop useful extensions

Conclusion

Proof of concept: works

SDN easy, at cost of overhead

Hardware not strictly required

Related work

Cisco, Bell Canada, Comcast, et al, technical workshops @ www.segment-routing.net

NFV with SRv6, with SRH unaware hosts
(NetSoft 2017, presented **today**)

Segment routing in container networks

Segment routing is effective at enabling **SDN** and **network functions** between **containers**

However, it is **not yet widely supported** in hardware, software

Check out the report for a full list of references

<http://rp.delaat.net/2016-2017/p95/report.pdf>

Backup slides

Security/RH0

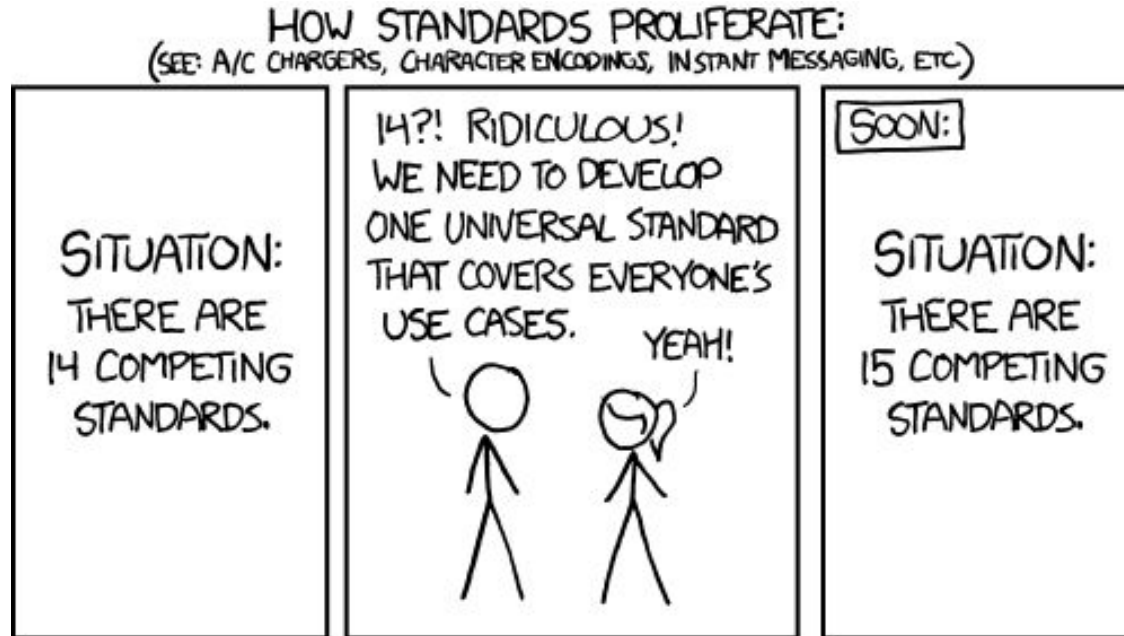
Enforce policy at network edges

SIDs must be explicitly enabled

HMAC: check at ingress

Simplify the network

Discussion

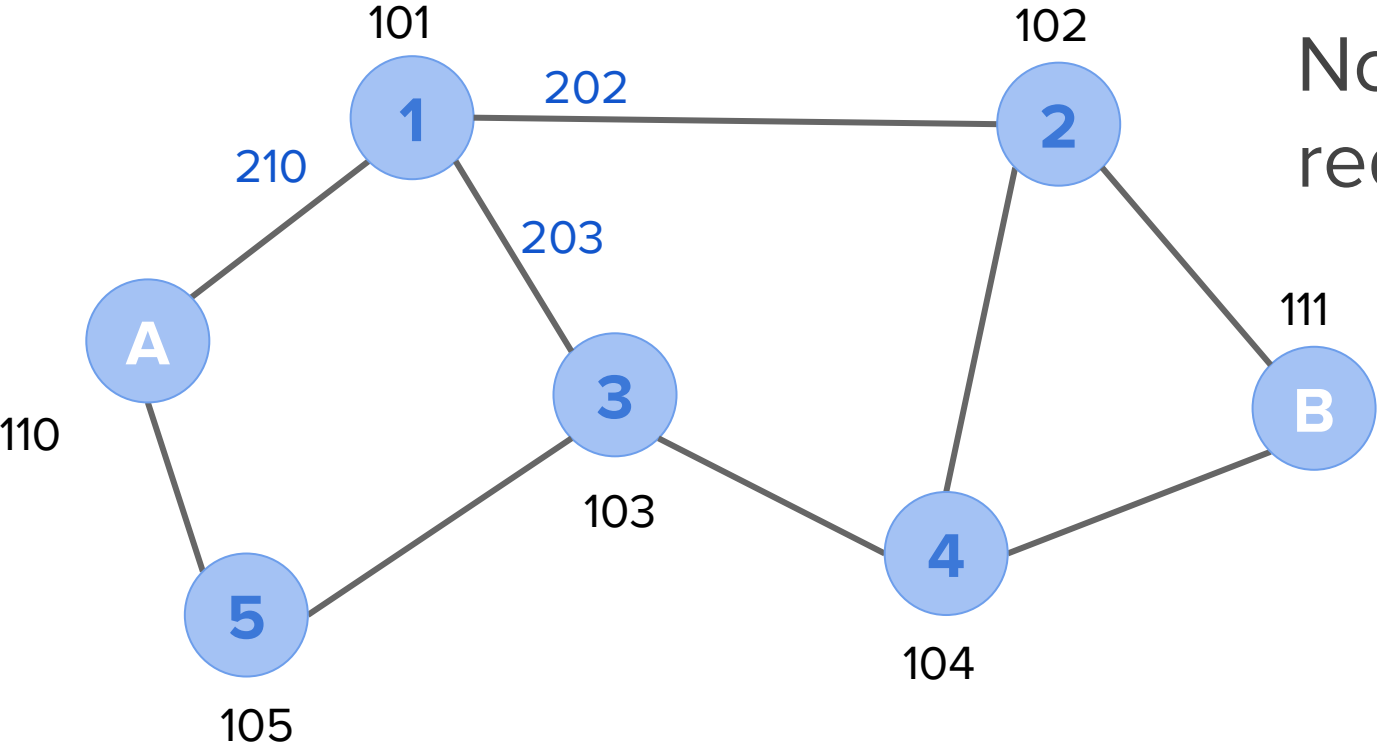


<https://xkcd.com/927/>

MPLS

Background

No LDP, RSVP
required



Multi-tenancy

Discussion

Layer 2 and 3
cross-connects

Multi-tenancy:
Segment ID or extension?

