

Better Understanding Openshift networking with the help of Wireshark



Sergey Guzenkov



1999..2012 sysadmin

2002.. start of linux journey

2012..2015 Ops of DevOps

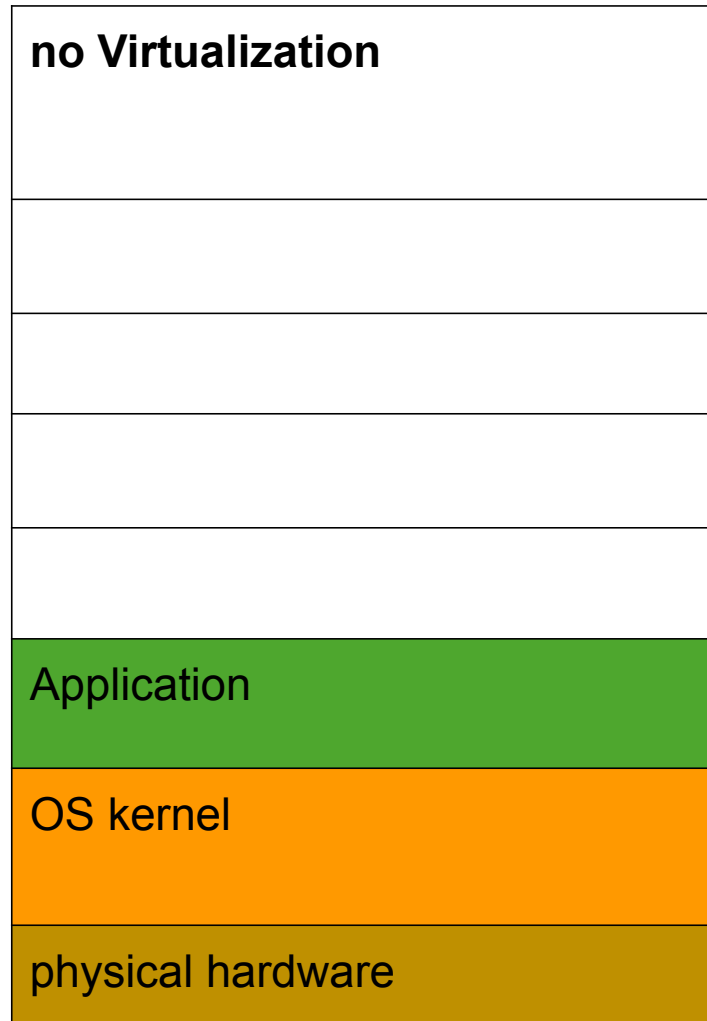
2014 first Wireshark Conference

2016.. Principal instructor at Red Hat

Red Hat Certified Architect (RHCA)
and examiner



- Overview of containers
- Overview of Kubernetes and Openshift
- Perform and analyze a capture on kubernetes node
- Discuss overlay networks
- Discuss the



Virtualization revolution

no Virtualization	Virtualization
	Application
	OS Kernel
Application	virtual hardware
OS kernel	hypervisor kernel
physical hardware	physical hardware

no Virtualization	Virtualization
	Application
	OS Kernel
Application	virtual hardware
OS kernel	hypervisor kernel
physical hardware	physical hardware

Problems addressed by virtualization:

- isolation of apps
 - security
 - performance
- capacity
- ease of management
-

Dedicated IP and disk.

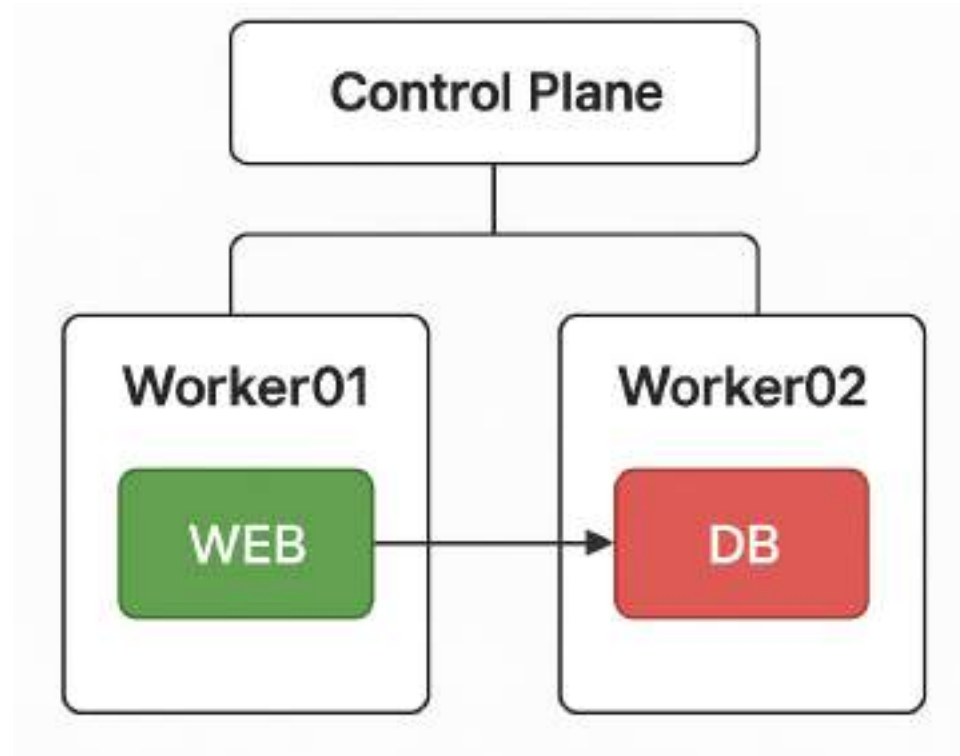
keywords: VMs, VMWare, Xen, KVM, Hyper-V

From VMs to Containers

no Virtualization	Virtualization	Containerization
	Application	
	OS Kernel	Application
Application	virtual hardware	Container
OS kernel	hypervisor kernel	OS kernel
physical hardware	physical hardware	physical hardware

From Containers to VMs

no Virtualization	Virtualization	Containerization	VMs in containers
			Application
	Application		mini kernel
	OS Kernel	Application	virtual hardware
Application	virtual hardware	Container	Container
OS kernel	hypervisor kernel	OS kernel	OS kernel
physical hardware	physical hardware	physical hardware	physical hardware



Kubernetes components

Worker01	Worker02	Master01	Master02	Master03
CRI	CRI	CRI	CRI	CRI
kubelet	kubelet	kubelet	kubelet	kubelet
		API	API	API
		etcd	etcd	etcd
		scheduler	scheduler	scheduler
		controller	controller	controller



What is Openshift

Openshift is kubernetes with multiple addons, including networking (OVN), container runtime (CRI-O), *storage (Ceph)*, ingress (HAProxy), monitoring (Prometheus), *logging (loki)*, container registry (Quay), *virtualization*.

Source to image and a catalog of base images.

Service Discovery with CoreDNS and optionally Istio.

CoreOS.

Web console.

Support.



OPENSIFT

What kubernetes version is shipped with Openshift

Release Date OpenShift Kubernetes

27 Jul 2021	4.8	1.21
-------------	-----	------

10 Mar 2022	4.10	1.23
-------------	------	------

10 Aug 2022	4.11	1.24
-------------	------	------

17 Jan 2023	4.12	1.25
-------------	------	------

14 Jun 2023	4.13	1.26
-------------	------	------

13 Dec 2023	4.14	1.27
-------------	------	------

24 Apr 2024	4.15	1.28
-------------	------	------

30 Aug 2024	4.16	1.29
-------------	------	------

20 Nov 2024	4.17	1.30
-------------	------	------

listing of pods on a worker node

```
[student@workstation ~]$ oc get pod -A --field-selector spec.nodeName=worker01
```

NAMESPACE	NAME	READY	STATUS	RESTARTS	AGE
cert-manager	cert-manager-webhook-58ffc98b58-17nfm	1/1	Running	3	3d11h
metallb-system	controller-7fc7c6c0ff-5m187	2/2	Running	6	3d11h
metallb-system	metallb-operator-webhook-server-584bd47dd9-nzvb4	1/1	Running	3	3d11h
metallb-system	speaker-jhzjl	2/2	Running	8	3d12h
netobserv-privileged	netobserv-ebpf-agent-p6qqg	1/1	Running	9	6d14h
netobserv	flowlogs-pipeline-tfw6z	1/1	Running	9	6d14h
nfs-client-provisioner	nfs-client-provisioner-6dfff48596-td5nl	1/1	Running	3	3d11h
openshift-cluster-node-tuning-operator	tuned-rsp5b	1/1	Running	4	3d11h
openshift-dns	dns-default-lghs9	2/2	Running	8	3d11h
openshift-dns	node-resolver-tds74	1/1	Running	4	3d11h
openshift-frr-k8s	frr-k8s-hgwz8	7/7	Running	28	3d11h
openshift-image-registry	image-registry-b44774958-5gl4f	1/1	Running	3	3d11h
openshift-image-registry	node-ca-zlcj9	1/1	Running	4	3d11h
openshift-ingress-canary	ingress-canary-l75jp	1/1	Running	4	3d11h
openshift-ingress	router-default-58c5cfb48b-5p2f8	1/1	Running	3	3d11h
openshift-insights	insights-runtime-extractor-h68tl	3/3	Running	12	3d11h
openshift-machine-config-operator	kube-rbac-proxy-crio-worker01	1/1	Running	4	3d11h
openshift-machine-config-operator	machine-config-daemon-8mrkz	2/2	Running	8	3d11h
openshift-monitoring	alertmanager-main-0	6/6	Running	18	3d11h
openshift-monitoring	kube-state-metrics-5bd9c98b56-s6x7s	3/3	Running	9	3d11h
openshift-monitoring	monitoring-plugin-69d747b4db-b76th	1/1	Running	3	3d11h
openshift-monitoring	node-exporter-v415x	2/2	Running	6	3d11h
openshift-monitoring	openshift-state-metrics-d86c7b545-fttr2	3/3	Running	9	3d11h
openshift-monitoring	prometheus-k8s-0	6/6	Running	18	3d11h
openshift-monitoring	prometheus-operator-admission-webhook-c9f987dd7-htkwm	1/1	Running	3	3d11h
openshift-monitoring	thanos-querier-6cd579bfb48-1rtdh	6/6	Running	18	3d11h
openshift-multus	multus-additional-cni-plugins-db9r8	1/1	Running	4	3d11h
openshift-multus	multus-rmhfrj	1/1	Running	5	3d11h
openshift-multus	network-metrics-daemon-9s96p	2/2	Running	8	3d11h
openshift-network-console	networking-console-plugin-7f8c6b9b7d-6nv7s	1/1	Running	3	3d11h
openshift-network-diagnostics	network-check-target-qnvxc	1/1	Running	4	3d11h
openshift-network-operator	iptables-alerter-5bs8p	1/1	Running	4	3d11h
openshift-operator-lifecycle-manager	collect-profiles-29378300-pgjqg	0/1	Completed	0	39m
openshift-operator-lifecycle-manager	collect-profiles-29378315-5drhh	0/1	Completed	0	24m
openshift-operator-lifecycle-manager	collect-profiles-29378330-6zrck	0/1	Completed	0	9m55s
openshift-operators-redhat	loki-operator-controller-manager-785467c996-626vr	2/2	Running	6	3d11h
openshift-ovn-kubernetes	ovnkube-node-sxzhm	8/8	Running	32	3d11h
openshift-storage	odf-console-5fc258988f-5278b	1/1	Running	3	3d11h

listing of pods on a master node

```
[student@workstation ~]$ oc get pod -A --field-selector spec.nodeName=master01
```

NAMESPACE	NAME	READY	STATUS	RESTARTS	AGE
metallb-system	speaker-nlbfg	2/2	Running	12	3d5h
netobserv-privileged	netobserv-ebpf-agent-gj8nh	1/1	Running	9	6d8h
netobserv	flowlogs-pipeline-cn528	1/1	Running	10	6d8h
openshift-apiserver	apiserver-748cbd8898-gfgqx	2/2	Running	10	3d4h
openshift-authentication	oauth-openshift-6559659b88-kmmz6	1/1	Running	5	3d4h
openshift-cluster-node-tuning-operator	tuned-gr8gt	1/1	Running	4	3d5h
openshift-controller-manager	controller-manager-675cc647cb-mk2ls	1/1	Running	1	23h
openshift-dns	dns-default-87k5t	2/2	Running	8	3d5h
openshift-dns	node-resolver-ppgb7	1/1	Running	4	3d5h
openshift-etcd	etcd-guard-master01	1/1	Running	3	3d4h
openshift-etcd	etcd-master01	5/5	Running	20	3d5h
openshift-etcd	revision-pruner-16-master01	0/1	Completed	0	3d4h
openshift-frr-k8s	frr-k8s-fxdtf	7/7	Running	36	3d5h
openshift-image-registry	node-ca-rkfw2	1/1	Running	4	3d5h
openshift-kube-apiserver	kube-apiserver-guard-master01	1/1	Running	3	3d4h
openshift-kube-apiserver	kube-apiserver-master01	5/5	Running	33 (15h ago)	3d5h
openshift-kube-apiserver	revision-pruner-26-master01	0/1	Completed	0	3d4h
openshift-kube-controller-manager	kube-controller-manager-guard-master01	1/1	Running	3	3d4h
openshift-kube-controller-manager	kube-controller-manager-master01	4/4	Running	21 (15h ago)	3d5h
openshift-kube-scheduler	openshift-kube-scheduler-guard-master01	1/1	Running	3	3d4h
openshift-kube-scheduler	openshift-kube-scheduler-master01	3/3	Running	12	3d5h
openshift-kube-scheduler	revision-pruner-14-master01	0/1	Completed	0	3d4h
openshift-machine-config-operator	kube-rbac-proxy-crio-master01	1/1	Running	4	3d4h
openshift-machine-config-operator	machine-config-daemon-28rcn	2/2	Running	8	3d5h
openshift-machine-config-operator	machine-config-server-z2qsx	1/1	Running	4	3d4h
openshift-marketplace	certified-operators-pdh6n	1/1	Running	0	5h20m


```
[student@workstation ~]$ oc get clusterversion
NAME      VERSION  AVAILABLE  PROGRESSING  SINCE   STATUS
version   4.19.16  True       False        20h     Cluster version is 4.19.16

[student@workstation ~]$ oc get nodes
NAME      STATUS  ROLES    AGE   VERSION
master01  Ready   control-plane,master  351d  v1.32.9
master02  Ready   control-plane,master  351d  v1.32.9
master03  Ready   control-plane,master  351d  v1.32.9
worker01  Ready   worker    346d  v1.32.9
worker02  Ready   worker    346d  v1.32.9
worker03  Ready   worker    346d  v1.32.9

[student@workstation ~]$
```

```
[student@workstation stoic]$ oc get node -o wide
NAME      STATUS  ROLES    AGE   VERSION  INTERNAL-IP  EXTERNAL-IP  OS-IMAGE                                     KERNEL-VERSION  CONTAINER-RUNTIME
master01  Ready   control-plane,master  366d  v1.33.5  192.168.50.10 <none>       Red Hat Enterprise Linux CoreOS 9.6.20251021-0 (Plow) 5.14.0-570.57.1.el9_0.x86_64 cri-o://1.33.5-3.rhosp4.20.gitd0ea985.el9
master02  Ready   control-plane,master  366d  v1.33.5  192.168.50.11 <none>       Red Hat Enterprise Linux CoreOS 9.6.20251021-0 (Plow) 5.14.0-570.57.1.el9_0.x86_64 cri-o://1.33.5-3.rhosp4.20.gitd0ea985.el9
master03  Ready   control-plane,master  366d  v1.33.5  192.168.50.12 <none>       Red Hat Enterprise Linux CoreOS 9.6.20251021-0 (Plow) 5.14.0-570.57.1.el9_0.x86_64 cri-o://1.33.5-3.rhosp4.20.gitd0ea985.el9
worker01  Ready   worker    361d  v1.33.5  192.168.50.13 <none>       Red Hat Enterprise Linux CoreOS 9.6.20251021-0 (Plow) 5.14.0-570.57.1.el9_0.x86_64 cri-o://1.33.5-3.rhosp4.20.gitd0ea985.el9
worker02  Ready   worker    361d  v1.33.5  192.168.50.14 <none>       Red Hat Enterprise Linux CoreOS 9.6.20251021-0 (Plow) 5.14.0-570.57.1.el9_0.x86_64 cri-o://1.33.5-3.rhosp4.20.gitd0ea985.el9
worker03  Ready   worker    361d  v1.33.5  192.168.50.15 <none>       Red Hat Enterprise Linux CoreOS 9.6.20251021-0 (Plow) 5.14.0-570.57.1.el9_0.x86_64 cri-o://1.33.5-3.rhosp4.20.gitd0ea985.el9
```

```
[student@workstation ~]$ oc debug node/master02
Temporary namespace openshift-debug-h7vqz is created for debugging node...
Starting pod/master02-debug-bbx4m ...
To use host binaries, run `chroot /host`
Pod IP: 192.168.50.11
If you don't see a command prompt, try pressing enter.
sh-5.1# tcpdump -D
1.ens3 [Up, Running, Connected]
2.ovn-k8s-mp0 [Up, Running, Connected]
3.genev_sys_6081 [Up, Running, Connected]
4.br-ex [Up, Running, Connected]
5.f8c8400300600f7 [Up, Running, Connected]
6.57cb95ba62b7ecf [Up, Running, Connected]
7.23f65e50a15f2ce [Up, Running, Connected]
8.0c32e34a2b2d82b [Up, Running, Connected]
9.e18d464168eb4af [Up, Running, Connected]
10.aeb42f2715eb977 [Up, Running, Connected]
11.5c287ce1f50d165 [Up, Running, Connected]
12.dcffa99d2d643b1 [Up, Running, Connected]
13.c0c488e0d59d671 [Up, Running, Connected]
14.66894538ec9c71c [Up, Running, Connected]
15.02d77a31cdbca7b [Up, Running, Connected]
16.d748b7372185c6e [Up, Running, Connected]
17.6c79d35a8b35001 [Up, Running, Connected]
18.a7d60c23c2fba8a [Up, Running, Connected]
19.92cf8860e1fe944 [Up, Running, Connected]
20.4cf41a6821a5f40 [Up, Running, Connected]
21.229b7f6fa4ff5f6 [Up, Running, Connected]
```



```
[core@master01 ~]$ toolbox
Trying to pull registry.redhat.io/rhel9/support-tools:latest...
Getting image source signatures
Checking if image destination supports signatures
Copying blob 7d071e8fd18e done |
Copying blob 35d6a5cce6a1 done |
Copying config 02e93d53c8 done |
Writing manifest to image destination
Storing signatures
02e93d53c8536aceb9a5538ae44b71c39722b31ccdb5038f68f74f509717f931
Spawning a container 'toolbox-core' with image 'registry.redhat.io/rhel9/support-tools'
Detected RUN label in the container image. Using that as the default...
f75904e189d79fd576c693531ff187d9b2daf0fd08970d769d96e0ec9b1db344
toolbox-core
Container started successfully. To exit, type 'exit'.
[root@master01 /]# ip -br link
lo                UNKNOWN      00:00:00:00:00:00 <LOOPBACK,UP,LOWER_UP>
ens3              UP          52:54:00:00:32:0a <BROADCAST,MULTICAST,UP,LOWER_UP>
ovs-system        DOWN        e6:ce:82:c9:55:df <BROADCAST,MULTICAST>
ovn-k8s-mp0       UNKNOWN    e2:87:b7:6e:5f:83 <BROADCAST,MULTICAST,UP,LOWER_UP>
genev_sys_6081    UNKNOWN    32:9b:11:d9:cd:c7 <BROADCAST,MULTICAST,UP,LOWER_UP>
br-int            DOWN        1a:70:b6:6d:c0:59 <BROADCAST,MULTICAST>
br-ex             UNKNOWN    52:54:00:00:32:0a <BROADCAST,MULTICAST,UP,LOWER_UP>
81c72927d86a77e@if2 UP          c6:76:97:82:be:90 <BROADCAST,MULTICAST,UP,LOWER_UP>
379ef916e04fb71@if2 UP          62:ae:33:9d:81:ff <BROADCAST,MULTICAST,UP,LOWER_UP>
2d6ad6e3de4cd3e@if2 UP          6e:31:0c:a5:a0:db <BROADCAST,MULTICAST,UP,LOWER_UP>
27c4132e218b2c1@if2 UP          6a:dd:58:bc:c1:0c <BROADCAST,MULTICAST,UP,LOWER_UP>
60fc034f38fd8f9@if2 UP          7e:b7:91:b7:89:75 <BROADCAST,MULTICAST,UP,LOWER_UP>
7bd300374770893@if2 UP          1e:53:39:a0:08:a3 <BROADCAST,MULTICAST,UP,LOWER_UP>
0ece3a09e4e4e89@if2 UP          76:8e:c4:07:ac:95 <BROADCAST,MULTICAST,UP,LOWER_UP>
16cc6ec9aecdb30@if2 UP          fa:eb:cb:4d:37:91 <BROADCAST,MULTICAST,UP,LOWER_UP>
6e70e5bd0d99445@if2 UP          6e:d1:29:0b:eb:22 <BROADCAST,MULTICAST,UP,LOWER_UP>
```

```
sh-5.1# tcpdump -w /tmp/ens3.pcap
dropped privs to tcpdump
tcpdump: listening on ens3, link-type EN10MB (Ethernet), snapshot length 262144 bytes
^C11745 packets captured
12064 packets received by filter
0 packets dropped by kernel
sh-5.1# cp /tmp/ens3.pcap /home/host/
sh-5.1# cp /tmp/ens3.pcap /home/host/
sh-5.1# mv /tmp/ens3.pcap /home/host/tmp/
sh-5.1#
```



```
[student@workstation ~]$ capinfos ens3.pcap
File name:          ens3.pcap
File type:          Wireshark/tcpdump/... - pcap
File encapsulation: Ethernet
File timestamp precision: microseconds (6)
Packet size limit:  file hdr: 262144 bytes
Number of packets:  11k
File size:          9748kB
Data size:          9560kB
Capture duration:   6.860851 seconds
First packet time:  2025-10-21 03:04:22.967802
Last packet time:   2025-10-21 03:04:29.828653
Data byte rate:     1393kBps
Data bit rate:      11Mbps
Average packet size: 814.03 bytes
Average packet rate: 1711 packets/s
SHA256:             54087d65a347182da16c8e85b144a51aae6fd1c8250da77872509467deb1f1f7
RIPEMD160:          d8d55ae1c38c9aec6b72a91ace4217442c5f0ea
SHA1:               5b10f38686ea9102b24f10c96ab31f8a5dc13ff5
Strict time order:  False
Number of interfaces in file: 1
Interface #0 info:
    Encapsulation = Ethernet (1 - ether)
    Capture length = 262144
    Time precision = microseconds (6)
    Time ticks per second = 1000000
    Number of stat entries = 0
    Number of packets = 11745
```

```

[student@workstation ~]$ tshark -r ens3.pcap -c30
 1  0.000000 192.168.50.12 → 192.168.50.11 TCP 66 45684 → 2379 [ACK] Seq=1 Ack=1 Win=800 Len=0 TSval=2919491341 TSecr=2428244694
 2  0.002372 192.168.50.11 → 192.168.50.10 TLSv1.2 209 Application Data
 3  0.002662 192.168.50.10 → 192.168.50.11 TCP 66 37686 → 10250 [ACK] Seq=1 Ack=144 Win=513 Len=0 TSval=1483964913 TSecr=2699152045
 4  0.015055 192.168.50.12 → 192.168.50.11 TCP 66 54510 → 2379 [ACK] Seq=1 Ack=1 Win=603 Len=0 TSval=2919491356 TSecr=2428244711
 5  0.026217 192.168.50.10 → 192.168.50.11 TCP 74 36127 → 2379 [SYN] Seq=0 Win=65280 Len=0 MSS=1360 SACK_PERM=1 TSval=244806269 TSecr=0 WS=128
 6  0.026325 192.168.50.11 → 192.168.50.10 TCP 74 2379 → 36127 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 TSval=2099152069 TSecr=244806269 WS=128
 7  0.026559 192.168.50.10 → 192.168.50.11 TCP 66 36127 → 2379 [ACK] Seq=1 Ack=1 Win=65280 Len=0 TSval=244806269 TSecr=2099152069
 8  0.026807 192.168.50.10 → 192.168.50.11 TLSv1 298 Client Hello
 9  0.026829 192.168.50.11 → 192.168.50.10 TCP 66 2379 → 36127 [ACK] Seq=1 Ack=233 Win=65024 Len=0 TSval=2099152069 TSecr=244806269
10  0.029182 192.168.50.11 → 192.168.50.10 TLSv1.3 2693 Server Hello, Change Cipher Spec, Application Data, Application Data, Application Data, A
pplication Data
11  0.029412 192.168.50.10 → 192.168.50.11 TCP 66 36127 → 2379 [ACK] Seq=233 Ack=2628 Win=69504 Len=0 TSval=244806272 TSecr=2099152071
12  0.031908 192.168.50.10 → 192.168.50.11 TLSv1.3 1295 Change Cipher Spec, Application Data, Application Data, Application Data
13  0.032010 192.168.50.10 → 192.168.50.11 TLSv1.3 112 Application Data
14  0.032036 192.168.50.11 → 192.168.50.10 TCP 66 2379 → 36127 [ACK] Seq=2628 Ack=1508 Win=63872 Len=0 TSval=2099152074 TSecr=244806274
15  0.032041 192.168.50.10 → 192.168.50.11 TLSv1.3 97 Application Data
16  0.032349 192.168.50.11 → 192.168.50.10 TLSv1.3 133 Application Data
17  0.032387 192.168.50.11 → 192.168.50.10 TLSv1.3 110 Application Data
18  0.032549 192.168.50.10 → 192.168.50.11 TCP 66 36127 → 2379 [ACK] Seq=1539 Ack=2739 Win=69504 Len=0 TSval=244806275 TSecr=2099152075
19  0.032700 192.168.50.10 → 192.168.50.11 TLSv1.3 97 Application Data
20  0.032838 192.168.50.10 → 192.168.50.11 TLSv1.3 209 Application Data
21  0.032875 192.168.50.11 → 192.168.50.10 TCP 66 2379 → 36127 [ACK] Seq=2739 Ack=1713 Win=63744 Len=0 TSval=2099152075 TSecr=244806275
22  0.033250 192.168.50.11 → 192.168.50.10 TLSv1.3 250 Application Data
23  0.033326 192.168.50.11 → 192.168.50.10 TLSv1.3 169 Application Data
24  0.033348 192.168.50.11 → 192.168.50.10 TLSv1.3 109 Application Data
25  0.033408 192.168.50.10 → 192.168.50.11 TCP 66 36127 → 2379 [ACK] Seq=1713 Ack=3078 Win=72192 Len=0 TSval=244806276 TSecr=2099152076
26  0.033581 192.168.50.10 → 192.168.50.11 TLSv1.3 118 Application Data
27  0.033610 192.168.50.10 → 192.168.50.11 TLSv1.3 130 Application Data
28  0.033659 192.168.50.11 → 192.168.50.10 TCP 66 2379 → 36127 [ACK] Seq=3078 Ack=1829 Win=63744 Len=0 TSval=2099152076 TSecr=244806276
29  0.033669 192.168.50.10 → 192.168.50.11 TCP 66 [TCP Previous segment not captured] 36127 → 2379 [FIN, ACK] Seq=1853 Ack=3078 Win=72192 Len=0 TSval=244806276 TSe
cr=2099152076
30  0.033670 192.168.50.10 → 192.168.50.11 TCP 90 [TCP Out-Of-Order] 36127 → 2379 [PSH, ACK] Seq=1829 Ack=3078 Win=72192 Len=24 TSval=244806276 TSecr=2099152076

```


Warns (257)

=====

Frequency	Group	Protocol	Summary
12	Sequence	TCP	Previous segment(s) not captured (common at capture start)
2	Sequence	TCP	This frame is a (suspected) out-of-order segment
71	Sequence	TCP	Connection reset (RST)
172	Sequence	TCP	ACKed segment that wasn't captured (common at capture start)

Notes (24)

=====

Frequency	Group	Protocol	Summary
10	Sequence	TCP	Duplicate ACK (#1)
10	Sequence	TCP	TCP keep-alive segment
4	Sequence	TCP	ACK to a TCP keep-alive segment

Chats (138)

=====

Frequency	Group	Protocol	Summary
15	Sequence	TCP	Connection establish request (SYN): server port 2379
15	Sequence	TCP	Connection establish acknowledge (SYN+ACK): server port 2379
59	Sequence	TCP	Connection finish (FIN)
8	Sequence	TCP	Connection establish request (SYN): server port 2380
8	Sequence	TCP	Connection establish acknowledge (SYN+ACK): server port 2380
7	Sequence	TCP	Connection establish request (SYN): server port 6443
3	Sequence	TCP	Connection establish request (SYN): server port 22623
3	Sequence	TCP	Connection establish request (SYN): server port 443
7	Sequence	TCP	Connection establish acknowledge (SYN+ACK): server port 6443
3	Sequence	TCP	Connection establish acknowledge (SYN+ACK): server port 22623
5	Sequence	TCP	Connection establish request (SYN): server port 10250
5	Sequence	TCP	Connection establish acknowledge (SYN+ACK): server port 10250


```
[student@workstation ~]$ tshark -r ens3.pcap -q -z conv,tcp
```

```
=====
```

TCP Conversations

Filter:<No Filter>

		<-		->		Total		Relative Start	Duration
		Frames	Bytes	Frames	Bytes	Frames	Bytes		
192.168.50.11:53694	<-> 192.168.50.12:2380	609	326kB	578	38kB	1187	364kB	0.077816000	0.6994
192.168.50.11:47164	<-> 192.168.50.10:2380	590	478kB	548	36kB	1138	514kB	0.077871000	0.7826
192.168.50.12:40928	<-> 192.168.50.11:2380	446	71kB	439	28kB	885	100kB	0.077324000	0.6996
192.168.50.10:33334	<-> 192.168.50.11:2380	421	67kB	416	27kB	837	95kB	0.077370000	0.6896
192.168.50.10:33134	<-> 192.168.50.11:2379	271	1846kB	214	47kB	485	1894kB	0.332050000	6.1501
192.168.50.12:54776	<-> 192.168.50.11:2379	236	1775kB	191	31kB	427	1807kB	0.332260000	6.1498
192.168.50.12:40936	<-> 192.168.50.11:2380	200	838kB	205	13kB	405	850kB	0.127244000	0.7338
192.168.50.10:33320	<-> 192.168.50.11:2380	192	835kB	195	12kB	387	848kB	0.127235000	0.3532
192.168.50.12:52277	<-> 192.168.50.11:6443	176	291kB	178	24kB	354	316kB	0.528942000	5.2725
192.168.50.13:40238	<-> 192.168.50.11:6443	156	470kB	179	17kB	335	487kB	5.945724000	0.2875
192.168.50.11:35554	<-> 192.168.50.254:6443	106	41kB	101	8839bytes	207	49kB	0.092886000	6.7154
192.168.50.254:53730	<-> 192.168.50.11:6443	106	41kB	100	8773bytes	206	49kB	0.092593000	6.7150
192.168.50.12:54456	<-> 192.168.50.11:2379	77	44kB	100	11kB	183	56kB	0.259700000	5.9692
192.168.50.10:41404	<-> 192.168.50.11:2379	75	44kB	101	10kB	176	54kB	0.257613000	5.9721
192.168.50.11:53766	<-> 192.168.50.10:2379	61	248kB	62	5313bytes	123	253kB	0.080715000	3.2944
192.168.50.11:55812	<-> 192.168.50.10:2379	58	214kB	51	48kB	109	263kB	0.308003000	4.5802
192.168.50.11:46408	<-> 192.168.50.254:6443	57	32kB	51	4585bytes	108	37kB	0.260528000	5.9686
10.0.0.2:59120	<-> 10.10.0.7:8443	50	33kB	49	7611bytes	99	41kB	6.437475000	0.0072
192.168.50.11:39086	<-> 192.168.50.12:2379	44	56kB	42	65kB	86	122kB	0.358398000	4.5977
192.168.50.12:54282	<-> 192.168.50.11:2379	42	254kB	37	3273bytes	79	257kB	0.716309000	3.0636
192.168.50.12:54270	<-> 192.168.50.11:2379	34	78kB	37	3212bytes	71	82kB	0.719531000	4.1306
10.0.0.2:56120	<-> 10.0.0.12:8443	31	15kB	46	6265bytes	77	21kB	6.437466000	0.0517
192.168.50.13:49364	<-> 192.168.50.11:6443	34	18kB	34	2388bytes	68	21kB	0.260071000	5.9286
192.168.50.12:54354	<-> 192.168.50.11:2379	28	48kB	34	2020bytes	62	51kB	0.935231000	5.1737
192.168.50.254:50520	<-> 192.168.50.11:6443	21	88kB	24	2787bytes	45	71kB	4.137849000	0.0530
192.168.50.12:59072	<-> 192.168.50.11:6443	22	17kB	28	3871bytes	42	21kB	0.079669000	6.7479
192.168.50.254:50530	<-> 192.168.50.11:6443	19	68kB	23	2625bytes	42	70kB	0.510571000	0.0497
10.0.0.2:60278	<-> 10.10.0.6:8443	17	9944bytes	20	3014bytes	37	12kB	6.440788000	0.0442
192.168.50.11:36230	<-> 192.168.50.10:2379	15	4178bytes	19	4158bytes	34	8336bytes	0.718433000	0.0106
192.168.50.12:33286	<-> 192.168.50.11:2379	14	4111bytes	19	3083bytes	33	7194bytes	0.517842000	0.0080
192.168.50.10:36127	<-> 192.168.50.11:2379	15	4120bytes	17	2958bytes	32	7084bytes	0.026217000	0.0077
192.168.50.10:41165	<-> 192.168.50.11:2379	13	4021bytes	19	3066bytes	32	7087bytes	5.444475000	0.0077
192.168.50.12:54546	<-> 192.168.50.11:2379	14	3468bytes	16	1704bytes	30	5184bytes	0.471933000	3.1696
192.168.50.12:34726	<-> 192.168.50.11:2379	13	3967bytes	17	2958bytes	30	6925bytes	5.021571000	0.0070
192.168.50.11:38564	<-> 192.168.50.12:2379	16	14kB	13	1412bytes	29	16kB	1.166576000	1.7934
192.168.50.11:55970	<-> 192.168.50.10:2379	13	13kB	16	1443bytes	29	14kB	1.171392000	1.5010
192.168.50.11:57840	<-> 192.168.50.254:6443	14	17kB	15	1173bytes	29	18kB	2.021363000	3.0870

```
[student@workstation ~]$ tshark -r ens3.pcap -q -z endpoints,ip
```

IPv4 Endpoints

Filter:<No Filter>

	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
192.168.50.11	11745	9560826	5745	7522620	6000	2038206
192.168.50.12	5663	4372897	2898	688871	2765	3684026
192.168.50.10	4522	4147939	2306	1172368	2216	2975571
192.168.50.254	879	407184	451	120791	428	286393
192.168.50.13	544	595740	278	43852	266	551888
10.9.0.2	332	127071	178	34449	154	92622
192.168.50.15	129	36250	63	11916	66	24334
10.10.0.7	99	41158	50	33547	49	7611
10.8.0.12	73	22243	32	15854	41	6389
10.8.2.8	68	32948	28	21152	40	11796
10.10.0.6	37	12958	17	9944	20	3014
10.11.0.17	17	8239	7	5288	10	2951
10.11.0.21	15	6254	6	894	9	5360
10.10.0.41	15	3359	8	2339	7	1020
10.8.0.33	12	2208	6	1312	6	896
10.8.0.11	11	3958	6	3186	5	772
10.9.0.63	9	4979	6	4532	3	447
192.168.50.14	8	816	4	408	4	408
10.9.0.64	6	1275	3	828	3	447

```
[student@workstation ~]$ oc get node -o custom-columns=Name:.metadata.name,IP:.status.addresses[].address
```

Name	IP
master01	192.168.50.10
master02	192.168.50.11
master03	192.168.50.12
worker01	192.168.50.13
worker02	192.168.50.14
worker03	192.168.50.15


```
[student@workstation ~]$ tshark -r ens3.pcap -q -T fields -e frame.protocols|sort -u
eth:ethertype:ip:tcp
eth:ethertype:ip:tcp:tls
eth:ethertype:ip:tcp:tls:tls
eth:ethertype:ip:udp:data
eth:ethertype:ip:udp:geneve:eth:ethertype:ip:tcp
eth:ethertype:ip:udp:geneve:eth:ethertype:ip:tcp:tls
5:eth:ethertype:ip:udp:geneve:eth:ethertype:ip:tcp:tls
```

```
a@sguzenko-thinkpadx1carbongen11:/var/tmp$ tshark -r worker01-worker02.pcap -q -T fields -e frame.protocols|sort -u
sll:ethertype:ip:tcp
sll:ethertype:ip:tcp:tls
sll:ethertype:ip:udp:data
sll:ethertype:ip:udp:geneve:eth:ethertype:ip:tcp
sll:ethertype:ip:udp:geneve:eth:ethertype:ip:tcp:http
sll:ethertype:ip:udp:geneve:eth:ethertype:ip:tcp:http:data-text-lines
sll:ethertype:ip:udp:geneve:eth:ethertype:ip:tcp:tls
```

oc get network cluster -o yaml

apiVersion: v1

items:

- apiVersion: config.openshift.io/v1

kind: Network

metadata:

name: cluster

spec:

clusterNetwork:

- cidr: 10.8.0.0/14

hostPrefix: 23

externalIP:

policy: {}

networkType: OVNKubernetes

serviceNetwork:

- 172.30.0.0/16

status:

clusterNetwork:

- cidr: 10.8.0.0/14

hostPrefix: 23

clusterNetworkMTU: 1400

apiVersion: v1

items:

- apiVersion: config.openshift.io/v1

kind: Network

metadata:

name: cluster

spec:

clusterNetwork:

- cidr: 10.8.0.0/14

hostPrefix: 23

externalIP:

policy: {}

networkType: OVNKubernetes

serviceNetwork:

- 172.30.0.0/16

status:

clusterNetwork:

- cidr: 10.8.0.0/14

hostPrefix: 23

clusterNetworkMTU: 1400

IP ranges for containers and services

apiVersion: v1

items:

- apiVersion: config.openshift.io/v1

kind: Network

metadata:

name: cluster

spec:

clusterNetwork:

- cidr: 10.8.0.0/14

hostPrefix: 23

externalIP:

policy: {}

networkType: OVNKubernetes

serviceNetwork:

- 172.30.0.0/16

status:

clusterNetwork:

- cidr: 10.8.0.0/14

hostPrefix: 23

clusterNetworkMTU: 1400

apiVersion: v1

items:

- apiVersion: config.openshift.io/v1

kind: Network

metadata:

name: cluster

spec:

clusterNetwork:

- cidr: 10.8.0.0/14

hostPrefix: 23

externalIP:

policy: {}

networkType: OVNKubernetes

serviceNetwork:

- 172.30.0.0/16

status:

clusterNetwork:

- cidr: 10.8.0.0/14

hostPrefix: 23

clusterNetworkMTU: 1400

OpenShift CNl plugin

OpenShift Version	CNI plugin	Encapsulation protocol
4.12+	OVN-Kubernetes	Geneve
3.x–4.11	OpenShift SDN	VXLAN

Internet Engineering Task Force (IETF)

[8926](#)

Standards Track

November 2020

2070-1721

J. Gross, Ed.

I. Ganga, Ed.

Intel

T. Sridhar, Ed.

VMware

Geneve: Generic Network Virtualization Encapsulation

Abstract

Network virtualization involves the cooperation of devices with a wide variety of capabilities such as software and hardware tunnel endpoints, transit fabrics, and centralized control clusters. As a result of their role in tying together different elements of the system, the requirements on tunnels are influenced by all of these components. Therefore, flexibility is the most important aspect of a tunneling protocol if it is to keep pace with the evolution of technology. This document describes Geneve, an encapsulation protocol designed to recognize and accommodate these changing capabilities and needs.

```
[student@workstation ~]$ tshark -r ens3.pcap -q -T fields -e frame.protocols|sort -u
eth:ethertype:ip:tcp
eth:ethertype:ip:tcp:tls
eth:ethertype:ip:tcp:tls:tls
eth:ethertype:ip:udp:data
eth:ethertype:ip:udp:geneve:eth:ethertype:ip:tcp
eth:ethertype:ip:udp:geneve:eth:ethertype:ip:tcp:tls
```

```
a@sguzenko-thinkpadx1carbongen11:/var/tmp$ tshark -r worker01-worker02.pcap -q -T fields -e frame.protocols|sort -u
sll:ethertype:ip:tcp
sll:ethertype:ip:tcp:tls
sll:ethertype:ip:udp:data
sll:ethertype:ip:udp:geneve:eth:ethertype:ip:tcp
sll:ethertype:ip:udp:geneve:eth:ethertype:ip:tcp:http
sll:ethertype:ip:udp:geneve:eth:ethertype:ip:tcp:http:data-text-lines
sll:ethertype:ip:udp:geneve:eth:ethertype:ip:tcp:tls
```

```
[student@workstation ~]$ tshark -r ens3.pcap -q -T fields -e frame.protocols|sort -u
eth:ethertype:ip:tcp
eth:ethertype:ip:tcp:tls
eth:ethertype:ip:tcp:tls:tls
eth:ethertype:ip:udp:data
eth:ethertype:ip:udp:geneve:eth:ethertype:ip:tcp
eth:ethertype:ip:udp:geneve:eth:ethertype:ip:tcp:tls
```

```
a@sguzenko-thinkpadx1carbongen11:/var/tmp$ tshark -r worker01-worker02.pcap -q -T fields -e frame.protocols|sort -u
sll:ethertype:ip:tcp
sll:ethertype:ip:tcp:tls
sll:ethertype:ip:udp:data
sll:ethertype:ip:udp:geneve:eth:ethertype:ip:tcp
sll:ethertype:ip:udp:geneve:eth:ethertype:ip:tcp:http
sll:ethertype:ip:udp:geneve:eth:ethertype:ip:tcp:http:data-text-lines
sll:ethertype:ip:udp:geneve:eth:ethertype:ip:tcp:tls
```

http

tls

tcp

ip

eth

gene
ve

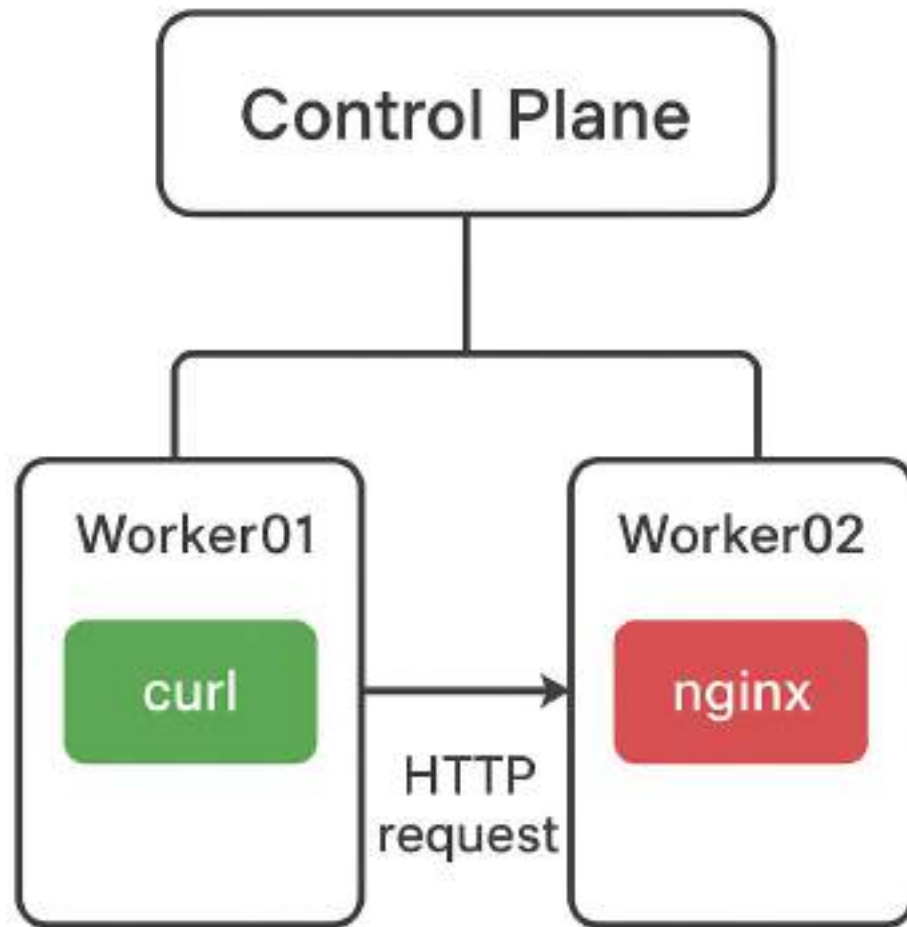
udp

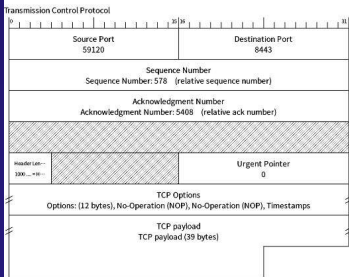
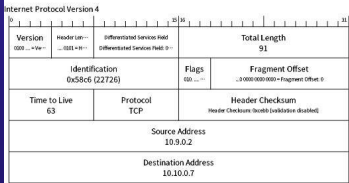
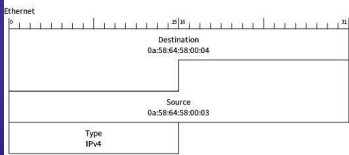
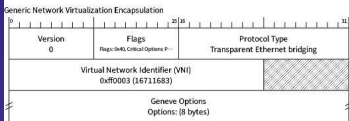
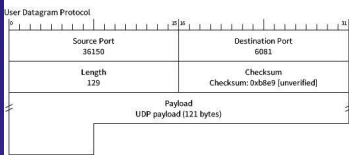
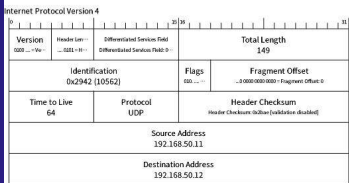
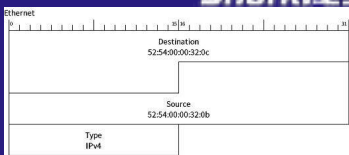
ip

eth

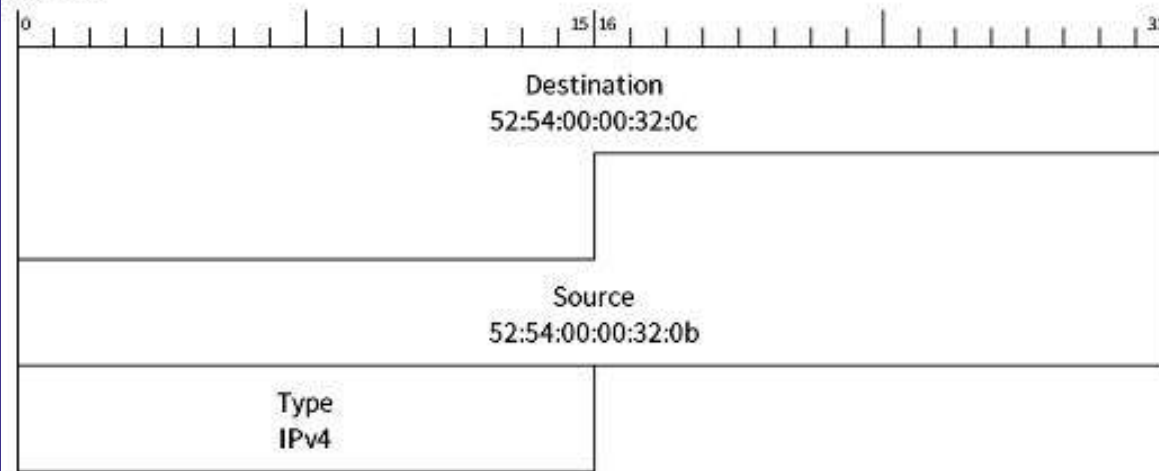

```
[student@workstation ~]$ tshark -r ens3.pcap -q -T fields -e frame.protocols|sort -u
eth:ethertype:ip:tcp
eth:ethertype:ip:tcp:tls
eth:ethertype:ip:tcp:tls:tls
eth:ethertype:ip:udp:data
eth:ethertype:ip:udp:geneve:eth:ethertype:ip:tcp
eth:ethertype:ip:udp:geneve:eth:ethertype:ip:tcp:tls
```

- Frame 11003: Packet, 188 bytes on wire (1504 bits), 188 bytes captured (1504 bits)
- Ethernet II, Src: 52:54:00:00:32:0c (52:54:00:00:32:0c), Dst: 52:54:00:00:32:0b (52:54:00:00:32:0b)
- Internet Protocol Version 4, Src: 192.168.50.12 (192.168.50.12), Dst: api.ocp4.example.com (192.168.50.11)
- User Datagram Protocol, Src Port: 41221, Dst Port: 6081
- Generic Network Virtualization Encapsulation, VNI: 0xff0003
 - Version: 0
 - Length: 8 bytes
 - Flags: 0x40, Critical Options Present
 - 0... = Operations, Administration and Management Frame: False
 - .1... = Critical Options Present: True
 - ..00 0000 = Reserved: False
 - Protocol Type: Transparent Ethernet bridging (0x6558)
 - Virtual Network Identifier (VNI): 0xff0003 (16711683)
 - Options: (8 bytes)
 - Unknown, Class: Open Virtual Networking (OVN) (0x0102) Type: 0x80 (Critical)
 - Class: Open Virtual Networking (OVN) (0x0102)
 - Type: 0x80 (Critical)
 - Length: 8 bytes
 - Unknown Option Data: 00040003
- Ethernet II, Src: 0a:58:64:58:00:04 (0a:58:64:58:00:04), Dst: 0a:58:64:58:00:03 (0a:58:64:58:00:03)
- Internet Protocol Version 4, Src: 10.10.0.7 (10.10.0.7), Dst: 10.9.0.2 (10.9.0.2)
- Transmission Control Protocol, Src Port: 8443, Dst Port: 59120, Seq: 5344, Ack: 504, Len: 64
- Transport Layer Security

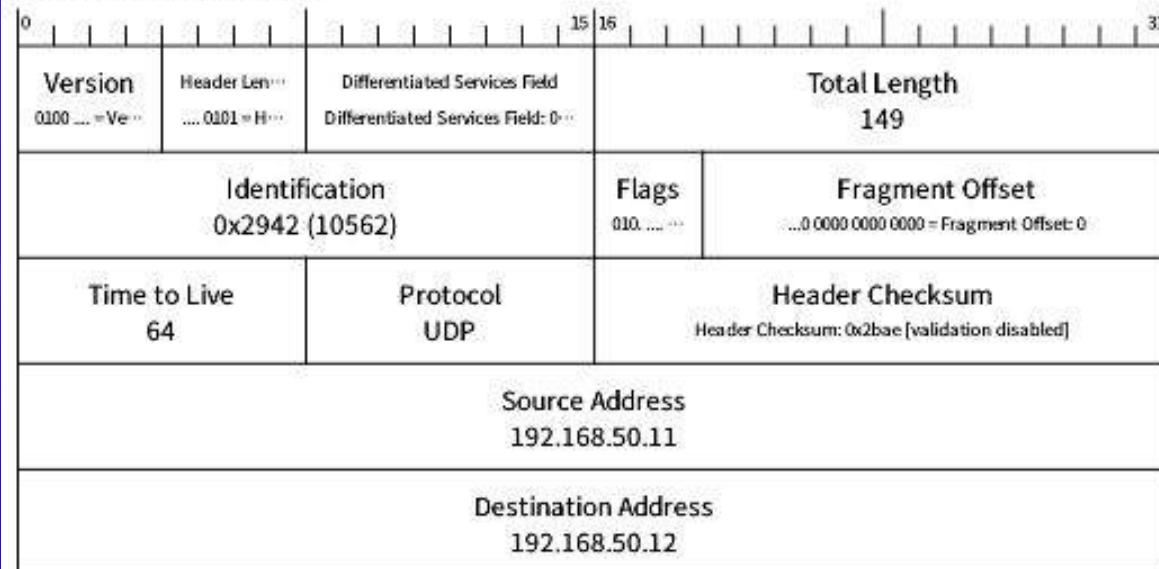




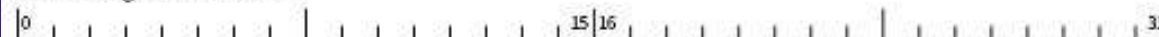
Ethernet

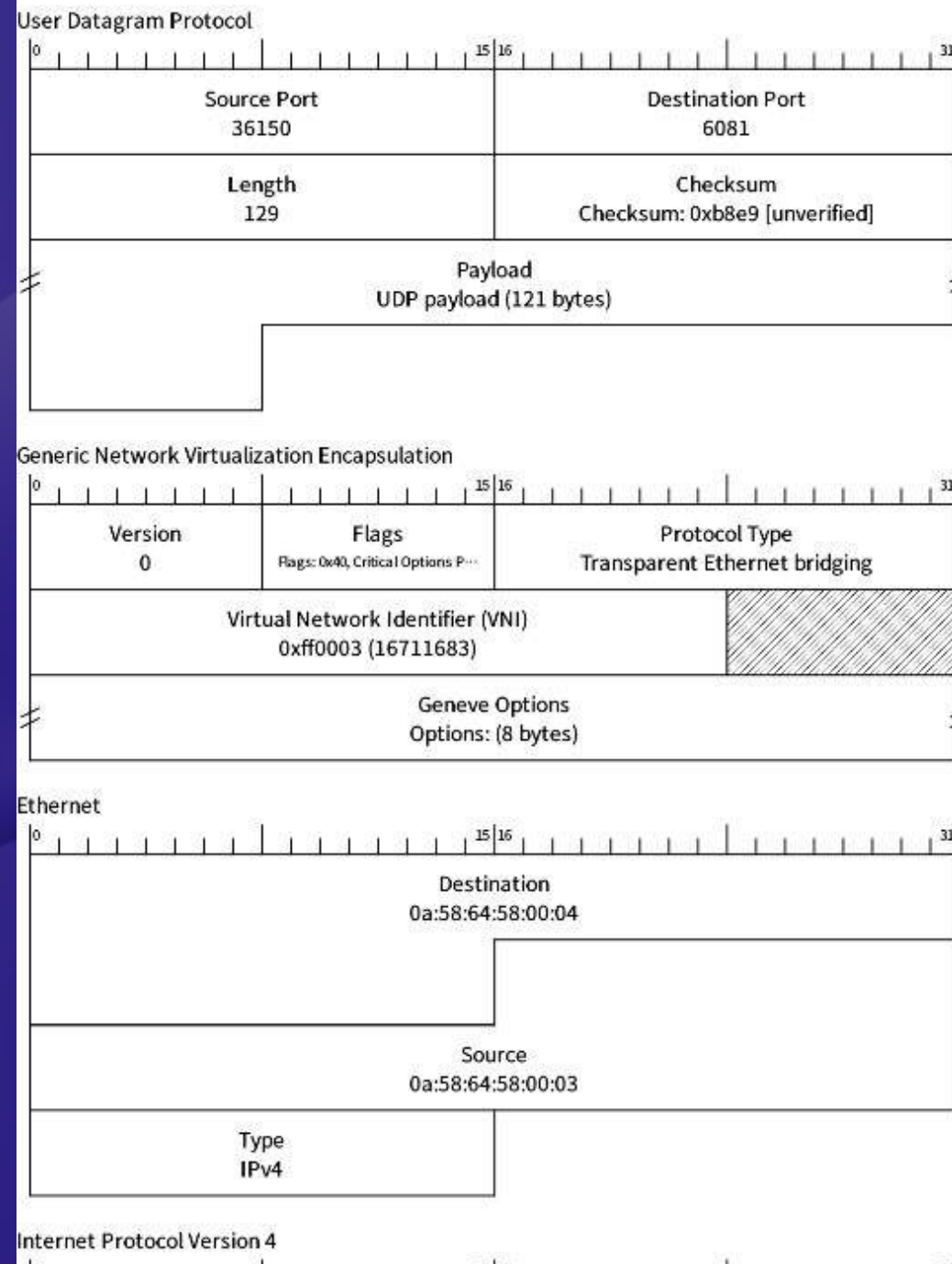


Internet Protocol Version 4



User Datagram Protocol





Internet Protocol Version 4

0																15																30																45																60																75																90																105																120																135																150																165																180																195																210																225																240																255															
Version 0100 ... = Ver...																Header Len... ... 0101 = H...																Differentiated Services Field Differentiated Services Field: 0...																Total Length 91																																																																																																																																																																																																																																															
Identification 0x58c6 (22726)																																																Flags 010.																Fragment Offset ...0 0000 0000 0000 = Fragment Offset: 0																																																																																																																																																																																																																															
Time to Live 63																								Protocol TCP																								Header Checksum Header Checksum: 0xcebb [validation disabled]																																																																																																																																																																																																																																															
Source Address 10.9.0.2																																																																																																																																																																																																																																																																																															
Destination Address 10.10.0.7																																																																																																																																																																																																																																																																																															

Transmission Control Protocol

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31																															
Source Port 59120																Destination Port 8443															
Sequence Number Sequence Number: 578 (relative sequence number)																															
Acknowledgment Number Acknowledgment Number: 5408 (relative ack number)																															
Header Len... 1000 = H...																Urgent Pointer 0															
TCP Options Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps																															
TCP payload TCP payload (39 bytes)																															

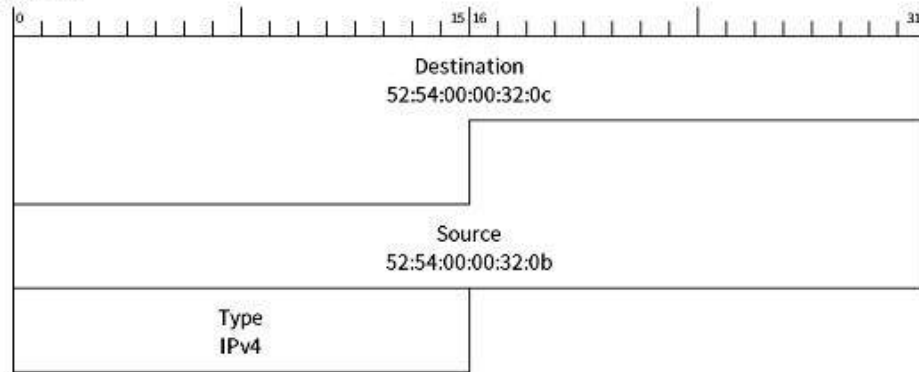
Transport Layer Security

0 15 16 a

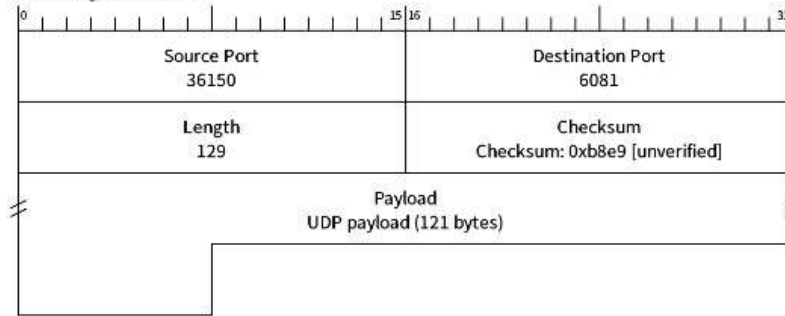
TLv1.2 Record Layer: Application Data Protocol: Application Data

example of a single encapsulated packet

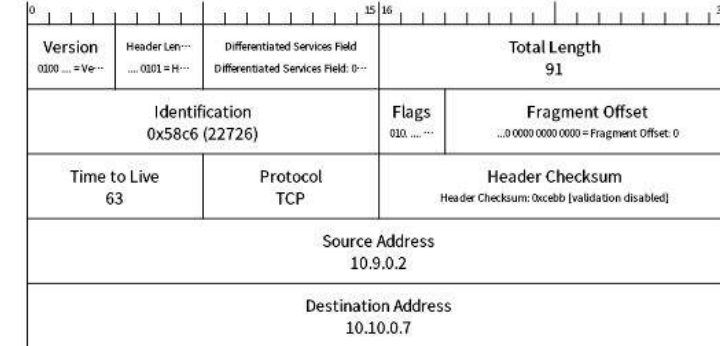
Ethernet



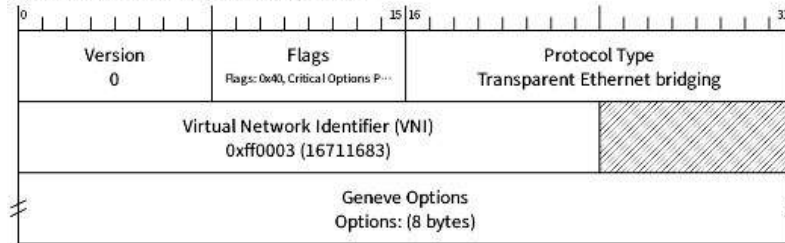
User Datagram Protocol



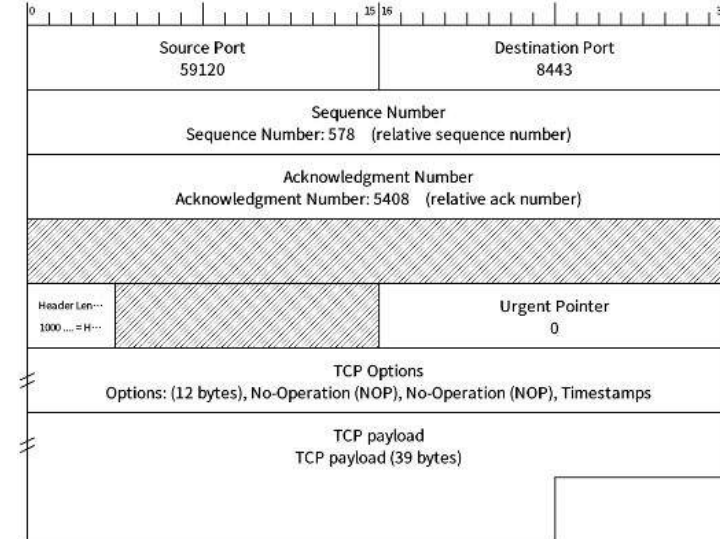
Internet Protocol Version 4



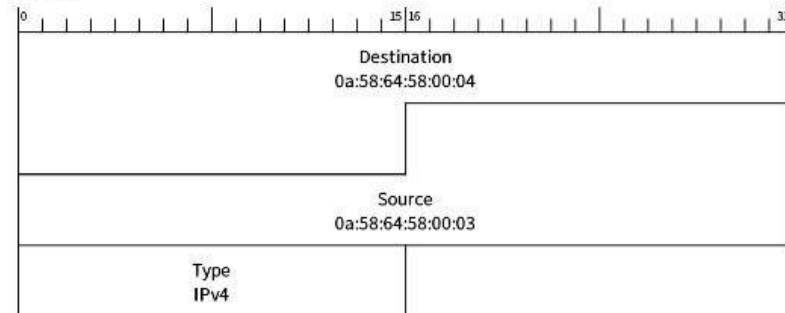
Generic Network Virtualization Encapsulation



Transmission Control Protocol



Ethernet

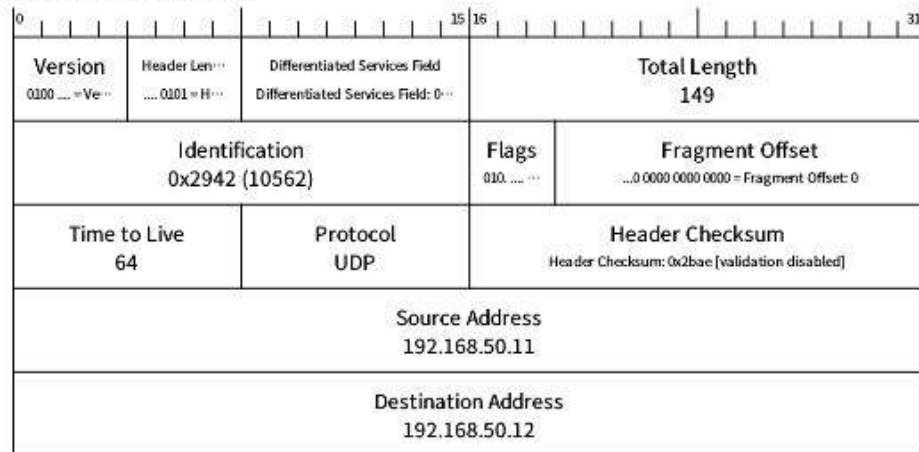


Internet Protocol Version 4

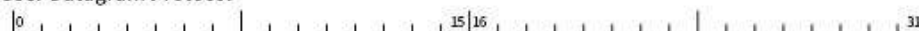
Transport Layer Security

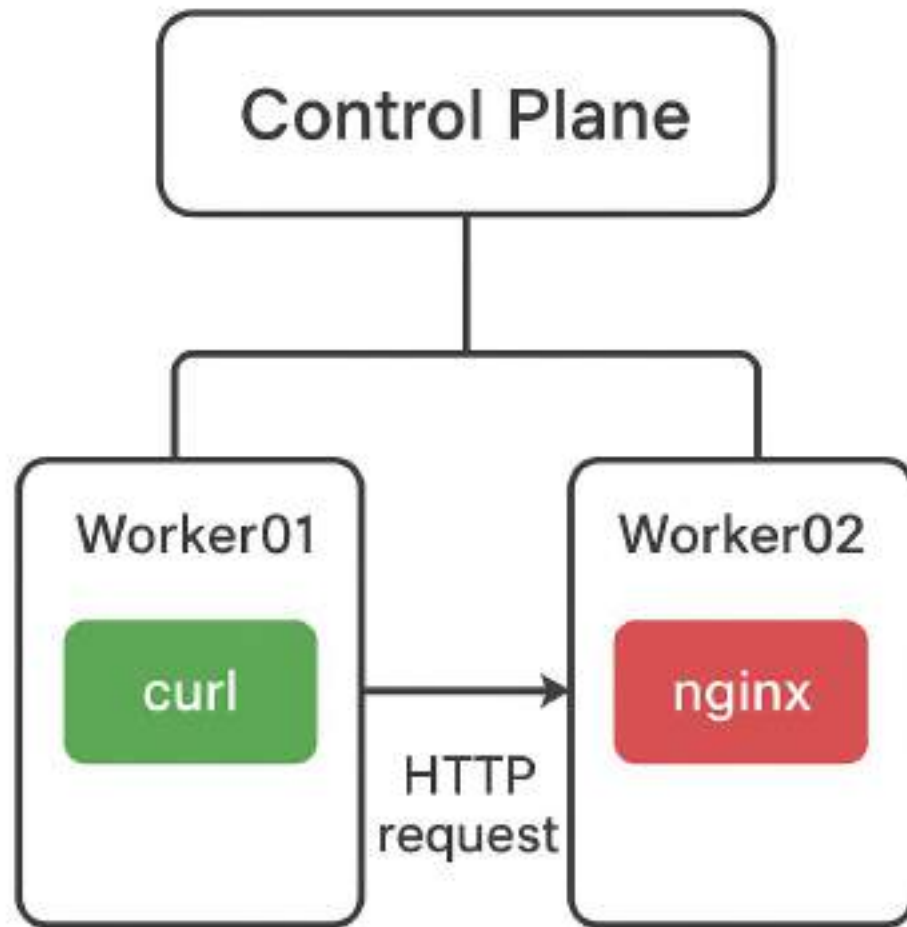


Internet Protocol Version 4



User Datagram Protocol






```
[student@workstation ~]$ oc create ns sharkproject-a
namespace/sharkproject-a created
[student@workstation ~]$ oc create ns sharkproject-b
namespace/sharkproject-b created
[student@workstation ~]$ oc annotate ns/sharkproject-a openshift.io/node-selector=region=A
namespace/sharkproject-a annotated
[student@workstation ~]$ oc annotate ns/sharkproject-b openshift.io/node-selector=region=B
namespace/sharkproject-b annotated
[student@workstation ~]$ oc get node -lregion
```

NAME	STATUS	ROLES	AGE	VERSION	REGION
master01	Ready	control-plane,master	368d	v1.33.5	
master02	Ready	control-plane,master	368d	v1.33.5	
master03	Ready	control-plane,master	368d	v1.33.5	
worker01	Ready	worker	361d	v1.33.5	A
worker02	Ready	worker	361d	v1.33.5	B
worker03	Ready	worker	361d	v1.33.5	

```
[student@workstation ~]$ oc project sharkproject-a
Already on project "sharkproject-a" on server "https://api.ocp4.example.com:6443".
[student@workstation ~]$ oc new-app --name shark-a --image quay.io/sguzenko/shark
--> Found container image 9e96692 (16 hours old) from quay.io for "quay.io/sguzenko/shark"
```

* An image stream tag will be created as "shark-a:latest" that will track this image

```
--> Creating resources ...
imagestream.image.openshift.io "shark-a" created
deployment.apps "shark-a" created
service "shark-a" created
--> Success
Application is not exposed. You can expose services to the outside world by executing one or more of the commands below:
'oc expose service/shark-a'
Run 'oc status' to view your app.
```

```
[student@workstation ~]$ oc get all
Warning: apps.openshift.io/v1 DeploymentConfig is deprecated in v4.14+, unavailable in v4.16.0.0+
```

NAME	READY	STATUS	RESTARTS	AGE
pod/shark-a-ff7cdd4d8-gzwns	1/1	Running	0	23s

NAME	TYPE	CLUSTER-IP	EXTERNAL-IP	PORT(S)	AGE
service/shark-a	ClusterIP	172.30.91.250	<none>	8080/TCP	23s

NAME	READY	UP-TO-DATE	AVAILABLE	AGE
deployment.apps/shark-a	1/1	1	1	23s

NAME	DESIRED	CURRENT	READY	AGE
replicaset.apps/shark-a-5b5b4f4488	0	0	0	23s
replicaset.apps/shark-a-ff7cdd4d8	1	1	1	23s

NAME	IMAGE REPOSITORY	TAGS	UPDATED
imagestream.image.openshift.io/shark-a	default-route-openshift-image-registry.apps.ocp4.example.com/sharkproject-a/shark-a	latest	23 seconds ago

```
[student@workstation ~]$ oc project sharkproject-b
Now using project "sharkproject-b" on server "https://api.ocp4.example.com:6443".
[student@workstation ~]$ oc new-app --name shark-b --image quay.io/sguzenko/shark
--> Found container image 9e06092 (16 hours old) from quay.io for "quay.io/sguzenko/shark"

* An image stream tag will be created as "shark-b:latest" that will track this image

--> Creating resources ...
  imagestream.image.openshift.io "shark-b" created
  deployment.apps "shark-b" created
  service "shark-b" created
--> Success
  Application is not exposed. You can expose services to the outside world by executing one or more of the commands below:
  'oc expose service/shark-b'
  Run 'oc status' to view your app.
[student@workstation ~]$ oc get all
Warning: apps.openshift.io/v1 DeploymentConfig is deprecated in v4.14+, unavailable in v4.10000+
NAME                                READY    STATUS    RESTARTS   AGE
pod/shark-b-6ddc49b8cd-n9qsh        1/1      Running   0           7s

NAME                                TYPE           CLUSTER-IP    EXTERNAL-IP  PORT(S)    AGE
service/shark-b                     ClusterIP      172.30.82.218 <none>       8080/TCP    7s

NAME                                READY    UP-TO-DATE   AVAILABLE   AGE
deployment.apps/shark-b             1/1      1            1           7s

NAME                                DESIRED    CURRENT    READY    AGE
replicaset.apps/shark-b-6ddc49b8cd  1          1          1        7s
replicaset.apps/shark-b-f594dd99b   0          0          0        7s

NAME                                IMAGE REPOSITORY                                TAGS    UPDATED
imagestream.image.openshift.io/shark-b default-route-openshift-image-registry.apps.ocp4.example.com/sharkproject-b/shark-b latest  7 seconds ago
```

```
[student@workstation ~]$ oc get po -o wide -n sharkproject-a
```

NAME	READY	STATUS	RESTARTS	AGE	IP	NODE	NOMINATED	NODE	READINESS	GATES
shark-a-ff7cdd4d8-gzmms	1/1	Running	0	21m	10.8.2.128	worker01	<none>		<none>	

```
[student@workstation ~]$ oc get po -o wide -n sharkproject-b
```

NAME	READY	STATUS	RESTARTS	AGE	IP	NODE	NOMINATED	NODE	READINESS	GATES
shark-b-6ddc49b8cd-n9qsh	1/1	Running	0	17m	10.9.2.34	worker02	<none>		<none>	

```
[student@workstation ~]$ oc exec deploy/shark-b -- curl 10.8.2.128:8080 -s
```

Welcome to Sharkfest 2025


```
[student@workstation ~]$ ssh core@worker01 -Jlab@utility
Warning: Permanently added 'worker01' (E025519) to the list of known hosts.
Red Hat Enterprise Linux CoreOS 9.0.20251021-0
Part of OpenShift 4.20, RHCOS is a Kubernetes-native operating system
managed by the Machine Config Operator ('clusteroperator/machine-config').

WARNING: Direct SSH access to machines is not recommended; instead,
make configuration changes via 'machineconfig' objects:
https://docs.openshift.com/container-platform/4.20/architecture/architecture-rhcos.html
```

```
[core@worker01 ~]$ toolbox
Trying to pull registry.redhat.io/rhel9/support-tools:latest...
Getting image source signatures
Checking if image destination supports signatures
Copying blob 7d071e8fe18e done |
Copying blob 35d8a5cc08a1 skipped: already exists
Copying config 02e83d53c8 done |
Writing manifest to image destination
Storing signatures
02e93d53c8536aceb0a5538ae44b71c30722b3fcdab5638f60f74f590717f93f
Spawning a container 'toolbox-core' with image 'registry.redhat.io/rhel9/support-tools'
Detected RUN label in the container image, using that as the default...
23c90b0943ae0513d200b1dc1fe7ce08d4704e0e01055e4f00d0055f3bb4c480
toolbox-core
Container started successfully. To exit, type 'exit'.
[root@worker01 /]# tcpdump -i any host 10.8.2.128
tcpdump: data link type LINUX_SLL2
dropped privs to tcpdump
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on any, link-type LINUX_SLL2 (Linux cooked v2), snapshot length 262144 bytes
03:43:59.102354 genev.sys_0001 P IP 10.8.2.34.54576 > 10.8.2.128.webcache: Flags [S], seq 419467409, win 65280, options [mss 1360,sackOK,TS val 2792630638 ecr 0,nop,wscale 7], length 0
03:43:59.103394 5fc577751b5f4eb Out IP 10.8.2.34.54576 > 10.8.2.128.webcache: Flags [S], seq 419467409, win 65280, options [mss 1360,sackOK,TS val 2792630638 ecr 0,nop,wscale 7], length 0
03:43:59.103440 5fc577751b5f4eb P IP 10.8.2.128.webcache > 10.8.2.34.54576: Flags [S.], seq 2843882782, ack 419467410, win 64704, options [mss 1360,sackOK,TS val 3168200031 ecr 2792630638,nop,wscale 7], length 0
03:43:59.103823 genev.sys_6001 Out IP 10.8.2.128.webcache > 10.8.2.34.54576: Flags [S.], seq 2843882782, ack 419467410, win 64704, options [mss 1360,sackOK,TS val 3168200031 ecr 2792630638,nop,wscale 7], length 0
03:43:59.105213 genev.sys_6001 P IP 10.8.2.34.54576 > 10.8.2.128.webcache: Flags [.], ack 1, win 510, options [nop,nop,TS val 2792630642 ecr 3168200031], length 0
03:43:59.105390 genev.sys_0001 P IP 10.8.2.34.54576 > 10.8.2.128.webcache: Flags [P.], seq 1:80, ack 1, win 510, options [nop,nop,TS val 2792630642 ecr 3168200031], length 79: HTTP: GET / HTTP/1.1
03:43:59.105450 5fc577751b5f4eb Out IP 10.8.2.34.54576 > 10.8.2.128.webcache: Flags [.], ack 1, win 510, options [nop,nop,TS val 2792630642 ecr 3168200031], length 0
03:43:59.105564 5fc577751b5f4eb Out IP 10.8.2.34.54576 > 10.8.2.128.webcache: Flags [P.], seq 1:80, ack 1, win 510, options [nop,nop,TS val 2792630642 ecr 3168200031], length 79: HTTP: GET / HTTP/1.1
03:43:59.105577 5fc577751b5f4eb P IP 10.8.2.128.webcache > 10.8.2.34.54576: Flags [-.], ack 80, win 505, options [nop,nop,TS val 316820003 ecr 2792630642], length 0
03:43:59.105588 genev.sys_6001 Out IP 10.8.2.128.webcache > 10.8.2.34.54576: Flags [.], ack 80, win 505, options [nop,nop,TS val 316820003 ecr 2792630642], length 0
03:43:59.105836 5fc577751b5f4eb P IP 10.8.2.128.webcache > 10.8.2.34.54576: Flags [F.], seq 1:263, ack 80, win 505, options [nop,nop,TS val 316820003 ecr 2792630642], length 262: HTTP: HTTP/1.1 200 OK
03:43:59.105855 genev.sys_0001 Out IP 10.8.2.128.webcache > 10.8.2.34.54576: Flags [P.], seq 1:263, ack 80, win 505, options [nop,nop,TS val 316820003 ecr 2792630642], length 262: HTTP: HTTP/1.1 200 OK
03:43:59.106003 genev.sys_0001 P IP 10.8.2.34.54576 > 10.8.2.128.webcache: Flags [.], ack 263, win 500, options [nop,nop,TS val 2792630643 ecr 316820003], length 0
03:43:59.106118 5fc577751b5f4eb Out IP 10.8.2.34.54576 > 10.8.2.128.webcache: Flags [.], ack 263, win 500, options [nop,nop,TS val 2792630643 ecr 316820003], length 0
03:43:59.106199 genev.sys_0001 P IP 10.8.2.34.54576 > 10.8.2.128.webcache: Flags [F.], seq 80, ack 263, win 500, options [nop,nop,TS val 2792630643 ecr 316820003], length 0
03:43:59.106206 5fc577751b5f4eb Out IP 10.8.2.34.54576 > 10.8.2.128.webcache: Flags [F.], seq 80, ack 263, win 500, options [nop,nop,TS val 2792630643 ecr 316820003], length 0
03:43:59.106250 5fc577751b5f4eb P IP 10.8.2.128.webcache > 10.8.2.34.54576: Flags [F.], seq 263, ack 81, win 505, options [nop,nop,TS val 316820003 ecr 2792630643], length 0
03:43:59.106256 genev.sys_6001 Out IP 10.8.2.128.webcache > 10.8.2.34.54576: Flags [F.], seq 263, ack 81, win 505, options [nop,nop,TS val 316820003 ecr 2792630643], length 0
03:43:59.106421 genev.sys_0001 P IP 10.8.2.34.54576 > 10.8.2.128.webcache: Flags [.], ack 264, win 500, options [nop,nop,TS val 2792630644 ecr 316820003], length 0
03:43:59.106430 5fc577751b5f4eb Out IP 10.8.2.34.54576 > 10.8.2.128.webcache: Flags [.], ack 264, win 500, options [nop,nop,TS val 2792630644 ecr 316820003], length 0
03:44:04.271351 5fc577751b5f4eb P ARP Request who-has 10.8.2.1 tell 10.8.2.128, length 28
03:44:04.271674 5fc577751b5f4eb Out ARP, Reply 10.8.2.1 is-at 0a:58:a9:fe:01:01 (oui Unknown), length 28
```



```

NAME                READY   STATUS    RESTARTS   AGE     IP            NODE          NOMINATED NODE   READINESS GATES
shark-b-6ddc49b8cd-n9qsh  1/1     Running   0           7m50s   10.9.2.34     worker02      <none>           <none>
[student@workstation ~]$ oc get po -o wide -n sharkproject-a
NAME                READY   STATUS    RESTARTS   AGE     IP            NODE          NOMINATED NODE   READINESS GATES
shark-a-ff7cdd4d8-gzmms  1/1     Running   0           12m     10.8.2.128     worker01      <none>           <none>
[student@workstation ~]$ oc get po -o wide -n sharkproject-a,sharkproject-b
No resources found in sharkproject-a,sharkproject-b namespace.
[student@workstation ~]$ oc get svc -n sharkproject-a
NAME      TYPE        CLUSTER-IP    EXTERNAL-IP   PORT(S)    AGE
shark-a   ClusterIP   172.30.91.250 <none>        8080/TCP   13m
[student@workstation ~]$ oc get svc -n sharkproject-b
NAME      TYPE        CLUSTER-IP    EXTERNAL-IP   PORT(S)    AGE
shark-b   ClusterIP   172.30.82.218 <none>        8080/TCP   9m14s

```

```
[root@worker01 /]# tcpdump -i any -w /host/var/tmp/worker01-worker02.pcap -nn host 192.168.50.13 and host 192.168.50.14
tcpdump: data link type LINUX_SLL2
dropped privs to tcpdump
tcpdump: listening on any, link-type LINUX_SLL2 (Linux cooked v2), snapshot length 262144 bytes
^C63 packets captured
74 packets received by filter
0 packets dropped by kernel
```

```
[student@workstation ~]$ oc exec deploy/shark-b -- curl 10.8.2.128:8080 -s
Welcome to Sharkfest 2025
```

```
a@sguzenko-thinkpadx1carbongen11:/var/tmp$ tshark -r worker01-worker02.pcap -q -T fields -e frame.protocols|sort -u
sll:ethertype:ip:tcp
sll:ethertype:ip:tcp:tls
sll:ethertype:ip:udp:data
sll:ethertype:ip:udp:geneve:eth:ethertype:ip:tcp
sll:ethertype:ip:udp:geneve:eth:ethertype:ip:tcp:http
sll:ethertype:ip:udp:geneve:eth:ethertype:ip:tcp:http:data-text-lines
sll:ethertype:ip:udp:geneve:eth:ethertype:ip:tcp:tls
```

Team: [Name] Problem Statement: [Text] Solution: [Text] Impact: [Text] Team Members: [List] Coaches: [List] Project Description: [Text] Business Model: [Text] Market Analysis: [Text] Financial Projections: [Text] Risk Assessment: [Text] Conclusion: [Text]	Team: [Name] Problem Statement: [Text] Solution: [Text] Impact: [Text] Team Members: [List] Coaches: [List] Project Description: [Text] Business Model: [Text] Market Analysis: [Text] Financial Projections: [Text] Risk Assessment: [Text] Conclusion: [Text]	Team: [Name] Problem Statement: [Text] Solution: [Text] Impact: [Text] Team Members: [List] Coaches: [List] Project Description: [Text] Business Model: [Text] Market Analysis: [Text] Financial Projections: [Text] Risk Assessment: [Text] Conclusion: [Text]	Team: [Name] Problem Statement: [Text] Solution: [Text] Impact: [Text] Team Members: [List] Coaches: [List] Project Description: [Text] Business Model: [Text] Market Analysis: [Text] Financial Projections: [Text] Risk Assessment: [Text] Conclusion: [Text]	Team: [Name] Problem Statement: [Text] Solution: [Text] Impact: [Text] Team Members: [List] Coaches: [List] Project Description: [Text] Business Model: [Text] Market Analysis: [Text] Financial Projections: [Text] Risk Assessment: [Text] Conclusion: [Text]	Team: [Name] Problem Statement: [Text] Solution: [Text] Impact: [Text] Team Members: [List] Coaches: [List] Project Description: [Text] Business Model: [Text] Market Analysis: [Text] Financial Projections: [Text] Risk Assessment: [Text] Conclusion: [Text]	Team: [Name] Problem Statement: [Text] Solution: [Text] Impact: [Text] Team Members: [List] Coaches: [List] Project Description: [Text] Business Model: [Text] Market Analysis: [Text] Financial Projections: [Text] Risk Assessment: [Text] Conclusion: [Text]
---	---	---	---	---	---	---

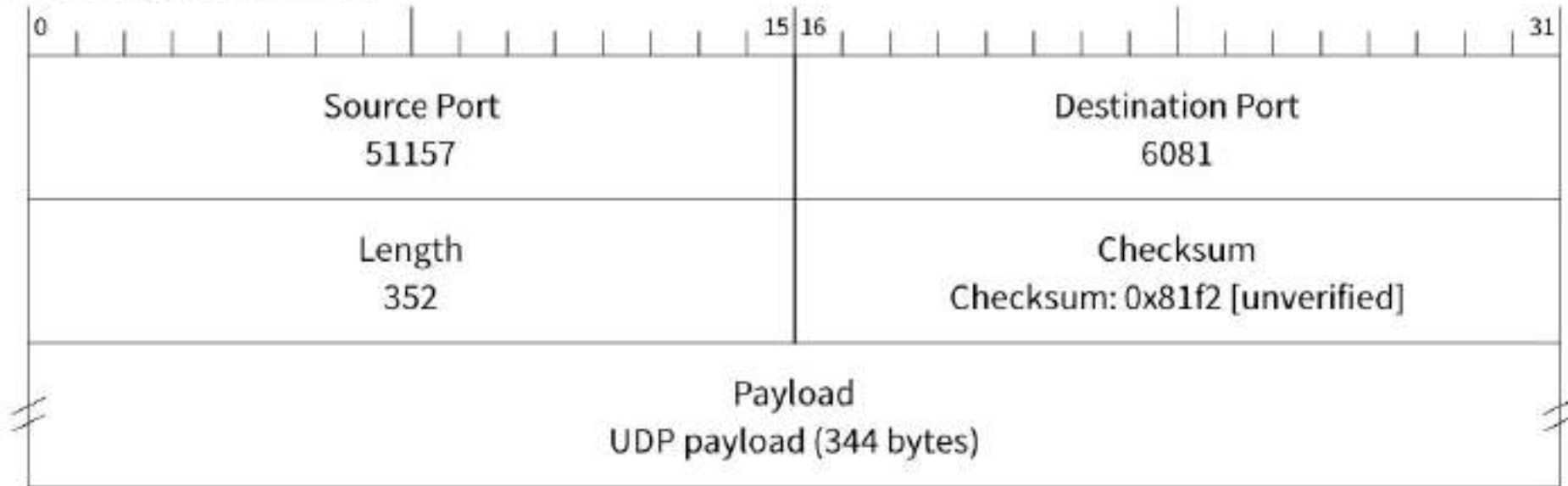
Linux cooked-mode capture

0																15																16																31															
Protocol IPv4																Reserved 0000																																															
Interface index 8																																																															
Link-layer address type Ethernet																																Packet type Sent by us																Link-layer address length 6															
Source 52:54:00:00:32:0d																																Unused 0000																															

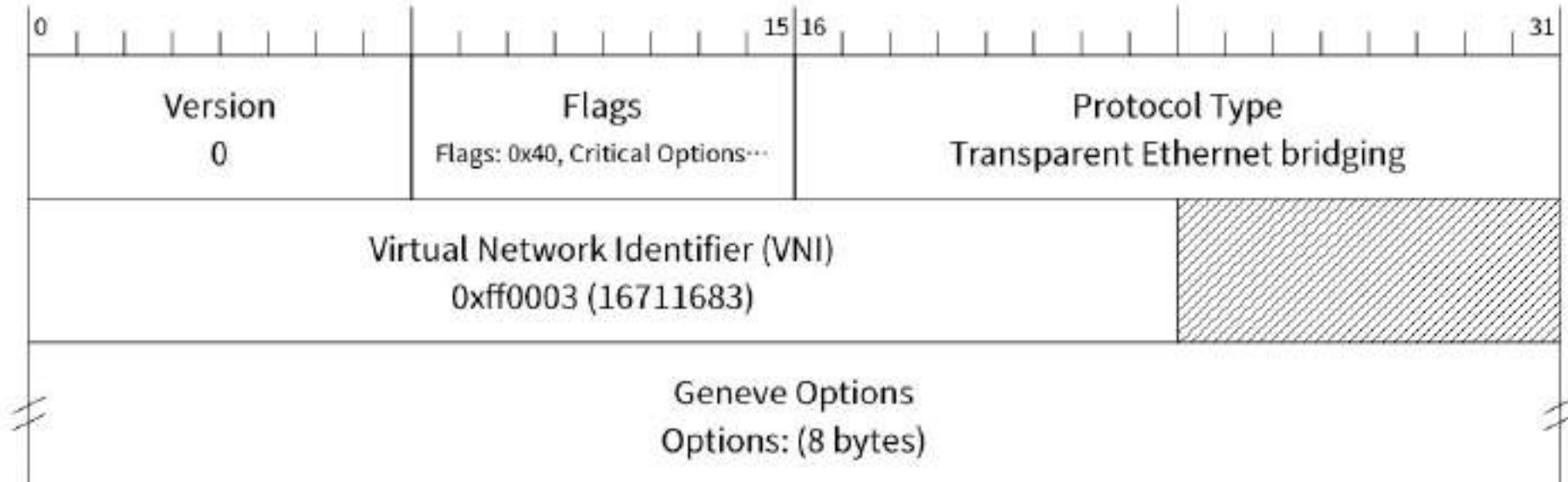
Internet Protocol Version 4

Version 0100 = ...		Header Length ... 0101 = ...	Differentiated Services Field Differentiated Services Field	Total Length 372	
Identification 0x8ae1 (35553)			Flags 010, ...	Fragment Offset ...0 0000 0000 0000 = Fragment Offset: 0	
Time to Live 64		Protocol UDP		Header Checksum Header Checksum: 0xc92b [validation disabled]	
Source Address 192.168.50.13					
Destination Address 192.168.50.14					

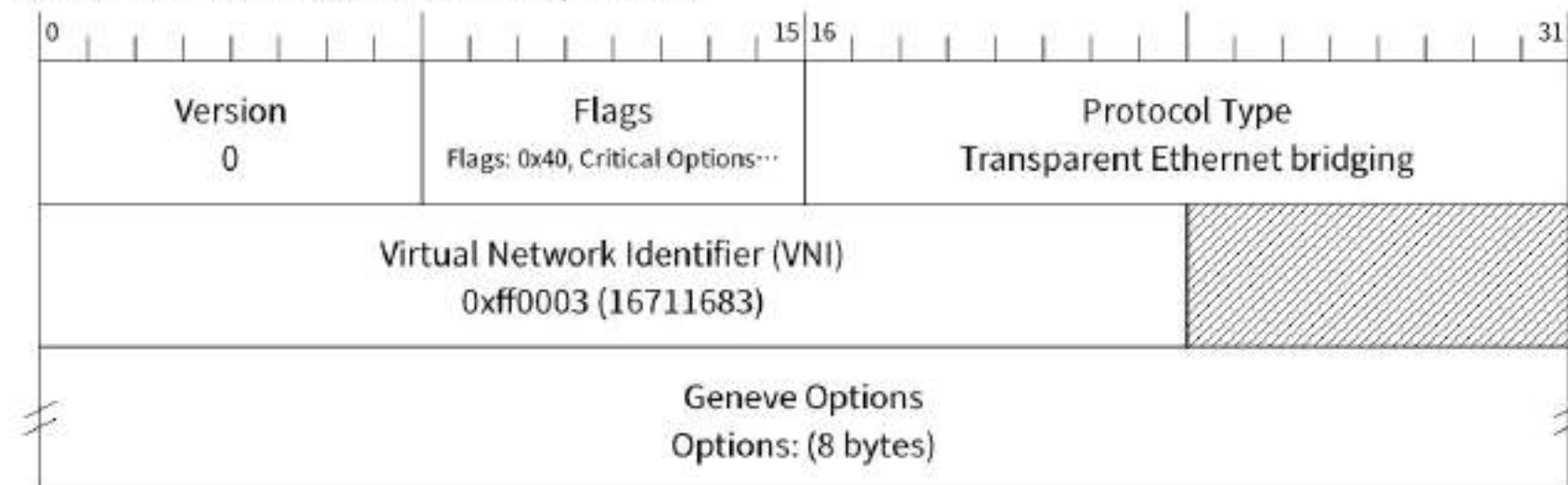
User Datagram Protocol



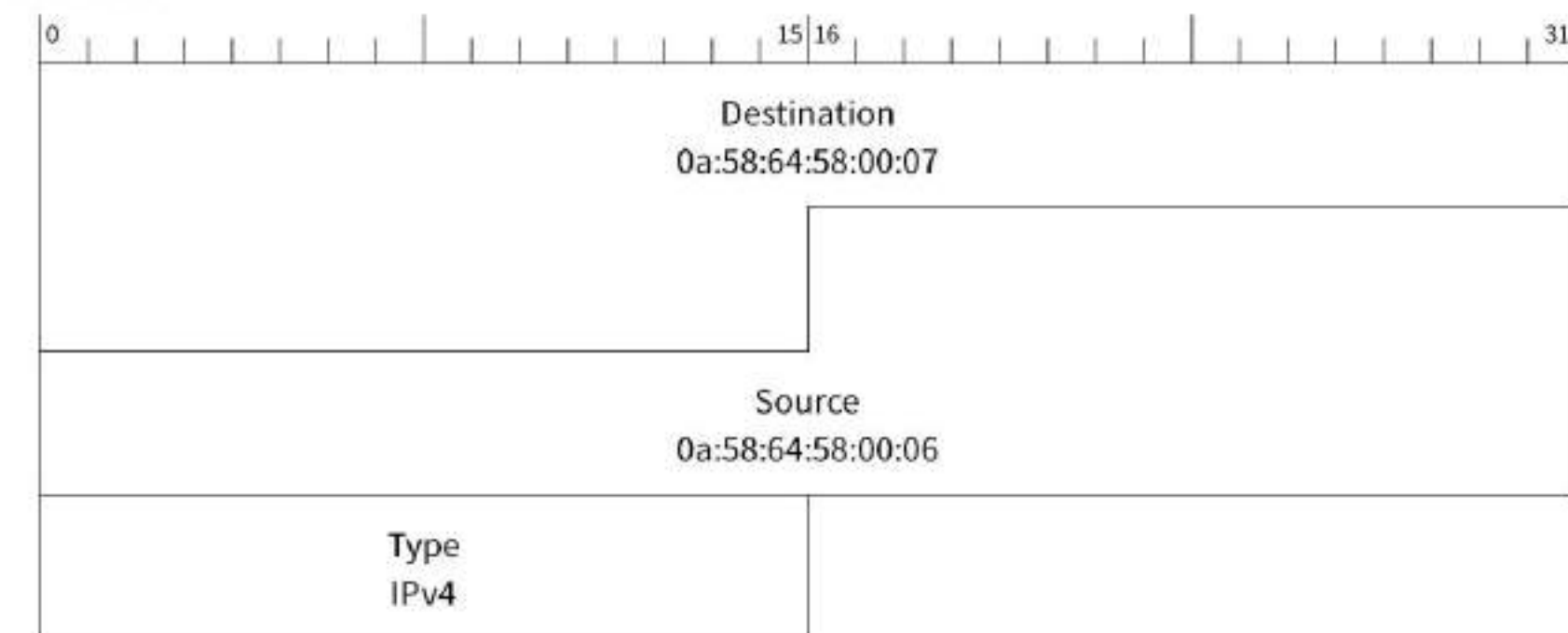
Generic Network Virtualization Encapsulation



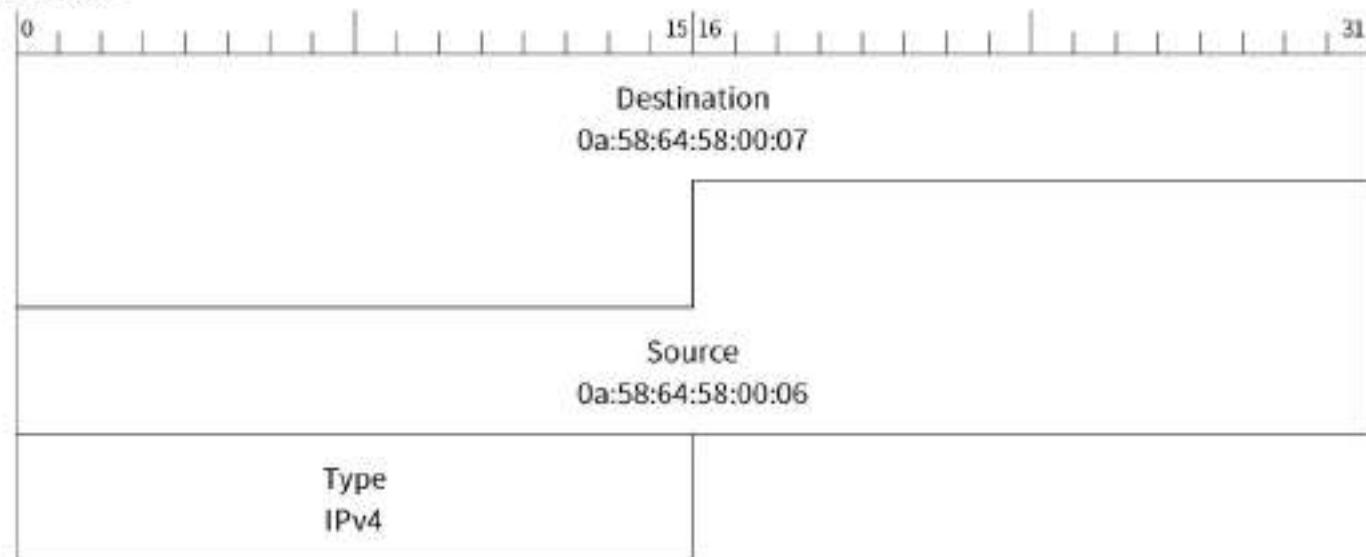
Generic Network Virtualization Encapsulation



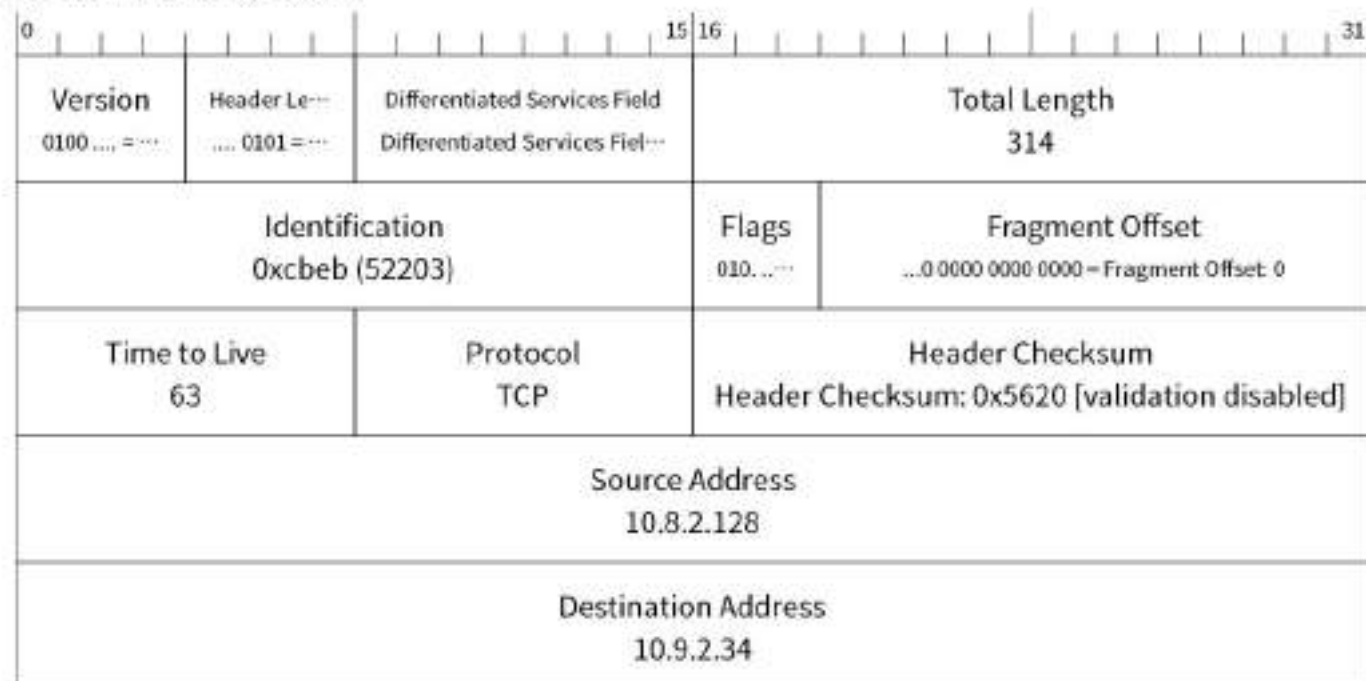
Ethernet



Ethernet

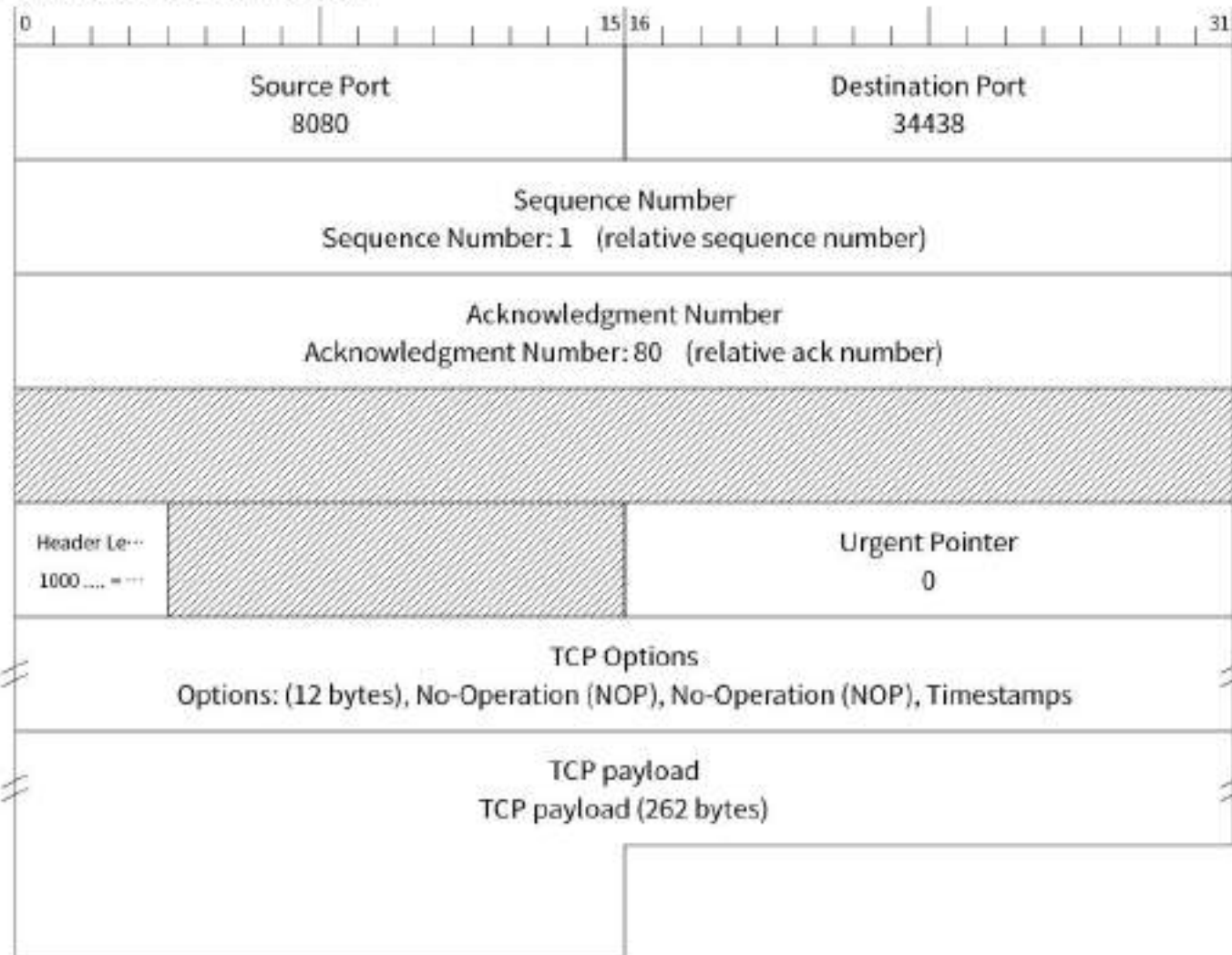


Internet Protocol Version 4

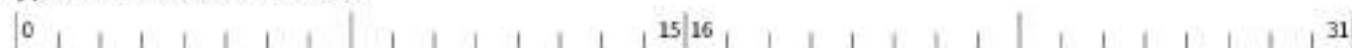


Destination Address
10.9.2.34

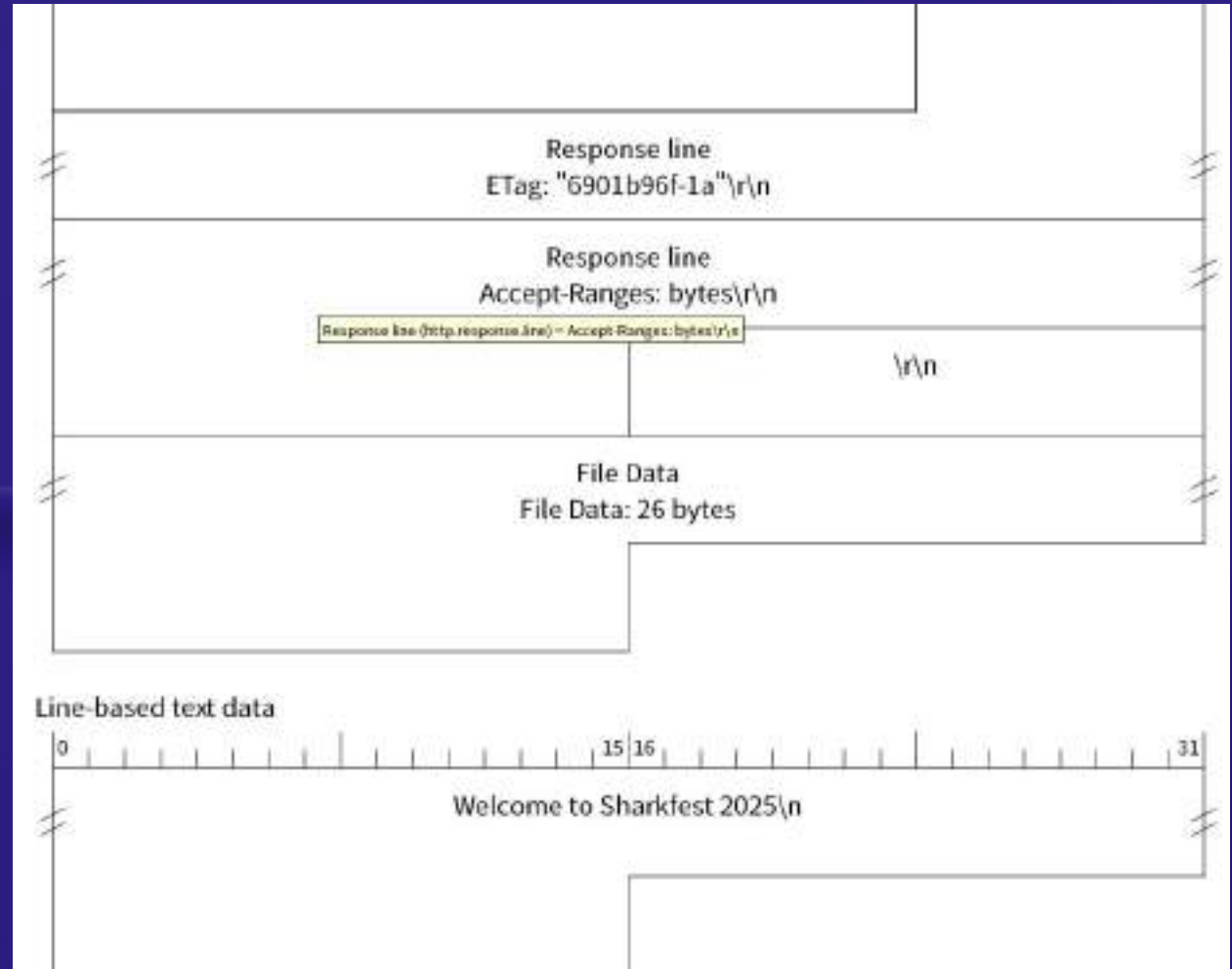
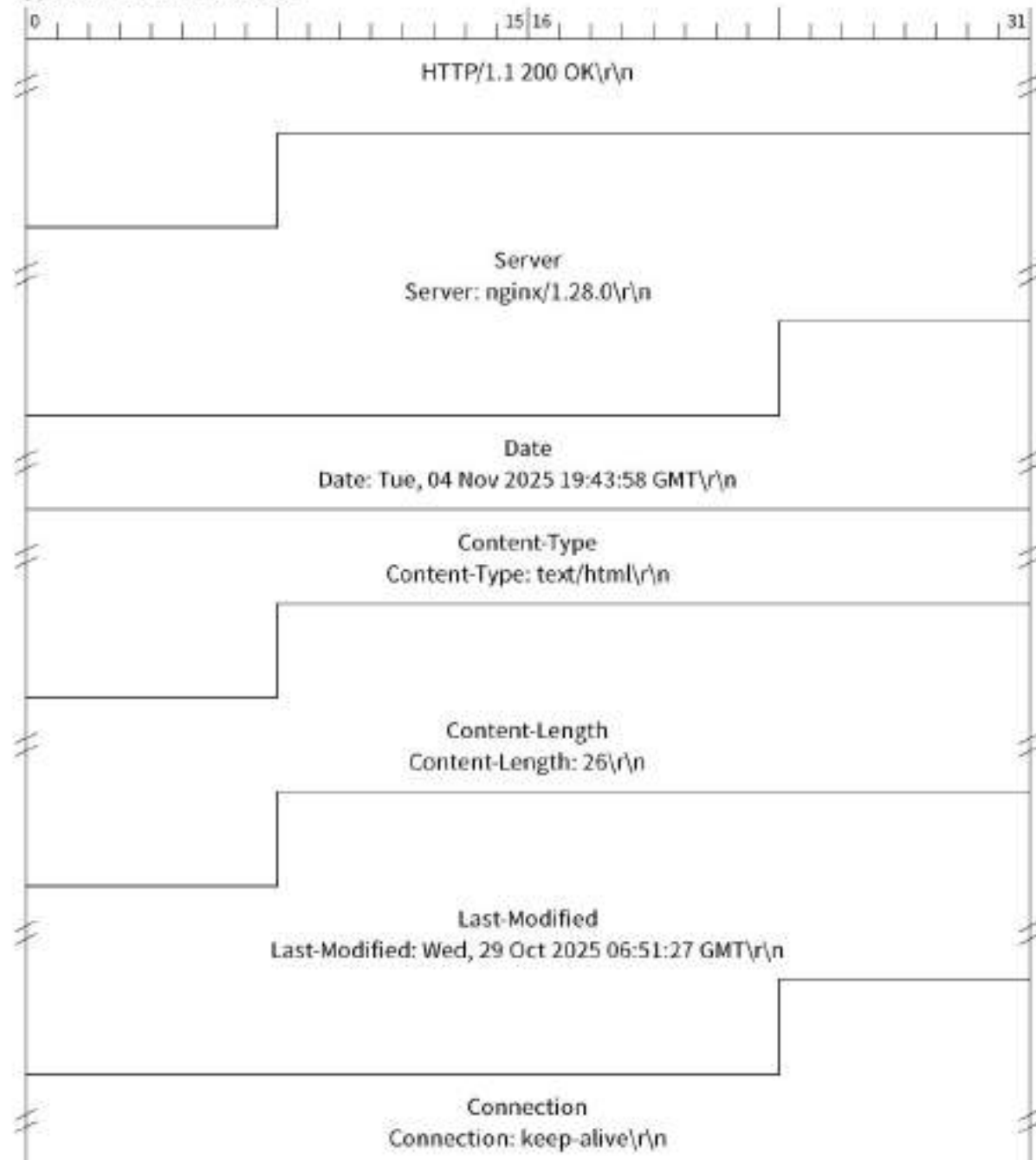
Transmission Control Protocol



Hypertext Transfer Protocol



Hypertext Transfer Protocol



Line-based text data



apiVersion: v1

items:

- apiVersion: config.openshift.io/v1

kind: Network

metadata:

name: cluster

spec:

clusterNetwork:

- cidr: 10.8.0.0/14

hostPrefix: 23

externalIP:

policy: {}

networkType: OVNKubernetes

serviceNetwork:

- 172.30.0.0/16

status:

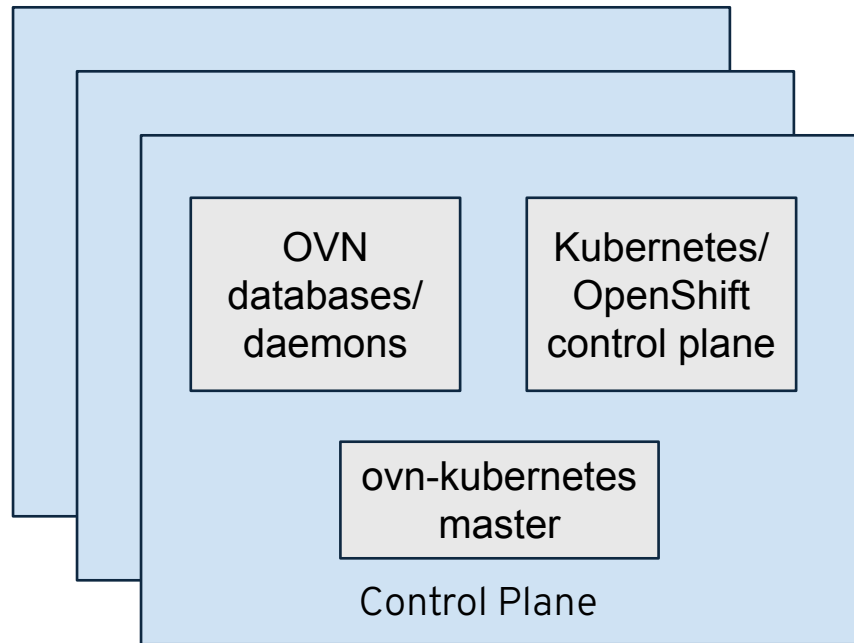
clusterNetwork:

- cidr: 10.8.0.0/14

hostPrefix: 23

clusterNetworkMTU: 1400

OVN Control Plane Architecture

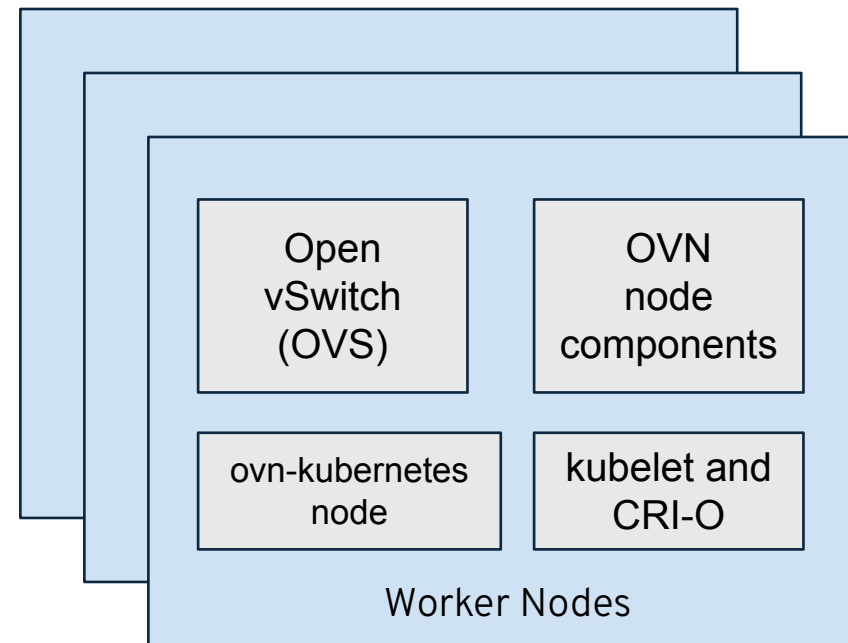


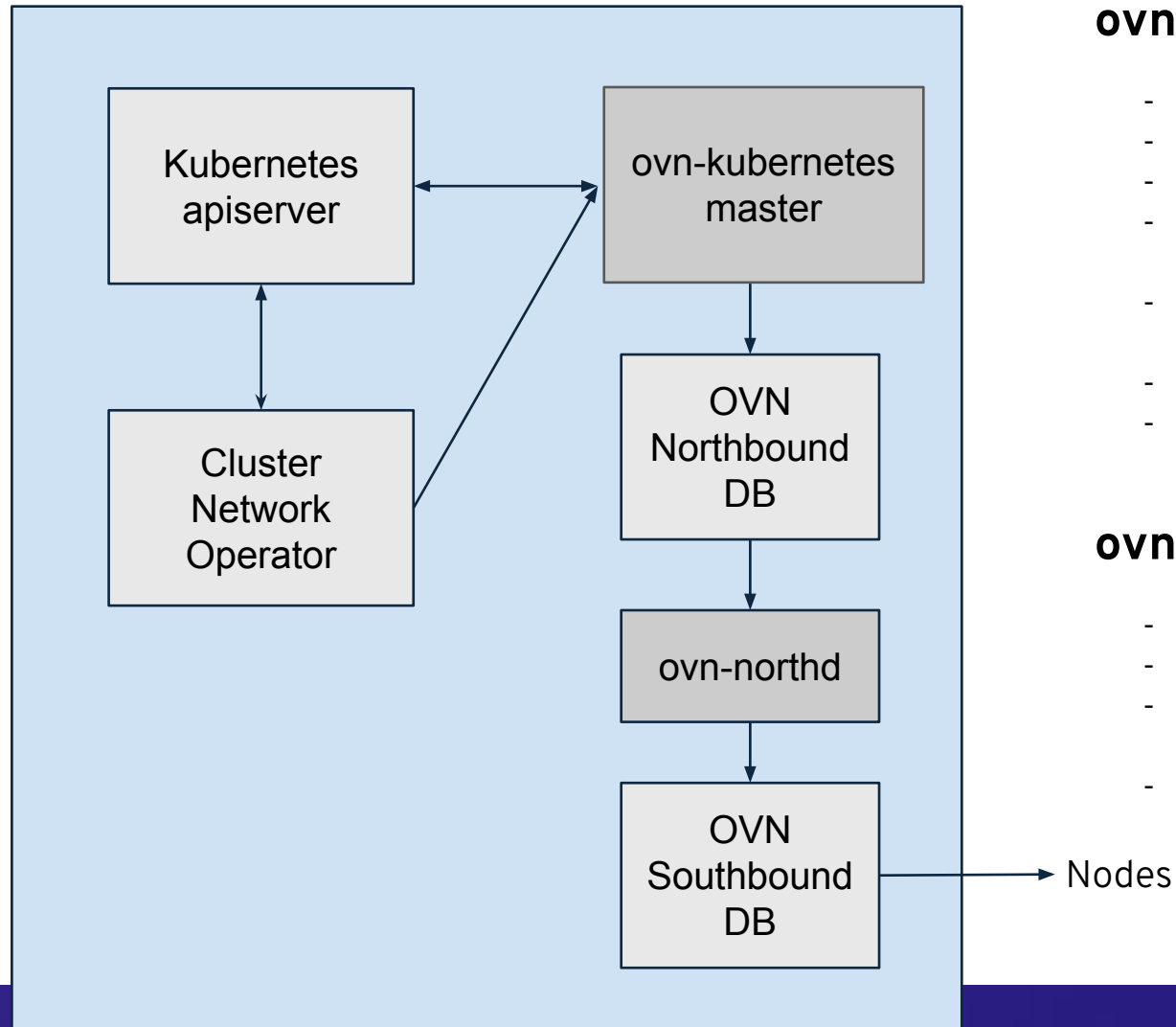
Features:

- Manages overlays and physical network connectivity
- Flexible security policies (ACLs)
- Distributed L3 routing, IPv4 and IPv6, L2/L3 Gateways
- Native support for NAT, load balancing, DHCP and RA
- Works with Linux, DPDK, and Hyper-V

Project:

- OVN = Open Virtual Network
- OVN is a network virtualization platform based on Open vSwitch (OVS)
- Originally part of the OVS project, now a Linux Foundation project





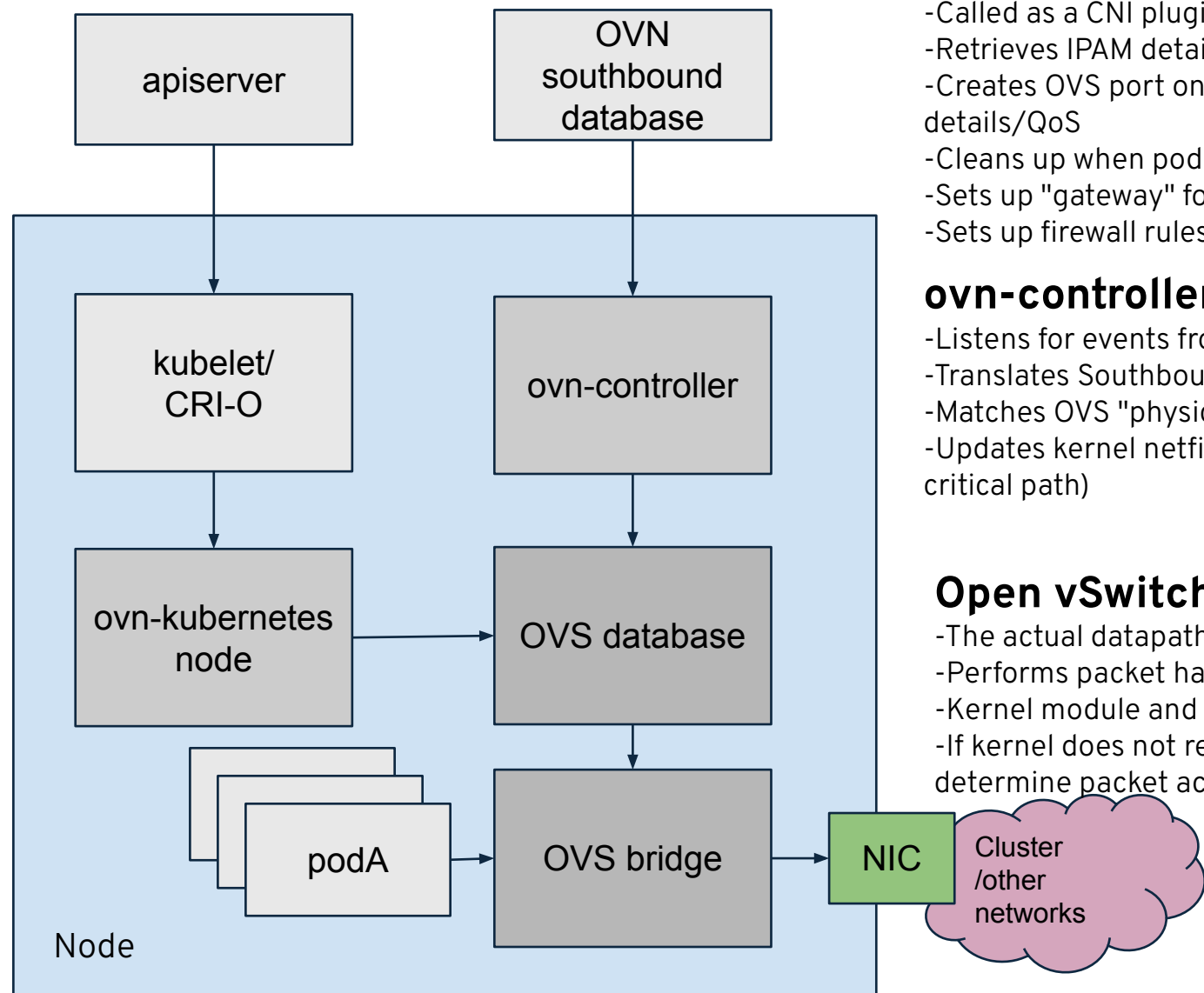
ovn-kubernetes master

- Deployment created by Cluster Network Operator
- Multiple instances elect a leader
- Kubernetes API is the single source of truth
- Listens for cluster events (Pods, Namespaces, Services, Endpoints, NetworkPolicy)
- Translates cluster events to OVN logical network elements (logical switches, ACLs, logical routers, switch ports)
- Handles all required IPAM
- Updates OVN Northbound database based on Kube API state

ovn-northd

- Multiple instances managed by ovn-kubernetes master
- Listens for Northbound DB changes
- Decomposes logical network elements into OVN pipeline and populates the Southbound DB
- Keeps no state itself (eg "cattle")

Worker Node Architecture from OVN standpoint



ovn-kubernetes node

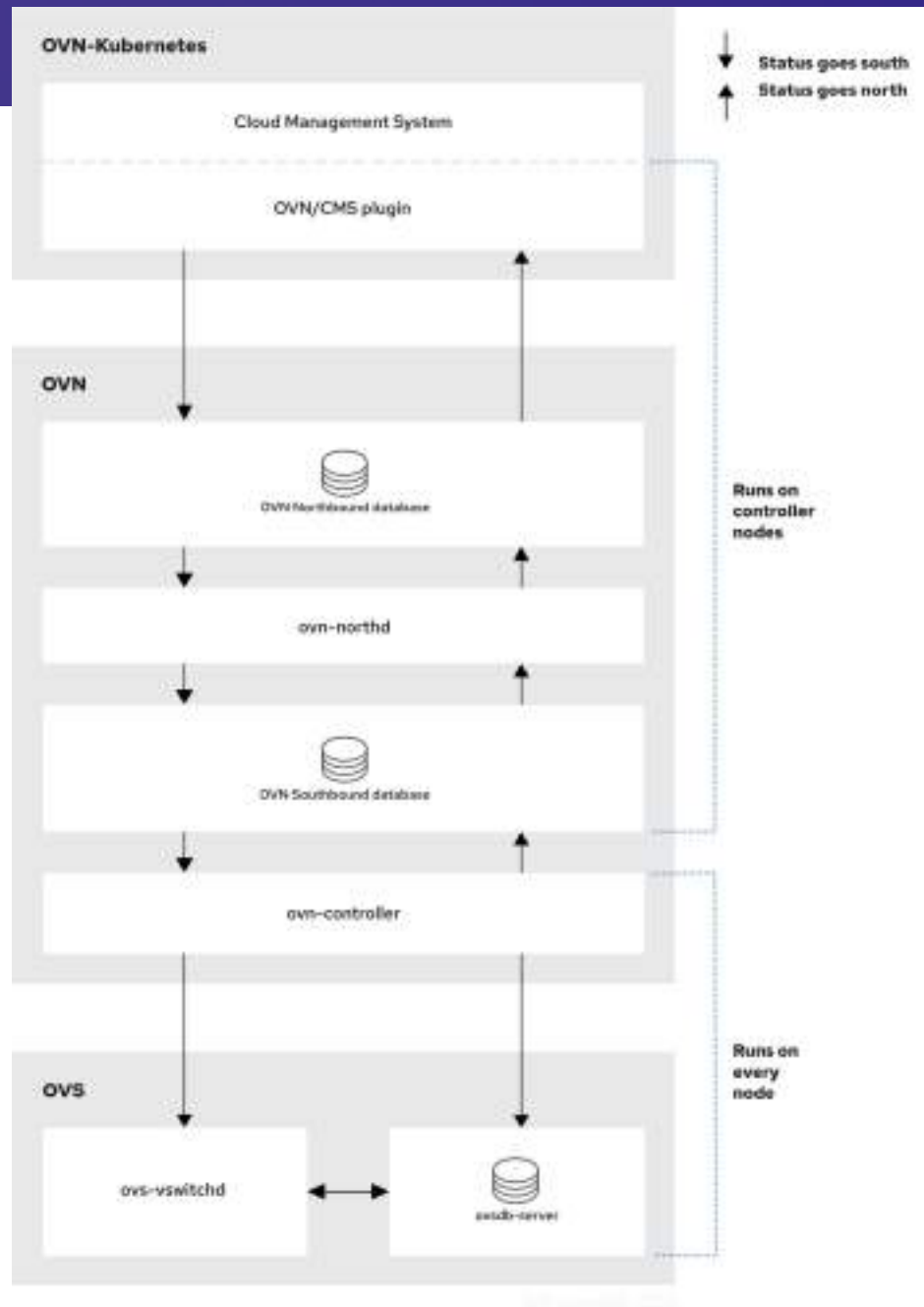
- Called as a CNI plugin from kubelet/CRI-O runtime
- Retrieves IPAM details from Kube API (written by ovn-kubernetes master)
- Creates OVS port on bridge, moves it into pod network namespace, sets IP details/QoS
- Cleans up when pods die
- Sets up "gateway" for cluster-external network access
- Sets up firewall rules and routes for HostPort and Service access from node

ovn-controller

- Listens for events from OVN Southbound database
- Translates Southbound database into OpenFlow and programs local OVS vSwitch
- Matches OVS "physical" ports with OVN logical ports
- Updates kernel netfilter tables for load balancing functionality (no iptables in critical path)

Open vSwitch

- The actual datapath for containers
- Performs packet handling based on OpenFlow rules
- Kernel module and userspace management daemon
- If kernel does not recognize a flow, calls up to management daemon to determine packet action, then caches the match+action for later





```
[student@workstation ~]$ oc project openshift-ovn-kubernetes
Already on project "openshift-ovn-kubernetes" on server "https://api.ocp4.example.com:6443".
```

```
[student@workstation ~]$ oc get deploy,ds
```

NAME	READY	UP-TO-DATE	AVAILABLE	AGE
deployment.apps/ovnkube-control-plane	2/2	2	2	351d

NAME	DESIRED	CURRENT	READY	UP-TO-DATE	AVAILABLE	NODE SELECTOR	AGE
daemonset.apps/ovnkube-node	6	6	6	6	6	kubernetes.io/os=linux	351d

```
[student@workstation ~]$ oc get po -o wide
```

NAME	READY	STATUS	RESTARTS	AGE	IP	NODE	NOMINATED	NODE	READINESS	GATES
ovnkube-control-plane-7dbbfddddf-l5tmp	2/2	Running	2	21h	192.168.50.12	master03	<none>		<none>	
ovnkube-control-plane-7dbbfddddf-q95mv	2/2	Running	2	21h	192.168.50.11	master02	<none>		<none>	
ovnkube-node-4f74r	8/8	Running	17 (11h ago)	21h	192.168.50.10	master01	<none>		<none>	
ovnkube-node-8h2ml	8/8	Running	16	21h	192.168.50.15	worker03	<none>		<none>	
ovnkube-node-bfvnh	8/8	Running	17	21h	192.168.50.12	master03	<none>		<none>	
ovnkube-node-g75s5	8/8	Running	16	21h	192.168.50.13	worker01	<none>		<none>	
ovnkube-node-q8z5c	8/8	Running	17	21h	192.168.50.14	worker02	<none>		<none>	
ovnkube-node-vzzt8	8/8	Running	16	21h	192.168.50.11	master02	<none>		<none>	

```
[student@workstation ~]$ oc get pods ovnkube-control-plane-7dbbfddddf-l5tmp -o jsonpath='{.spec.containers[*].name}' -n openshift-ovn-kubernetes
kube-rbac-proxy ovnkube-cluster-manager
```

```
[student@workstation ~]$ oc get pods ovnkube-node-4f74r -o jsonpath='{.spec.containers[*].name}' -n openshift-ovn-kubernetes;echo
ovn-controller ovn-acl-logging kube-rbac-proxy-node kube-rbac-proxy-ovn-metrics northd nbdb sbdb ovnkube-controller
```

```
[student@workstation ~]$ oc exec ovnkube-node-4f74r -c nbdb -- ovn-nbctl ls-list
```

```
a5c8d790-401c-4a7b-aced-18d77cf10c13 (ext_master01)
```

```
12b49a4c-5fc6-4434-97df-ea42250c9295 (join)
```

```
339cb013-7055-4838-a940-f9f0981321d0 (master01)
```

```
4b55828c-9cef-44d4-be95-8ca3c4dd9042 (transit_switch)
```

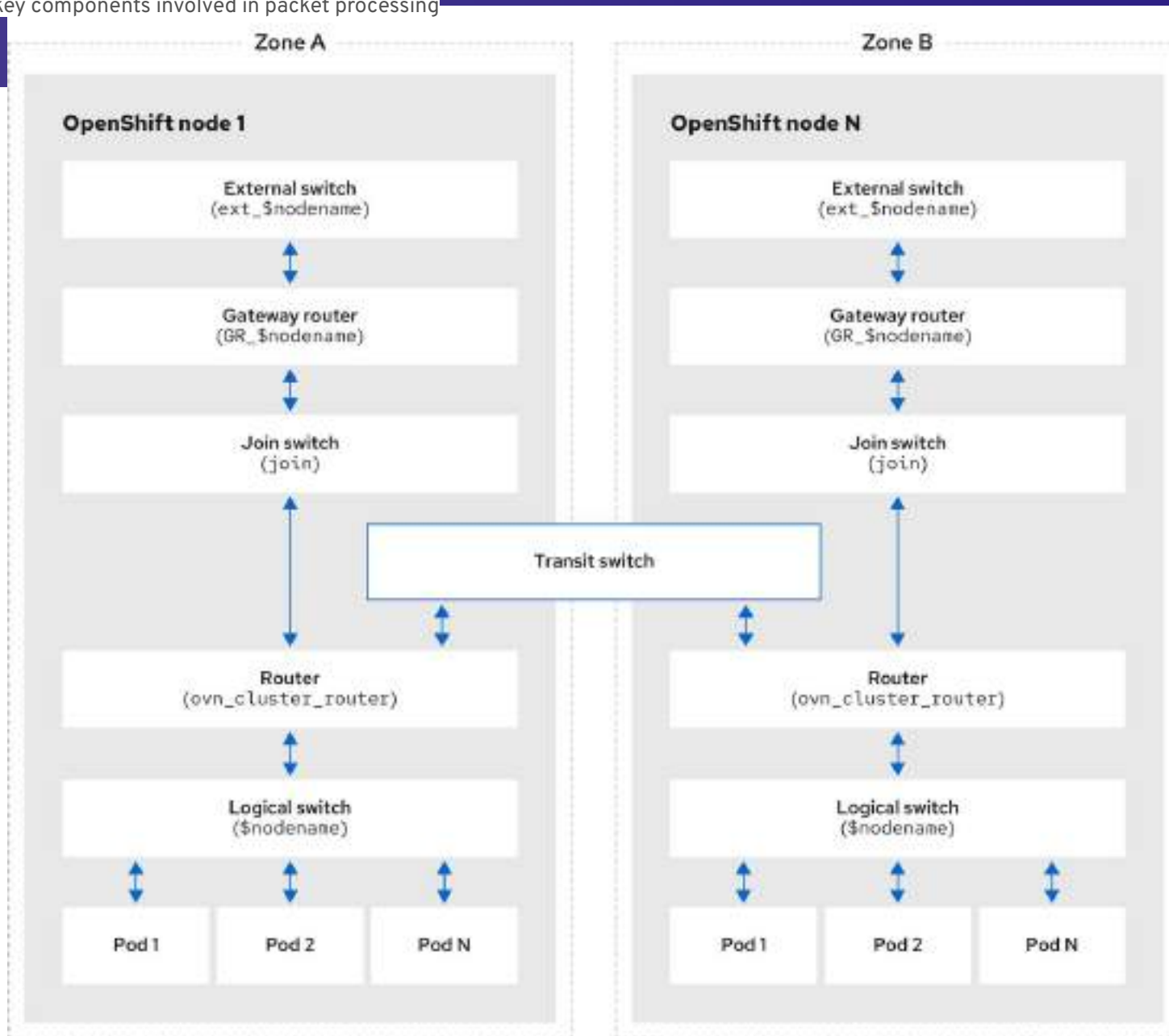
```
[student@workstation ~]$ oc exec ovnkube-node-4f74r -c nbdb -- ovn-nbctl lr-list
```

```
53750661-d7ca-46c3-bce5-019c50b51ce3 (GR_master01)
```

```
8d10fdac-3ab4-4848-b346-8927009f95bf (ovn_cluster_router)
```

```
[student@workstation ~]$ oc exec ovnkube-node-4f74r -c nbdb -- ovn-nbctl lb-list
```

UUID	LB	PROTO	VIP	IPs
8d3b3f30-c9f2-4587-b015-1d41d43f9c9b	Service_cert-man	tcp	172.30.244.210:8443	
fafde66f-5608-4cf0-baa6-f4db03360f0b	Service_cert-man	tcp	172.30.6.99:9402	10.11.0.10:9402
eac82885-7512-4228-a84f-b8e2034a67c5	Service_cert-man	tcp	172.30.137.71:9402	10.11.0.11:9402



Gateway routers aka L3 gateway routers, are typically used between the distributed routers and the physical network. Gateway routers including their logical patch ports are bound to a physical location (not distributed), or chassis. The patch ports on this router are known as I3gateway ports in the ovn-sbdb database (ovn-sbdb).

Distributed logical routers and the logical switches behind them, to which virtual machines and containers attach, effectively reside on each hypervisor.

Join local switches are used to connect the distributed router and gateway routers. It reduces the number of IP addresses needed on the distributed router.

Logical switches with patch ports - Logical switches with patch ports are used to virtualize the network stack. They connect remote logical ports through tunnels. Logical switches with localnet ports are used to connect OVN to the physical network. They connect remote logical ports by bridging the packets to directly connected physical L2 segments using localnet ports.

Patch ports represent connectivity between logical switches and logical routers and between peer logical routers. A single connection has a pair of patch ports at each such point of connectivity, one on each side.

I3gateway ports are the port binding entries in the ovn-sbdb for logical patch ports used in the gateway routers. They are called I3gateway ports rather than patch ports just to portray the fact that these ports are bound to a chassis just like the gateway router itself.

localnet ports are present on the bridged logical switches that allows a connection to a locally accessible network from each ovn-controller instance. This helps model the direct connectivity to the physical network from the logical switches. A logical switch can only have a single localnet port attached to it.


```
[student@workstation ~]$ oc exec ovnkube-node-4f74r -c nbdb -- ovn-sbctl show
```

```
Chassis "ab4f5fbf-e637-4405-8bd5-439edde69d63"
```

```
hostname: master02
```

```
Encap geneve
```

```
ip: "192.168.50.11"
```

```
options: {csum="true"}
```

```
Port_Binding tstor-master02
```

```
Chassis "236527af-9c52-45da-8692-4410f6524f05"
```

```
hostname: worker03
```

```
Encap geneve
```

```
ip: "192.168.50.15"
```

```
options: {csum="true"}
```

```
Port_Binding tstor-worker03
```

```
Chassis "d7180dac-1d2f-4e70-8cba-4214d6208ed7"
```

```
hostname: worker02
```

```
Encap geneve
```

```
ip: "192.168.50.14"
```

```
options: {csum="true"}
```

```
Port_Binding tstor-worker02
```

```
Chassis "461c83c9-6f60-4369-bf9e-b5b1aefcb6cf"
```

```
hostname: master03
```

```
Encap geneve
```

```
ip: "192.168.50.12"
```

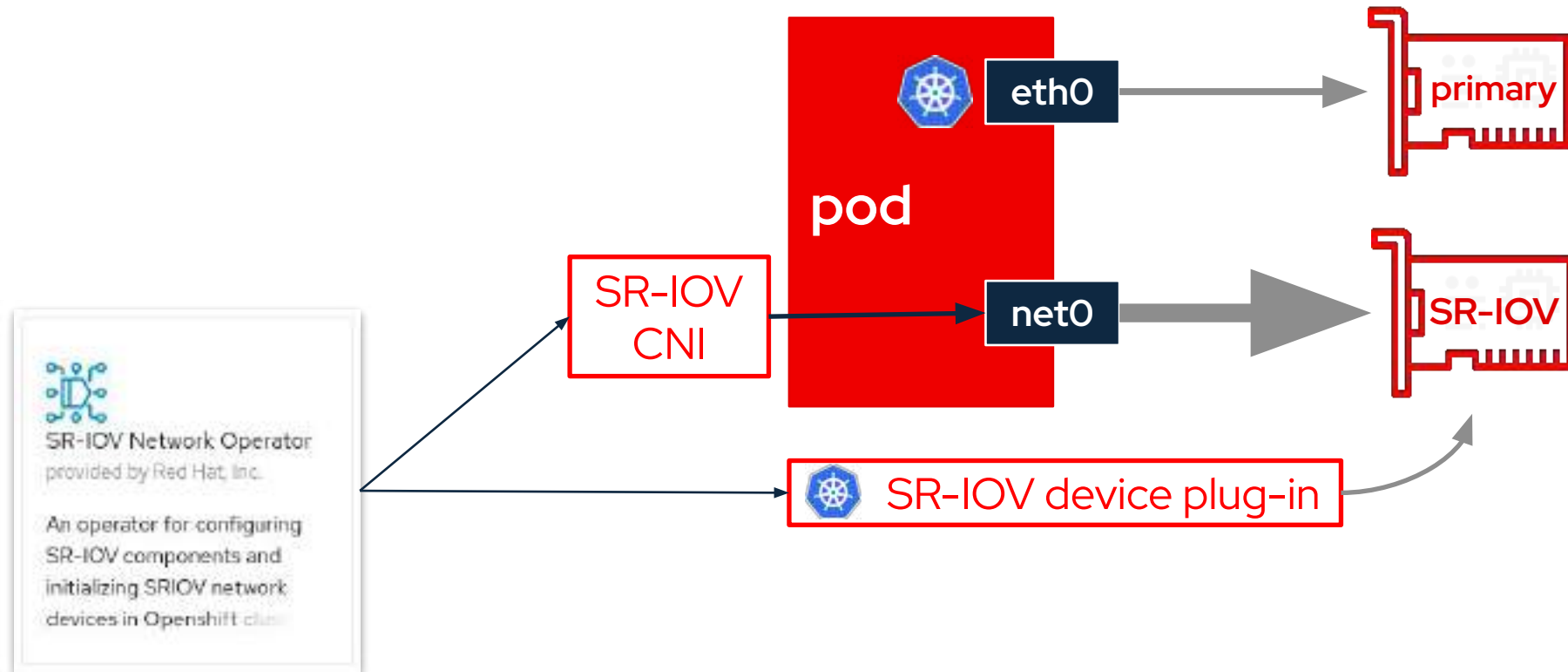
```
options: {csum="true"}
```

```
Port_Binding tstor-master03
```

```
Chassis "48edacea-db4b-46df-9890-86720c3c8404"
```

```
hostname: worker01
```

```
Encap geneve
```



- Home >
- Favorites >
- Operators >
- Helm >
- Workloads >
- Networking >
- Storage >
- Builds >
- Observe >
- Compute >
- User Management >
- Administration >

Project: openshift-netobserv-ope

OperatorHub

Discover Operators from the Kubernetes ecosystem that can install Operators on your clusters to help you manage your infrastructure. See the [Software Catalog](#), providing a self-service interface to install Operators.

All Items

- AI/Machine Learning
- Application Runtime
- Big Data
- Cloud Provider
- Database
- Developer Tools
- Drivers and plugins
- Integration & Delivery
- Logging & Tracing
- Modernization & Migration
- Monitoring
- Networking
- Observability
- OpenShift Optional
- Openshift Optional
- Other
- Security



Network Observability

1.9.3 provided by Red Hat

Uninstall

Channel

stable ▾

Version

1.9.3 ▾

Capability level

- ☒ Basic Install
- ☒ Seamless Upgrades
- ☐ Full Lifecycle
- ☐ Deep Insights
- ☐ Auto Pilot

Source

Red Hat

Provider

Red Hat

Infrastructure features

Designed for FIPS
Disconnected

Installed Operator

This Operator has been installed on the cluster. [View it here.](#)

Network Observability is an OpenShift operator that deploys a monitoring pipeline consisting in:

- an eBPF agent, that generates network flows from captured packets
- flowlogs-pipeline, a component that collects, enriches and exports these flows
- a Console plugin for flows visualization with powerful filtering options, a topology representation and more

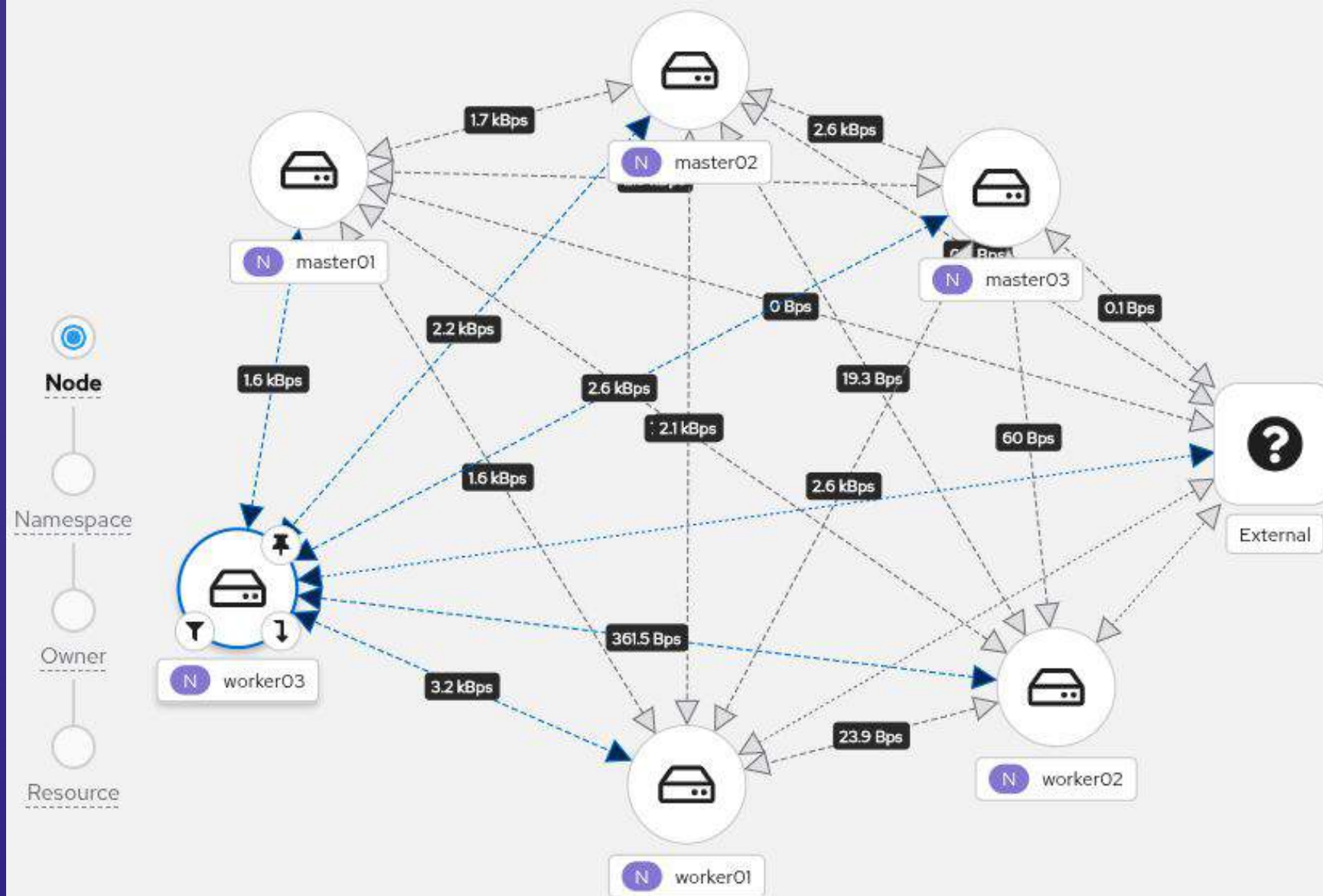
Flow data is then available in multiple ways, each optional:

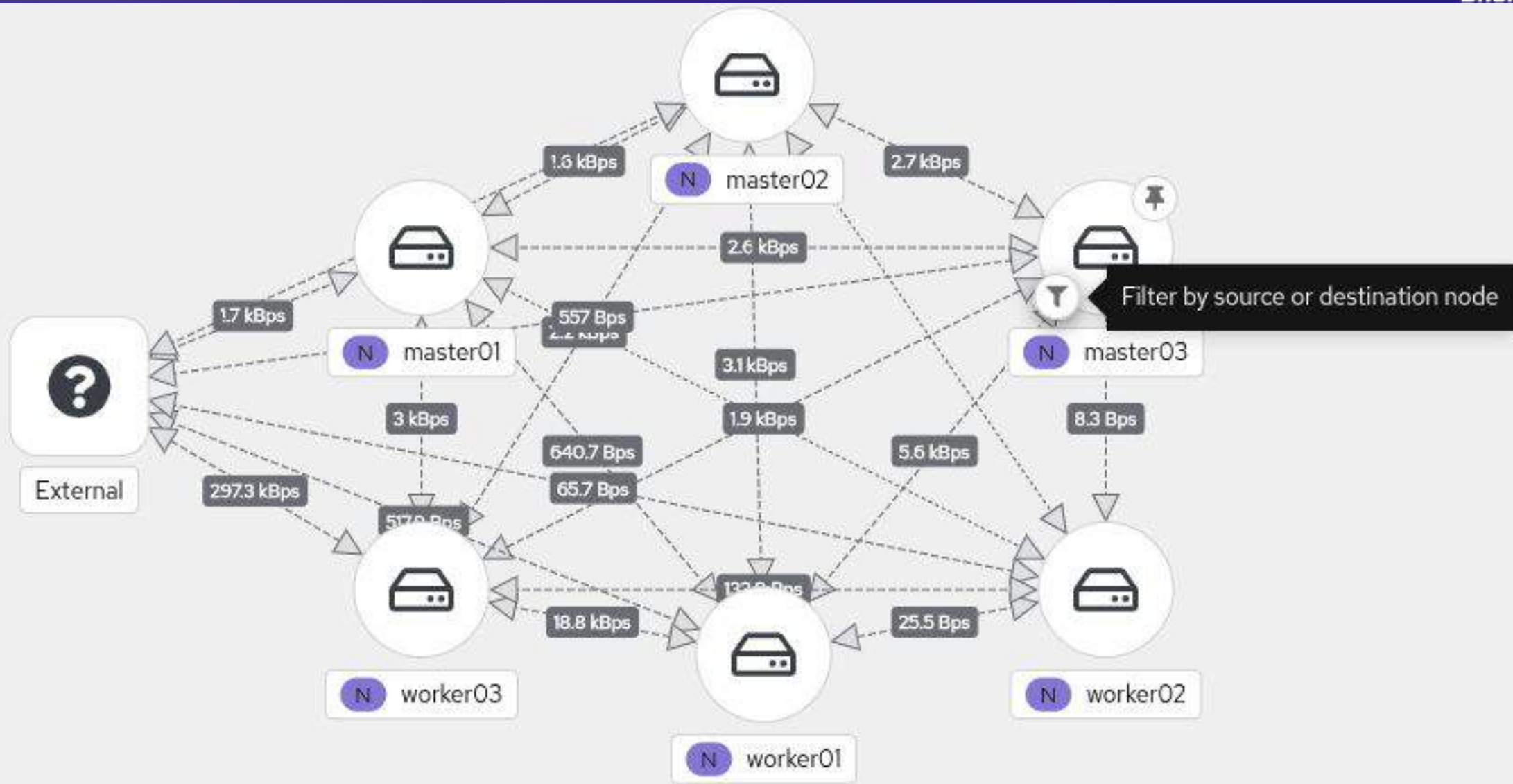
- As Cluster Monitoring metrics
- As raw flow logs stored in Grafana Loki
- As raw flow logs exported to a collector

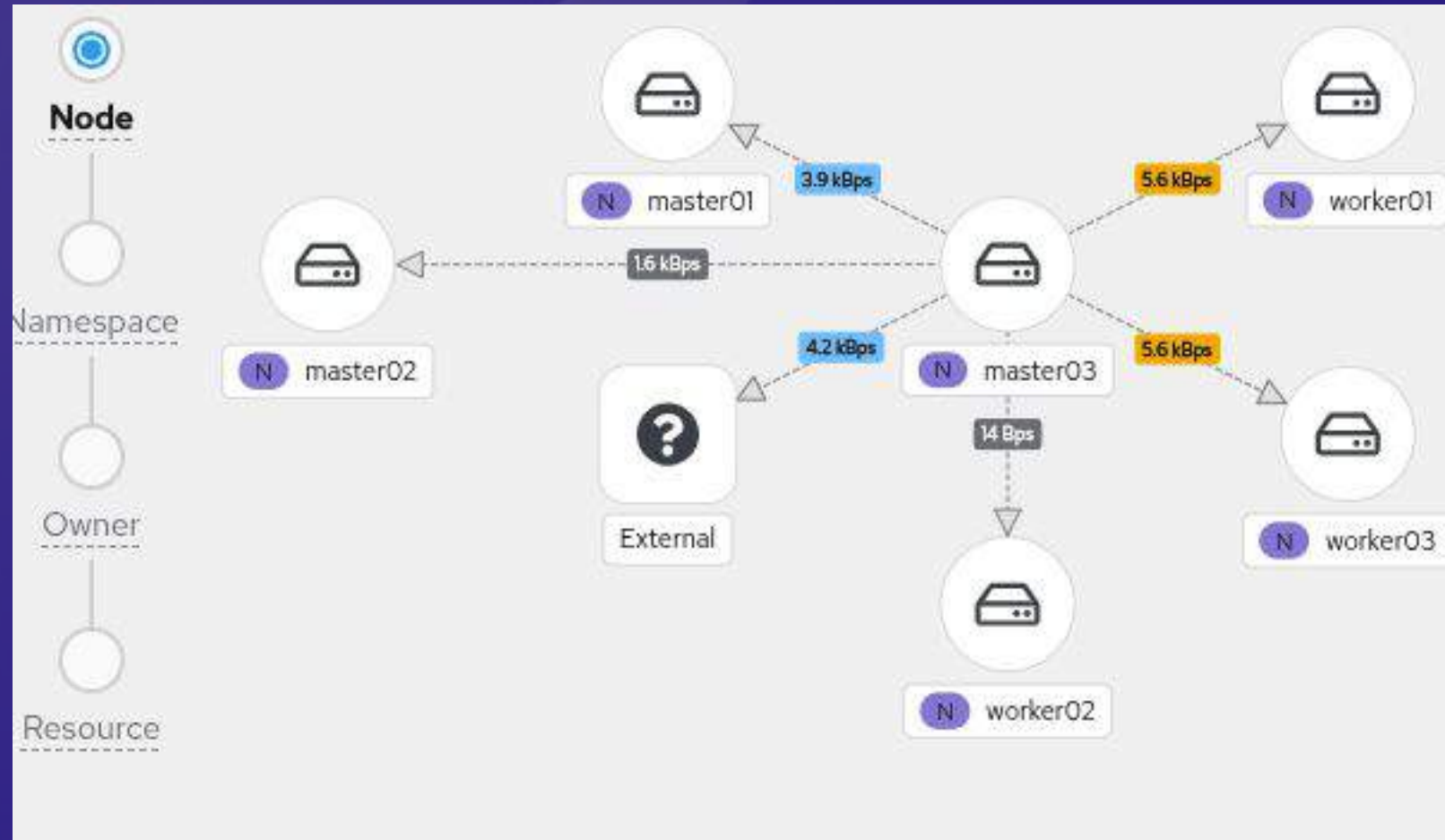
Dependencies

Loki

[Loki](#), from GrafanaLabs, can optionally be used as the backend to store all collected flows. The Network Observability operator does not install Loki directly, however we provide some guidance to help you there.







Network Traffic

Time range: Last 5 minutes Refresh interval: 5 minutes

Query options: Quick filters: Source Namespace: E.g. namespace Specify a single Kubernetes name Learn more

Expand Source Node Name: worker01 Destination Node Name: worker02 Reset defaults Clear all Swap One way Overview Traffic flows Topology Show Notogram Hide advanced options

Display options: Manage columns Export data

Source			Destination			L3 Layer
Name	Namespace	Port	Name	Namespace	Port	Protocol
worker01	n/a	5100 (655)	worker02	n/a	6081	UDP
worker01	n/a	3362	worker02	n/a	6081	UDP
worker01	n/a	7580	worker02	n/a	6081	UDP
worker01	n/a	9122	worker02	n/a	9122	UDP
worker01	n/a	9122	worker02	n/a	9122	UDP
worker01	n/a	9122	worker02	n/a	9122	UDP
worker01	n/a	9122	worker02	n/a	9122	UDP
worker01	n/a	9122	worker02	n/a	9122	UDP
worker01	n/a	9122	worker02	n/a	9122	UDP
worker01	n/a	16407	worker02	n/a	6081	UDP
worker01	n/a	16407	worker02	n/a	6081	UDP
worker01	n/a	17486	worker02	n/a	6081	UDP
worker01	n/a	20266	worker02	n/a	6081	UDP
worker01	n/a	25823	worker02	n/a	6081	UDP
worker01	n/a	28830	worker02	n/a	6081	UDP
worker01	n/a	28888	worker02	n/a	6081	UDP
worker01	n/a	28888	worker02	n/a	6081	UDP

Source		Destination		L3 Layer							
Owner Kubernetes Object	IP & Port	Owner Kubernetes Object	IP & Port	Protocol	Interfaces and Directions ⓘ ⓘ					Bytes ⓘ	Duration
 worker01	192.168.50.13:35348	 worker02	192.168.50.14:9105	TCP	ens3	Egress	ens3	Ingress	1 more...	66	n/a
 worker01	192.168.50.13:1362	 worker02	192.168.50.14:6081	UDP	ens3	Egress	ens3	Ingress		124	n/a
 worker01	192.168.50.13:9122	 worker02	192.168.50.14:9122	UDP	ens3	Egress	br-ex	Egress	2 more...	91	n/a
 worker01	192.168.50.13:54419	 worker02	192.168.50.14:9140	TCP	ens3	Egress	br-ex	Ingress	1 more...	66	n/a
 worker01	192.168.50.13:39958	 worker02	192.168.50.14:10250	TCP	ens3	Egress	br-ex	Ingress	1 more...	360	95ms
 worker01	192.168.50.13:40791	 worker02	192.168.50.14:9103	TCP	br-ex	Ingress	ens3	Egress	1 more...	66	n/a
 worker01	192.168.50.13:15078	 worker02	192.168.50.14:6081	UDP	br-ex		Egress			124	n/a
 worker01	192.168.50.13:16407	 worker02	192.168.50.14:6081	UDP	br-ex		Egress			164	n/a
 worker01	192.168.50.13:55376	 worker02	192.168.50.14:9637	TCP	ens3	Egress	br-ex	Ingress	1 more...	66	n/a
 worker01	192.168.50.13:1362	 worker02	192.168.50.14:6081	UDP	ens3	Egress	ens3	Ingress		486	n/a
 worker01	192.168.50.13:39958	 worker02	192.168.50.14:10250	TCP	ens3	Egress	br-ex	Ingress	1 more...	531	216ms
 prometheus-k8s  openshift-monitoring	10.8.2.18:46322	 worker02	192.168.50.14:9100	TCP	b2d420c70592d6c		Ingress			66	n/a
 prometheus-k8s  openshift-monitoring	10.8.2.18:56108	 worker02	192.168.50.14:10250	TCP	b2d420c70592d6c		Ingress			864	39ms
 prometheus-k8s  openshift-monitoring	10.8.2.18:52700	 worker02	192.168.50.14:9637	TCP	b2d420c70592d6c		Ingress			66	n/a
 prometheus-k8s  openshift-monitoring	10.8.2.18:56108	 worker02	192.168.50.14:10250	TCP	b2d420c70592d6c		Ingress			588	80ms
Summary ⓘ 15:16:51 ⓘ 125 Flows ⓘ 23 kB ⓘ 192 Packets ⓘ 77.25 Bps ⓘ See more											

Source		Destination		L3 Layer					Bytes	Duration
Owner Kubernetes Object	IP & Port	Owner Kubernetes Object	IP & Port	Protocol	Interfaces and Directions					
 worker01	192.168.50.13:35348	 worker02	192.168.50.14:9105	TCP	ens3	Ingress	br-ex	Ingress	66	n/a
 worker01	192.168.50.13:58078	 worker02	192.168.50.14:6081	UDP	br-ex	Ingress	ens3	Ingress	164	n/a
 worker01	192.168.50.13:7976	 worker02	192.168.50.14:6081	UDP	ens3		Ingress		124	n/a
 prometheus-k8s	10.8.2.18:36486	 loki-operator-controller...	10.9.2.44:8443	TCP	genev_sys_6081	Egress	b2d420c70592...Ingress	2 more...	66	n/a
 openshift-monitoring		 openshift-operators-redh...								
 prometheus-k8s	10.8.2.18:36486	 loki-operator-controller...	10.9.2.44:8443	TCP	genev_sys_6081	Egress	b2d420c70592...Ingress	2 more...	66	n/a
 openshift-monitoring		 openshift-operators-redh...								
 prometheus-k8s	10.8.2.18:36486	 loki-operator-controller...	10.9.2.44:8443	TCP	genev_sys_6081	Egress	b2d420c70592...Ingress	2 more...	66	n/a
 openshift-monitoring		 openshift-operators-redh...								
 network-check-source	10.8.2.4:55370	 network-check-target	10.9.2.32:8080	TCP	genev_sys_6081		Egress		66	n/a
 openshift-network-dia...		 openshift-network-diagn...								
 network-check-source	10.8.2.4:48162	 network-check-target	10.9.2.32:8080	TCP	0786f92081dbe44		Egress		74	n/a
 openshift-network-dia...		 openshift-network-diagn...								
 prometheus-k8s	10.8.2.18:33986	 network-metrics-dae...	10.9.2.30:8443	TCP	b2d420c70592...Ingress		genev_sys_6081	Egress	1 more...	106
 openshift-monitoring		 openshift-multus								
 prometheus-k8s	10.8.2.18:33986	 network-metrics-dae...	10.9.2.30:8443	TCP	b2d420c70592...Ingress		genev_sys_6081	Egress	1 more...	66
 openshift-monitoring		 openshift-multus								
 prometheus-k8s	10.8.2.18:33986	 network-metrics-dae...	10.9.2.30:8443	TCP	b2d420c70592...Ingress		genev_sys_6081	Egress	1 more...	101
 openshift-monitoring		 openshift-multus								
 worker01	10.8.2.2:59908	 ingress-canary	10.9.2.6:8443	TCP	genev_sys_6081		Egress		74	n/a
		 openshift-ingress-canary								

Source Node Name: worker03 ✕ ⓘ
Destination Node Name: worker01 ✕ ⓘ

Overview
Traffic flows
Topology
Show Histogram

Display options ▼

Source			Destination			L3 Layer
Name	Namespace	Port	Name	Namespace	Port	Protocol
worker03	n/a	1580	worker01	n/a	6081	UDP
worker03	n/a	2940	worker01	n/a	6081	UDP
worker03	n/a	2940	worker01	n/a	6081	UDP
worker03	n/a	2940	worker01	n/a	6081	UDP
icki	netobserv	3100	flowlogs-pipeline-6r75d	netobserv	51958	TCP
worker03	n/a	8874	worker01	n/a	6081	UDP
thanos-ruler-user-work...	openshift-user-worklo...	9091	worker01	n/a	47640	TCP
thanos-querier-6d8bb...	openshift-monitoring	9091	worker01	n/a	45152	TCP
prometheus-k8s-0	openshift-monitoring	9091	worker01	n/a	33702	TCP
worker03	n/a	9103	prometheus-k8s-1	openshift-monitoring	59490	TCP
worker03	n/a	9120	worker01	n/a	59954	TCP
worker03	n/a	9122	worker01	n/a	51004	TCP
dns-default-fjhx2	openshift-dns	9154	prometheus-k8s-1	openshift-monitoring	50586	TCP

Source			Destination			L3 Layer
Name	Namespace	Port	Name	Namespace	Port	Protocol
Nworker03	n/a	10250	Nworker01	n/a	35426	TCP
Nworker03	n/a	10250	Pprometheus-k8s-1	NSopenshift-monitoring	47078	TCP
Nworker03	n/a	18882	Nworker01	n/a	6081	UDP
Nworker03	n/a	19083	Nworker01	n/a	6081	UDP
Nworker03	n/a	20788	Nworker01	n/a	6081	UDP
Nworker03	n/a	21871	Nworker01	n/a	6081	UDP
Nworker03	n/a	26150	Nworker01	n/a	6081	UDP
Nworker03	n/a	28963	Nworker01	n/a	6081	UDP
Nworker03	n/a	32260	Nworker01	n/a	6081	UDP
Nworker03	n/a	33020	Nworker01	n/a	10250	TCP
Nworker03	n/a	33089	Nworker01	n/a	10250	TCP
Nworker03	n/a	34427	Nworker01	n/a	6081	UDP
Nworker03	n/a	34887	Nworker01	n/a	6081	UDP

Source Node Name: worker03 X ⓘ Destination Node Name: worker01 X ⓘ

Overview Traffic flows Topology Show histogram

Display options ▼

Source			Destination			L3 Layer
Name ⓘ	Namespace ⓘ	Port ⓘ	Name ⓘ	Namespace ⓘ	Port ⓘ	Protocol
worker03	n/a	37572	worker01	n/a	6081	UDP
worker03	n/a	38333	worker01	n/a	6081	UDP
worker03	n/a	40182	worker01	n/a	6081	UDP
prometheus-k8s-0	NS openshift-monitoring	40710	worker01	n/a	10250	TCP
worker03	n/a	44872	worker01	n/a	6081	UDP
worker03	n/a	46033	worker01	n/a	10250	TCP
worker03	n/a	47429	worker01	n/a	6081	UDP
worker03	n/a	47782	worker01	n/a	6081	UDP
worker03	n/a	49286	thanos-ruler-user-work...	NS openshift-user-workdo...	9091	TCP
worker03	n/a	50460	worker01	n/a	6081	UDP
worker03	n/a	54261	worker01	n/a	10250	TCP
worker03	n/a	54491	worker01	n/a	6081	UDP
worker03	n/a	55445	worker01	n/a	6081	UDP

N worker03	n/a	57060	P thanos-querier-6d8bb...	NS openshift-monitoring	9091
N worker03	n/a	57076	P thanos-querier-6d8bb...	NS openshift-monitoring	9091
P thanos-querier-6d8bb...	NS openshift-monitoring	58022	P prometheus-user-work...	NS openshift-user-worklo...	10901
N worker03	n/a	59328	P prometheus-user-work...	NS openshift-user-worklo...	9092
P alertmanager-user-wor...	NS openshift-user-worklo...	60882	P alertmanager-user-wor...	NS openshift-user-worklo...	9094
N worker03	n/a	61029	N worker01	n/a	6081

```
[student@workstation ~]$ oc netobserv flows
```

```
Checking dependencies...
```

```
'yq' is up to date (version v4.45.1).
```

```
'bash' is up to date (version v5.1.8).
```

```
Setting up...
```

```
admin
```

```
creating netobserv-cli namespace
```

```
namespace/netobserv-cli created
```

```
creating service account
```

```
serviceaccount/netobserv-cli created
```

```
clusterrole.rbac.authorization.k8s.io/netobserv-cli configured
```

```
clusterrolebinding.rbac.authorization.k8s.io/netobserv-cli unchanged
```

```
clusterrole.rbac.authorization.k8s.io/netobserv-cli-metrics configured
```

```
clusterrolebinding.rbac.authorization.k8s.io/netobserv-cli-metrics unchanged
```

```
creating collector service
```

```
service/collector created
```

```
creating flow-capture agents:
```

```
daemonset.apps/netobserv-cli created
```

```
Waiting for daemon set "netobserv-cli" rollout to finish: 0 of 6 updated pods are available...
```

```
Waiting for daemon set "netobserv-cli" rollout to finish: 1 of 6 updated pods are available...
```

```
Waiting for daemon set "netobserv-cli" rollout to finish: 2 of 6 updated pods are available...
```

```
Waiting for daemon set "netobserv-cli" rollout to finish: 3 of 6 updated pods are available...
```

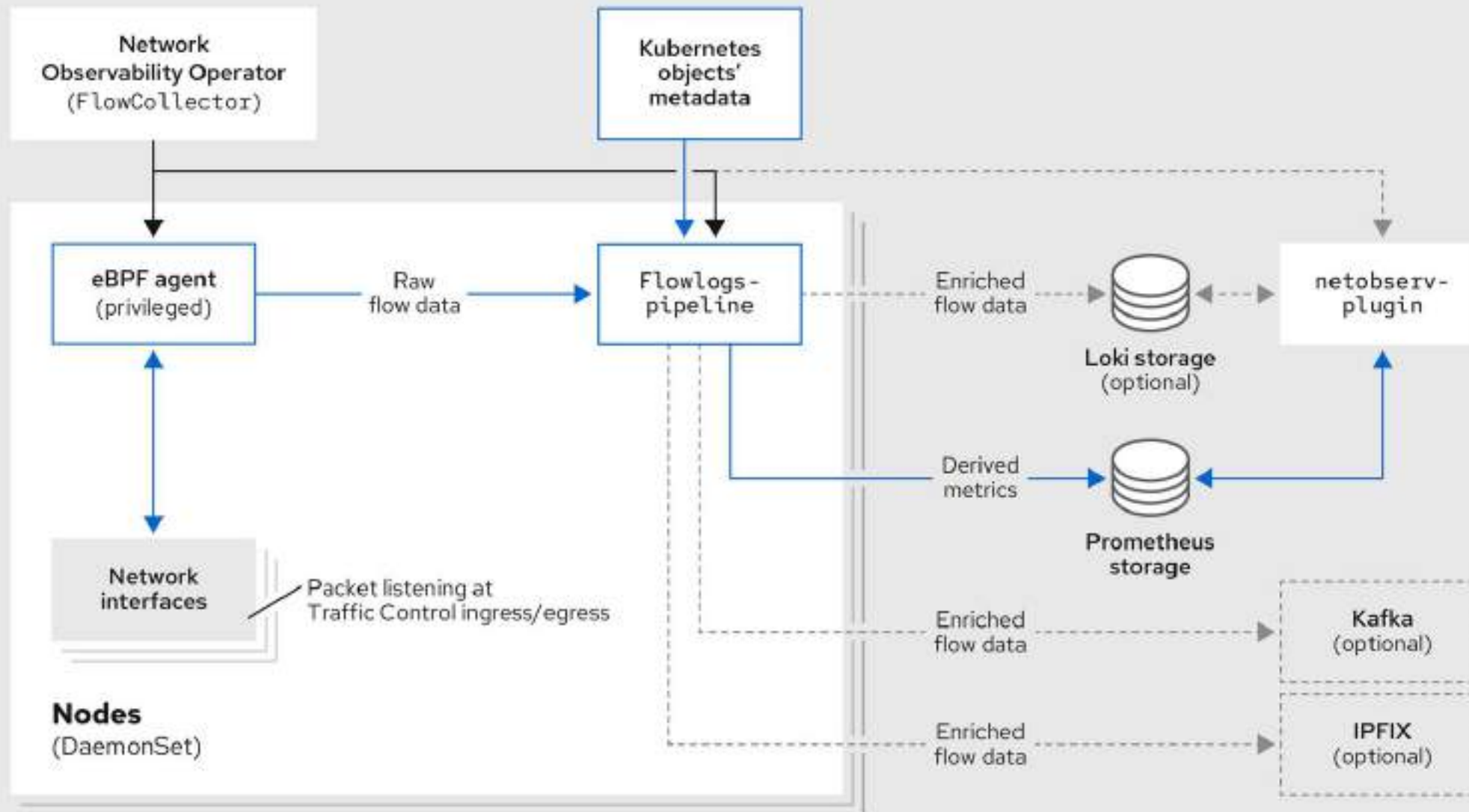
```
Waiting for daemon set "netobserv-cli" rollout to finish: 4 of 6 updated pods are available...
```

```
Waiting for daemon set "netobserv-cli" rollout to finish: 5 of 6 updated pods are available...
```

```
daemon set "netobserv-cli" successfully rolled out
```

```
Running network-observability-cli get-flows...
```

```
pod/collector created
```



Running network-observability-cli as Flow Capture
 Log level: Info Duration: 5s Capture size: 5.7MB
 Showing last: 35 Use Up / Down keyboard arrows to increase / decrease limit
 Display: Standard Use Left / Right keyboard arrows to cycle views
 Enrichment: Resource Use Page Up / Page Down keyboard keys to cycle enrichment scopes

Time	Source Node	Src Node	Src Name	Src Name	Src Namespace	Src Namespace	Interface	Interface Name	Dest Node	Dest Layer	Dest Layer
07:39:21.864000	n/a	Node	n/a	worker83	n/a	n/a	ens3	Ingress	Ingress	UDP	Standard
07:39:21.865000	Pod	Node	prometheus-k8s-0	worker82	openshift-monitoring	n/a	eth8,4b81745f7bb0425	Egress,Ingress	Egress	TCP	Standard
07:39:21.865000	Node	Node	worker83	worker82	n/a	n/a	ens3,br-ex	Egress,Ingress	Egress	TCP	Standard
07:39:21.866000	Node	Pod	worker82	prometheus-k8s-0	n/a	openshift-monitoring	4b81745f7bb0425,eth8	Egress,Ingress	Ingress	TCP	Standard
07:39:21.866000	Node	Node	worker82	worker83	n/a	n/a	ens3	Ingress	Ingress	TCP	Standard
07:39:21.868000	n/a	Pod	n/a	dns-default-fjhx2	n/a	openshift-dns	genev_sys_8081,d02c3ba322f921f,eth0	Ingress,Egress,Ingress	Ingress	UDP	Standard
07:39:21.868000	Node	Node	worker81	worker83	n/a	n/a	ens3,br-ex	Ingress,Ingress	Ingress	UDP	Standard
07:39:21.869000	Pod	n/a	dns-default-fjhx2	n/a	openshift-dns	n/a	eth0,d02c3ba322f921f,genev_sys_8081	Egress,Ingress,Egress	Egress	UDP	Standard
07:39:21.869000	Node	Node	worker83	worker81	n/a	n/a	br-ex,ens3	Egress,Egress	Egress	UDP	Standard
07:39:21.875000	Node	Node	worker82	worker83	n/a	n/a	ens3,br-ex	Ingress,Ingress	Ingress	UDP	Standard
07:39:21.876000	n/a	Pod	n/a	dns-default-fjhx2	n/a	openshift-dns	genev_sys_8081,d02c3ba322f921f,eth8	Ingress,Egress,Ingress	Ingress	UDP	Standard
07:39:21.876000	Node	Node	worker83	worker82	n/a	n/a	br-ex,ens3	Egress,Egress	Egress	UDP	Standard
07:39:21.878000	Node	Node	worker83	worker82	n/a	n/a	br-ex,ens3	Egress,Egress	Egress	UDP	Standard
07:39:21.878000	Pod	n/a	dns-default-fjhx2	n/a	openshift-dns	n/a	eth8,d02c3ba322f921f,genev_sys_8081	Egress,Ingress,Egress	Egress	UDP	Standard
07:39:21.882000	Node	Node	worker82	worker83	n/a	n/a	ens3,br-ex	Ingress,Ingress	Ingress	UDP	Standard
07:39:21.882000	Pod	n/a	dns-default-fjhx2	n/a	openshift-dns	n/a	eth0,d02c3ba322f921f,genev_sys_8081	Egress,Ingress,Egress	Egress	UDP	Standard
07:39:21.883000	n/a	Pod	n/a	dns-default-fjhx2	n/a	openshift-dns	genev_sys_8081,d02c3ba322f921f,eth0	Ingress,Egress,Ingress	Ingress	UDP	Standard
07:39:21.883000	Node	Node	worker83	worker82	n/a	n/a	br-ex,ens3	Egress,Egress	Egress	UDP	Standard
07:39:21.884000	Pod	n/a	dns-default-fjhx2	n/a	openshift-dns	n/a	eth8,d02c3ba322f921f,genev_sys_8081	Egress,Ingress,Egress	Egress	UDP	Standard
07:39:21.884000	Node	Node	worker81	worker83	n/a	n/a	br-ex,ens3	Egress,Egress	Egress	UDP	Standard
07:39:21.884000	Node	Node	worker81	worker83	n/a	n/a	ens3,br-ex	Ingress,Ingress	Ingress	UDP	Standard
07:39:21.884000	n/a	Pod	n/a	dns-default-fjhx2	n/a	openshift-dns	genev_sys_8081,d02c3ba322f921f,eth8	Ingress,Egress,Ingress	Ingress	UDP	Standard
07:39:21.886000	Node	Node	worker81	worker83	n/a	n/a	ens3,br-ex	Ingress,Ingress	Ingress	UDP	Standard
07:39:21.886000	Node	Node	worker83	worker81	n/a	n/a	br-ex,ens3	Egress,Egress	Egress	UDP	Standard
07:39:21.890000	Pod	n/a	dns-default-fjhx2	n/a	openshift-dns	n/a	eth8,d02c3ba322f921f,genev_sys_8081	Egress,Ingress,Egress	Egress	UDP	Standard
07:39:21.890000	n/a	Pod	n/a	dns-default-fjhx2	n/a	openshift-dns	genev_sys_8081,d02c3ba322f921f,eth0	Ingress,Egress,Ingress	Ingress	UDP	Standard
07:39:21.890000	Pod	Pod	network-metrics-daemon-wdhy	prometheus-k8s-1	openshift-multus	openshift-monitoring	eth0,015136010d0b2f,genev_sys_8081	Egress,Ingress,Egress	Egress	TCP	Standard
07:39:21.890000	Node	Node	worker83	worker81	n/a	n/a	br-ex,ens3	Egress,Egress	Egress	UDP	Standard
07:39:21.890000	Pod	Pod	prometheus-k8s-1	network-metrics-daemon-wdhy	openshift-monitoring	openshift-multus	genev_sys_8081,015136010d0b2f,eth0	Ingress,Egress,Ingress	Ingress	TCP	Standard
07:39:21.890000	Node	Node	worker81	worker83	n/a	n/a	ens3,br-ex	Ingress,Ingress	Ingress	UDP	Standard
07:39:21.897000	Pod	Pod	controller-7bc4c8677c-898xt	prometheus-k8s-1	metallb-system	openshift-monitoring	eth8,3f1858e7af27c5e,genev_sys_8081	Egress,Ingress,Egress	Egress	TCP	Standard
07:39:21.897000	Node	Node	worker83	worker81	n/a	n/a	br-ex,ens3	Egress,Egress	Egress	UDP	Standard
07:39:21.898000	Pod	Pod	prometheus-k8s-1	controller-7bc4c8677c-898xt	openshift-monitoring	metallb-system	genev_sys_8081,3f1858e7af27c5e,eth8	Ingress,Egress,Ingress	Ingress	TCP	Standard
07:39:21.898000	Node	Node	worker81	worker83	n/a	n/a	ens3,br-ex	Ingress,Ingress	Ingress	UDP	Standard
07:39:21.899000	n/a	Node	n/a	worker83	n/a	n/a	ens3,br-ex	Ingress,Ingress	Ingress	TCP	Standard
07:39:21.899000	Node	n/a	worker83	n/a	n/a	n/a	br-ex,ens3	Egress,Egress	Egress	TCP	Standard

Type anything to filter incoming flows in view

INFO[0894] Ctrl-C pressed, exiting program.

admin

Copy the capture output locally? [yes/no] ☐

Running network-observability-cli as Flow Capture

Log level: Info Duration: 7s Capture size: 0.02MB

Showing last: 35 Use Up / Down keyboard arrows to increase / decrease limit

Display: Standard Use Left / Right keyboard arrows to cycle views

Enrichment: Resource Use Page Up / Page Down keyboard keys to cycle enrichment scopes

End Time	Src Kind	Dst Kind	Src Name	Dst Name	Src Namespace
07:33:22.770000	Node	Node	master02	worker02	n/a
07:33:22.780000	Node	Node	worker02	master02	n/a
07:33:22.800000	Service	Pod	kubernetes	prometheus-k8s-1	default
07:33:22.800000	Node	Node	worker01	master03	n/a
07:33:22.800000	Node	Node	master03	worker01	n/a
07:33:22.800000	Pod	Service	prometheus-k8s-1	kubernetes	openshift-mon
07:33:22.810000	Pod	Pod	prometheus-user-workload-0	thanos-querier-6d8bb7f8db-nmkdx	openshift-user
07:33:22.810000	Node	Node	worker03	worker01	n/a
07:33:22.810000	Pod	Pod	thanos-ruler-user-workload-1	thanos-querier-6d8bb7f8db-nmkdx	openshift-user
07:33:22.810000	Pod	Pod	thanos-querier-6d8bb7f8db-nmkdx	prometheus-user-workload-1	openshift-mon
07:33:22.810000	Pod	Pod	thanos-querier-6d8bb7f8db-nmkdx	prometheus-user-workload-0	openshift-mon
07:33:22.810000	Pod	Pod	thanos-ruler-user-workload-0	thanos-querier-6d8bb7f8db-nmkdx	openshift-user
07:33:22.810000	Node	Node	worker01	worker03	n/a
07:33:22.810000	Pod	Pod	prometheus-user-workload-1	thanos-querier-6d8bb7f8db-nmkdx	openshift-user
07:33:22.810000	Node	Node	worker03	worker01	n/a
07:33:22.820000	Node	Node	worker03	worker01	n/a
07:33:22.820000	Pod	Pod	prometheus-k8s-0	thanos-querier-6d8bb7f8db-nmkdx	openshift-mon
07:33:22.821000	Node	Node	worker01	worker03	n/a
07:33:22.821000	Pod	Pod	thanos-querier-6d8bb7f8db-nmkdx	prometheus-k8s-0	openshift-mon
07:33:22.830000	Node	Node	worker01	master03	n/a
07:33:22.830000	Node	Node	master03	worker01	n/a
07:33:22.834000	Pod	Pod	prometheus-k8s-1	thanos-querier-6d8bb7f8db-nmkdx	openshift-mon
07:33:22.836000	Pod	Pod	thanos-querier-6d8bb7f8db-nmkdx	prometheus-k8s-1	openshift-mon
07:33:22.837000	Node	Node	worker01	master02	n/a
07:33:22.837000	Node	Node	master02	worker01	n/a
07:33:22.837000	Pod	n/a	collector	n/a	netobserv-cl
07:33:22.839000	n/a	Pod	n/a	collector	n/a
07:33:23.160000	Node	Node	worker02	worker03	n/a
07:33:23.160000	Pod	Pod	image-registry-cffdd7744-krgrb	prometheus-k8s-0	openshift-imag
07:33:23.161000	Pod	Pod	prometheus-k8s-0	image-registry-cffdd7744-krgrb	openshift-mon
07:33:23.161000	Node	Node	worker03	worker02	n/a
07:33:23.190000	Node	Node	worker03	worker02	n/a
07:33:23.191000	Node	Node	worker02	worker03	n/a
07:33:23.443000	Node	n/a	worker02	n/a	n/a
07:33:23.443000	n/a	Node	n/a	worker02	n/a

Type anything to filter incoming flows in view

INFO[0006] Ctrl-C pressed, exiting program.

admin

Copy the capture output locally? [yes/no] yes

Interface #5372 info:

Name = Pod: metallb-operator-controller-manager-7d94f788f7-rtvxx -> Node: worker03
Description = Deployment: metallb-operator-controller-manager Namespace: metallb-system -> Node: worker03 Namespace: n/a
Encapsulation = Ethernet (1 - ether)
Capture length = 4294967295
Time precision = microseconds (6)
Time ticks per second = 1000000
Number of stat entries = 0
Number of packets = 1

Interface #5373 info:

Name = Node: worker03 -> Pod: metallb-operator-controller-manager-7d94f788f7-rtvxx
Description = Node: worker03 Namespace: n/a -> Deployment: metallb-operator-controller-manager Namespace: metallb-system
Encapsulation = Ethernet (1 - ether)
Capture length = 4294967295
Time precision = microseconds (6)
Time ticks per second = 1000000
Number of stat entries = 0
Number of packets = 1

Interface #5374 info:

Name = Node: worker03 -> Pod: metallb-operator-controller-manager-7d94f788f7-rtvxx
Description = Node: worker03 Namespace: n/a -> Deployment: metallb-operator-controller-manager Namespace: metallb-system
Encapsulation = Ethernet (1 - ether)
Capture length = 4294967295
Time precision = microseconds (6)
Time ticks per second = 1000000
Number of stat entries = 0
Number of packets = 1

[student@workstation output]\$ capinfos pcap/2025-11-05T052830Z.pcapng |grep -c Interface

5375



Syntax: netobserv packets [options]

filters:

--action:	filter action	(default: Accept)
--cidr:	filter CIDR	(default: 0.0.0.0/0)
--direction:	filter direction	(default: n/a)
--dport:	filter destination port	(default: n/a)
--dport_range:	filter destination port range	(default: n/a)
--dports:	filter on either of two destination ports	(default: n/a)
--drops:	filter flows with only dropped packets	(default: false)
--icmp_code:	filter ICMP code	(default: n/a)
--icmp_type:	filter ICMP type	(default: n/a)
--node-selector:	capture on specific nodes	(default: n/a)
--peer_ip:	filter peer IP	(default: n/a)
--peer_cidr:	filter peer CIDR	(default: n/a)
--port_range:	filter port range	(default: n/a)
--port:	filter port	(default: n/a)
--ports:	filter on either of two ports	(default: n/a)
--protocol:	filter protocol	(default: n/a)
--query:	filter flows using a custom query	(default: n/a)
--sport_range:	filter source port range	(default: n/a)
--sport:	filter source port	(default: n/a)
--sports:	filter on either of two source ports	(default: n/a)
--tcp_flags:	filter TCP flags	(default: n/a)

options:

--background:	run in background	(default: false)
--copy:	copy the output files locally	(default: prompt)
--log-level:	components logs	(default: info)
--max-time:	maximum capture time	(default: 5m)
--max-bytes:	maximum capture bytes	(default: 50000000 = 50MB)
--yaml:	generate YAML without applying it	(default: false)


```
Cleaning up...
Deleting service monitor...
Deleting dashboard configmap...
Deleting daemonset...
Deleting pod...
Deleting namespace... namespace "netobserv-cli" deleted
^C
[student@workstation test]$ oc netobserv packets --peer_ip=10.8.2.128
Checking dependencies...
'yq' is up to date (version v4.45.1).
'bash' is up to date (version v5.1.8).
Setting up...
admin
creating netobserv-cli namespace
namespace/netobserv-cli created
creating service account
serviceaccount/netobserv-cli created
clusterrole.rbac.authorization.k8s.io/netobserv-cli configured
clusterrolebinding.rbac.authorization.k8s.io/netobserv-cli unchanged
creating collector service
service/collector created
creating packet-capture agents
opt: filter_peer_ip, value: 10.8.2.128
```

```
Collector is waiting for messages... Please wait.  
Running network-observability-cli as Packet Capture  
log level: info Duration: 3s Capture size: 0B
```


Options: peer_ip=10.8.2.128

```
Collector is waiting for messages... Please wait.  
Running network-observability-cli as Packet Capture  
Log level: Info Duration: 3s Capture size: 0B  
Options: peer_ip=10.8.2.128
```

```
Collector is waiting for messages... Please wait.  
Running network-observability-cli as Packet Capture  
Log level: info Duration: 4s Capture size: 8B  
Options: peer_ip=10.8.2.128
```

```
Collector is waiting for messages... Please wait.  
Running network-observability-cli as Packet Capture  
Log level: info Duration: 5s Capture size: 8B  
Options: peer_ip=10.8.2.128
```

```
Collector is waiting for messages... Please wait.  
Running network-observability-cli as Packet Capture  
Log level: Info Duration: 6s Capture size: 34.9KB  
Options: peer_ip=10.8.2.128
```

Showing last: 20 Use Up / Down keyboard arrows to increase / decrease limit

Display: Standard Use Left / Right keyboard arrows to cycle views

Enrichment: Resource Use Page Up / Page Down keyboard keys to cycle enrichment scopes

End Time	Src Kind	Dst Kind	Src Name	Dst Name	Src Namespace	Dst Namespace	Interfaces	IntfIP
09:32:28.241000	Pod	Pod	shark-b-6ddc49b8cd-n9qsh	shark-a-ff7cdd4d8-gzmms	sharkproject-b	sharkproject-a	n/a	n/a
09:32:28.241000	Pod	Pod	shark-b-6ddc49b8cd-n9qsh	shark-a-ff7cdd4d8-gzmms	sharkproject-b	sharkproject-a	n/a	n/a
09:32:28.241000	Pod	Pod	shark-a-ff7cdd4d8-gzmms	shark-b-6ddc49b8cd-n9qsh	sharkproject-a	sharkproject-b	n/a	n/a
09:32:28.241000	Pod	Pod	shark-a-ff7cdd4d8-gzmms	shark-b-6ddc49b8cd-n9qsh	sharkproject-a	sharkproject-b	n/a	n/a
09:32:28.241000	Pod	Pod	shark-b-6ddc49b8cd-n9qsh	shark-a-ff7cdd4d8-gzmms	sharkproject-b	sharkproject-a	n/a	n/a
09:32:28.241000	Pod	Pod	shark-b-6ddc49b8cd-n9qsh	shark-a-ff7cdd4d8-gzmms	sharkproject-b	sharkproject-a	n/a	n/a
09:32:28.241000	Pod	Pod	shark-b-6ddc49b8cd-n9qsh	shark-a-ff7cdd4d8-gzmms	sharkproject-b	sharkproject-a	n/a	n/a
09:32:28.241000	Pod	Pod	shark-b-6ddc49b8cd-n9qsh	shark-a-ff7cdd4d8-gzmms	sharkproject-b	sharkproject-a	n/a	n/a
09:32:28.241000	Pod	Pod	shark-a-ff7cdd4d8-gzmms	shark-b-6ddc49b8cd-n9qsh	sharkproject-a	sharkproject-b	n/a	n/a
09:32:28.241000	Pod	Pod	shark-a-ff7cdd4d8-gzmms	shark-b-6ddc49b8cd-n9qsh	sharkproject-a	sharkproject-b	n/a	n/a
09:32:28.241000	Pod	Pod	shark-a-ff7cdd4d8-gzmms	shark-b-6ddc49b8cd-n9qsh	sharkproject-a	sharkproject-b	n/a	n/a
09:32:28.241000	Pod	Pod	shark-a-ff7cdd4d8-gzmms	shark-b-6ddc49b8cd-n9qsh	sharkproject-a	sharkproject-b	n/a	n/a
09:32:28.241000	Pod	Pod	shark-b-6ddc49b8cd-n9qsh	shark-a-ff7cdd4d8-gzmms	sharkproject-b	sharkproject-a	n/a	n/a
09:32:28.241000	Pod	Pod	shark-b-6ddc49b8cd-n9qsh	shark-a-ff7cdd4d8-gzmms	sharkproject-b	sharkproject-a	n/a	n/a
09:32:28.241000	Pod	Pod	shark-b-6ddc49b8cd-n9qsh	shark-a-ff7cdd4d8-gzmms	sharkproject-b	sharkproject-a	n/a	n/a
09:32:28.241000	Pod	Pod	shark-b-6ddc49b8cd-n9qsh	shark-a-ff7cdd4d8-gzmms	sharkproject-b	sharkproject-a	n/a	n/a

End Time	Src Kind	Dst Kind	Src Name	Dst Name	Src Namespace	Dst Namespace	Interfaces	Interf
09:32:28.271000	Pod	Pod	shark-b-6ddc49b8cd-n9qsh	shark-a-ff7cdd4d8-gzmms	sharkproject-b	sharkproject-a	n/a	n/a
09:32:28.271000	Pod	Pod	shark-b-6ddc49b8cd-n9qsh	shark-a-ff7cdd4d8-gzmms	sharkproject-b	sharkproject-a	n/a	n/a
09:32:28.271000	Pod	Pod	shark-a-ff7cdd4d8-gzmms	shark-b-6ddc49b8cd-n9qsh	sharkproject-a	sharkproject-b	n/a	n/a
09:32:28.271000	Pod	Pod	shark-a-ff7cdd4d8-gzmms	shark-b-6ddc49b8cd-n9qsh	sharkproject-a	sharkproject-b	n/a	n/a
09:32:28.271000	Pod	Pod	shark-b-6ddc49b8cd-n9qsh	shark-a-ff7cdd4d8-gzmms	sharkproject-b	sharkproject-a	n/a	n/a
09:32:28.271000	Pod	Pod	shark-b-6ddc49b8cd-n9qsh	shark-a-ff7cdd4d8-gzmms	sharkproject-b	sharkproject-a	n/a	n/a
09:32:28.271000	Pod	Pod	shark-b-6ddc49b8cd-n9qsh	shark-a-ff7cdd4d8-gzmms	sharkproject-b	sharkproject-a	n/a	n/a
09:32:28.271000	Pod	Pod	shark-b-6ddc49b8cd-n9qsh	shark-a-ff7cdd4d8-gzmms	sharkproject-b	sharkproject-a	n/a	n/a
09:32:28.271000	Pod	Pod	shark-b-6ddc49b8cd-n9qsh	shark-a-ff7cdd4d8-gzmms	sharkproject-b	sharkproject-a	n/a	n/a
09:32:28.271000	Pod	Pod	shark-b-6ddc49b8cd-n9qsh	shark-a-ff7cdd4d8-gzmms	sharkproject-b	sharkproject-a	n/a	n/a
09:32:28.271000	Pod	Pod	shark-a-ff7cdd4d8-gzmms	shark-b-6ddc49b8cd-n9qsh	sharkproject-a	sharkproject-b	n/a	n/a
09:32:28.271000	Pod	Pod	shark-a-ff7cdd4d8-gzmms	shark-b-6ddc49b8cd-n9qsh	sharkproject-a	sharkproject-b	n/a	n/a
09:32:28.271000	Pod	Pod	shark-a-ff7cdd4d8-gzmms	shark-b-6ddc49b8cd-n9qsh	sharkproject-a	sharkproject-b	n/a	n/a
09:32:28.271000	Pod	Pod	shark-a-ff7cdd4d8-gzmms	shark-b-6ddc49b8cd-n9qsh	sharkproject-a	sharkproject-b	n/a	n/a
09:32:28.271000	Pod	Pod	shark-b-6ddc49b8cd-n9qsh	shark-a-ff7cdd4d8-gzmms	sharkproject-b	sharkproject-a	n/a	n/a
09:32:28.271000	Pod	Pod	shark-b-6ddc49b8cd-n9qsh	shark-a-ff7cdd4d8-gzmms	sharkproject-b	sharkproject-a	n/a	n/a
09:32:28.271000	Pod	Pod	shark-b-6ddc49b8cd-n9qsh	shark-a-ff7cdd4d8-gzmms	sharkproject-b	sharkproject-a	n/a	n/a
09:32:28.271000	Pod	Pod	shark-a-ff7cdd4d8-gzmms	shark-b-6ddc49b8cd-n9qsh	sharkproject-a	sharkproject-b	n/a	n/a
09:32:28.271000	Pod	Pod	shark-a-ff7cdd4d8-gzmms	shark-b-6ddc49b8cd-n9qsh	sharkproject-a	sharkproject-b	n/a	n/a
09:32:28.271000	Pod	Pod	shark-b-6ddc49b8cd-n9qsh	shark-a-ff7cdd4d8-gzmms	sharkproject-b	sharkproject-a	n/a	n/a
09:32:28.271000	Pod	Pod	shark-b-6ddc49b8cd-n9qsh	shark-a-ff7cdd4d8-gzmms	sharkproject-b	sharkproject-a	n/a	n/a

Type anything to filter incoming flows in view

^Ccommand terminated with exit code 130

admin

Copy the capture output locally? [yes/no] yes

Copying collector output files...

Cleaning up...

Deleting service monitor...

Deleting dashboard configmap...

Deleting daemonset... daemonset.apps "netobserv-cli" deleted

Deleting pod... pod "collector" deleted

Deleting namespace... namespace "netobserv-cli" deleted

[student@workstation test]\$ tree

```

├── output
│   └── pcap
│       └── 2025-11-05T131045Z.pcapng

```

2 directories, 1 file

```
[student@workstation test]$ capinfos output/pcap/2025-11-05T131045Z.pcapng
capinfos: An error occurred after reading 163 packets from "output/pcap/2025-11-05T131045Z.pcapng".
capinfos: The file "output/pcap/2025-11-05T131045Z.pcapng" appears to have been cut short in the middle of a packet.
(will continue anyway, checksums might be incorrect)
File name:          output/pcap/2025-11-05T131045Z.pcapng
File type:          Wireshark/... - pcapng
File encapsulation: Ethernet
File timestamp precision: nanoseconds (9)
Packet size limit:  file hdr: (not set)
Number of packets:  163
File size:          122kB
Data size:          16kB
Capture duration:   36.800000000 seconds
First packet time:  2025-11-05 08:10:35.000000000
Last packet time:   2025-11-05 08:11:11.000000000
Data byte rate:     457 bytes/s
Data bit rate:      3668 bits/s
Average packet size: 101.04 bytes
Average packet rate: 4 packets/s
SHA256:             383940846a82ec08ec9aa56270f6faa08a1fa4e3dee9d581053c20d0ac697e57
RIPEMD160:          fc450b53f9ac27cdbaf67ab5ff7b91446ed05d5a
SHA1:               d1139e997fa617f142c54293b53782db99e36872
Strict time order:  False
Capture hardware:   amd64
Capture oper-sys:   linux
Capture application: gopacket
Number of interfaces in file: 1
Interface #0 info:
    Name = intf0
    Encapsulation = Ethernet (1 - ether)
    Capture length = 0
    Time precision = nanoseconds (9)
    Time ticks per second = 1000000000
    Time resolution = 0x09
    Operating system = linux
    Number of stat entries = 0
    Number of packets = 163
```



```

130 36.000000000 10.9.2.34 → 10.8.2.128 HTTP 145 GET / HTTP/1.1
131 36.000000000 10.9.2.34 → 10.8.2.128 TCP 66 56036 → 8080 [ACK] Seq=1 Ack=1 Win=65280 Len=0 TSval=2913063180 TSecr=437252538
132 36.000000000 10.9.2.34 → 10.8.2.128 TCP 145 [TCP Retransmission] 56036 → 8080 [PSH, ACK] Seq=1 Ack=1 Win=65280 Len=79 TSval=2913063180 TSecr=437252538
133 36.000000000 10.8.2.128 → 10.9.2.34 TCP 66 8080 → 56036 [ACK] Seq=1 Ack=80 Win=64640 Len=0 TSval=437252541 TSecr=2913063180
134 36.000000000 10.8.2.128 → 10.9.2.34 TCP 66 [TCP Dup ACK 133#1] 8080 → 56036 [ACK] Seq=1 Ack=80 Win=64640 Len=0 TSval=437252541 TSecr=2913063180
135 36.000000000 10.8.2.128 → 10.9.2.34 HTTP 328 HTTP/1.1 200 OK (text/html)
136 36.000000000 10.8.2.128 → 10.9.2.34 TCP 328 [TCP Retransmission] 8080 → 56036 [PSH, ACK] Seq=1 Ack=80 Win=64640 Len=262 TSval=437252541 TSecr=2913063180
137 36.000000000 10.9.2.34 → 10.8.2.128 TCP 66 56036 → 8080 [ACK] Seq=80 Ack=263 Win=65024 Len=0 TSval=2913063181 TSecr=437252541
138 36.000000000 10.9.2.34 → 10.8.2.128 TCP 66 [TCP Dup ACK 137#1] 56036 → 8080 [ACK] Seq=80 Ack=263 Win=65024 Len=0 TSval=2913063181 TSecr=437252541
139 36.000000000 10.9.2.34 → 10.8.2.128 TCP 66 56036 → 8080 [FIN, ACK] Seq=80 Ack=263 Win=65024 Len=0 TSval=2913063181 TSecr=437252541
140 36.000000000 10.9.2.34 → 10.8.2.128 TCP 66 [TCP Out-Of-Order] 56036 → 8080 [FIN, ACK] Seq=80 Ack=263 Win=65024 Len=0 TSval=2913063181 TSecr=437252541
141 36.000000000 10.8.2.128 → 10.9.2.34 TCP 66 8080 → 56036 [FIN, ACK] Seq=263 Ack=81 Win=64640 Len=0 TSval=437252542 TSecr=2913063181
142 36.000000000 10.8.2.128 → 10.9.2.34 TCP 66 [TCP Out-Of-Order] 8080 → 56036 [FIN, ACK] Seq=263 Ack=81 Win=64640 Len=0 TSval=437252542 TSecr=2913063181
143 36.000000000 10.9.2.34 → 10.8.2.128 TCP 66 56036 → 8080 [ACK] Seq=81 Ack=264 Win=65024 Len=0 TSval=2913063181 TSecr=437252542
144 36.000000000 10.9.2.34 → 10.8.2.128 TCP 66 [TCP Dup ACK 143#1] 56036 → 8080 [ACK] Seq=81 Ack=264 Win=65024 Len=0 TSval=2913063181 TSecr=437252542
145 36.000000000 10.9.2.34 → 10.8.2.128 TCP 74 [TCP Out-Of-Order] 56036 → 8080 [SYN] Seq=0 Win=65280 Len=0 MSS=1360 SACK_PERM=1 TSval=2913063176 TSecr=0 WS=128
146 36.000000000 10.9.2.34 → 10.8.2.128 TCP 74 [TCP Out-Of-Order] 56036 → 8080 [SYN] Seq=0 Win=65280 Len=0 MSS=1360 SACK_PERM=1 TSval=2913063176 TSecr=0 WS=128
147 36.000000000 10.8.2.128 → 10.9.2.34 TCP 74 [TCP Out-Of-Order] 8080 → 56036 [SYN, ACK] Seq=0 Ack=1 Win=64704 Len=0 MSS=1360 SACK_PERM=1 TSval=437252538 TSecr=2913063180
148 36.000000000 10.8.2.128 → 10.9.2.34 TCP 74 [TCP Out-Of-Order] 8080 → 56036 [SYN, ACK] Seq=0 Ack=1 Win=64704 Len=0 MSS=1360 SACK_PERM=1 TSval=437252538 TSecr=2913063180
149 36.000000000 10.9.2.34 → 10.8.2.128 TCP 66 56036 → 8080 [ACK] Seq=1 Ack=1 Win=65280 Len=0 TSval=2913063180 TSecr=437252538
150 36.000000000 10.9.2.34 → 10.8.2.128 TCP 145 [TCP Out-Of-Order] 56036 → 8080 [PSH, ACK] Seq=1 Ack=1 Win=65280 Len=79 TSval=2913063180 TSecr=437252538
151 36.000000000 10.9.2.34 → 10.8.2.128 TCP 66 56036 → 8080 [ACK] Seq=1 Ack=1 Win=65280 Len=0 TSval=2913063180 TSecr=437252538
152 36.000000000 10.9.2.34 → 10.8.2.128 TCP 145 [TCP Out-Of-Order] 56036 → 8080 [PSH, ACK] Seq=1 Ack=1 Win=65280 Len=79 TSval=2913063180 TSecr=437252538
153 36.000000000 10.8.2.128 → 10.9.2.34 TCP 66 8080 → 56036 [ACK] Seq=1 Ack=80 Win=64640 Len=0 TSval=437252541 TSecr=2913063180
154 36.000000000 10.8.2.128 → 10.9.2.34 TCP 66 8080 → 56036 [ACK] Seq=1 Ack=80 Win=64640 Len=0 TSval=437252541 TSecr=2913063180
155 36.000000000 10.8.2.128 → 10.9.2.34 TCP 328 [TCP Out-Of-Order] 8080 → 56036 [PSH, ACK] Seq=1 Ack=80 Win=64640 Len=262 TSval=437252541 TSecr=2913063180
156 36.000000000 10.8.2.128 → 10.9.2.34 TCP 328 [TCP Out-Of-Order] 8080 → 56036 [PSH, ACK] Seq=1 Ack=80 Win=64640 Len=262 TSval=437252541 TSecr=2913063180
157 36.000000000 10.9.2.34 → 10.8.2.128 TCP 66 [TCP Keep-Alive] 56036 → 8080 [ACK] Seq=80 Ack=263 Win=65024 Len=0 TSval=2913063181 TSecr=437252541
158 36.000000000 10.9.2.34 → 10.8.2.128 TCP 66 [TCP Keep-Alive] 56036 → 8080 [ACK] Seq=80 Ack=263 Win=65024 Len=0 TSval=2913063181 TSecr=437252541
159 36.000000000 10.9.2.34 → 10.8.2.128 TCP 66 [TCP Out-Of-Order] 56036 → 8080 [FIN, ACK] Seq=80 Ack=263 Win=65024 Len=0 TSval=2913063181 TSecr=437252541
160 36.000000000 10.9.2.34 → 10.8.2.128 TCP 66 [TCP Out-Of-Order] 56036 → 8080 [FIN, ACK] Seq=80 Ack=263 Win=65024 Len=0 TSval=2913063181 TSecr=437252541
161 36.000000000 10.8.2.128 → 10.9.2.34 TCP 66 [TCP Out-Of-Order] 8080 → 56036 [FIN, ACK] Seq=263 Ack=81 Win=64640 Len=0 TSval=437252542 TSecr=2913063181
162 36.000000000 10.8.2.128 → 10.9.2.34 TCP 66 [TCP Out-Of-Order] 8080 → 56036 [FIN, ACK] Seq=263 Ack=81 Win=64640 Len=0 TSval=437252542 TSecr=2913063181
163 36.000000000 10.9.2.34 → 10.8.2.128 TCP 66 56036 → 8080 [ACK] Seq=81 Ack=264 Win=65024 Len=0 TSval=2913063181 TSecr=437252542

```

tshark: The file "output/pcap/2025-11-05T131045Z.pcapng" appears to have been cut short in the middle of a packet.

```
sergey@sharkfest:~$ tshark -r /var/tmp/2025-11-05T131045Z-.pcapng -q -T fields -e frame.protocols|sort -u  
eth:ethertype:ip:tcp  
eth:ethertype:ip:tcp:http  
eth:ethertype:ip:tcp:http:data-text-lines
```


Feedback



Sergey Guzenkov RHCA
Principal Instructor at Red Hat



#sf25eu