OVS Extension

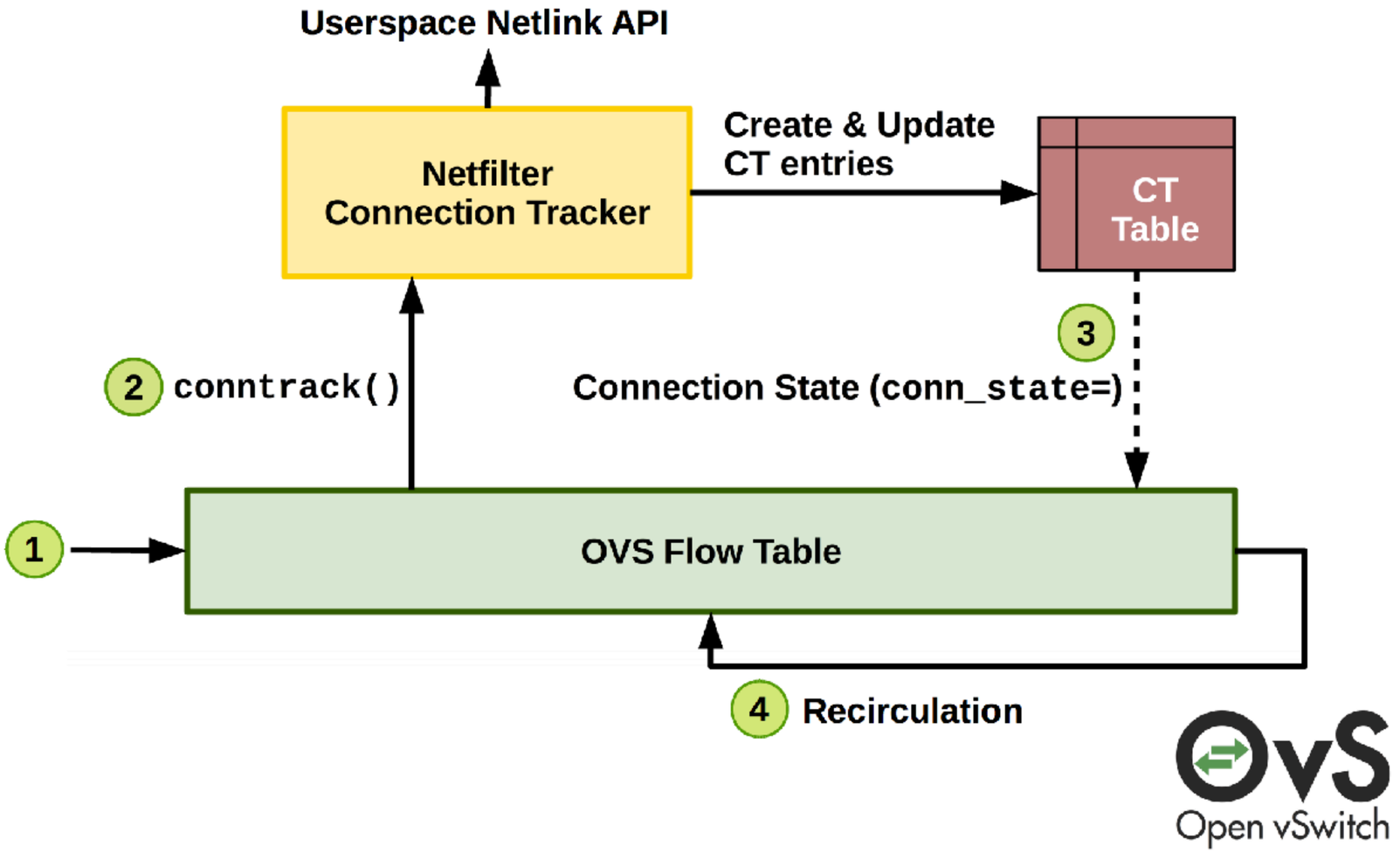
ONOS Korea Dev Forum 2/17/2016

Sangho Shin

OVS Extension

- Connection Tracking : OVS 2.5
- NAT: OVS 2.6

OVS ConnTrack Architecture

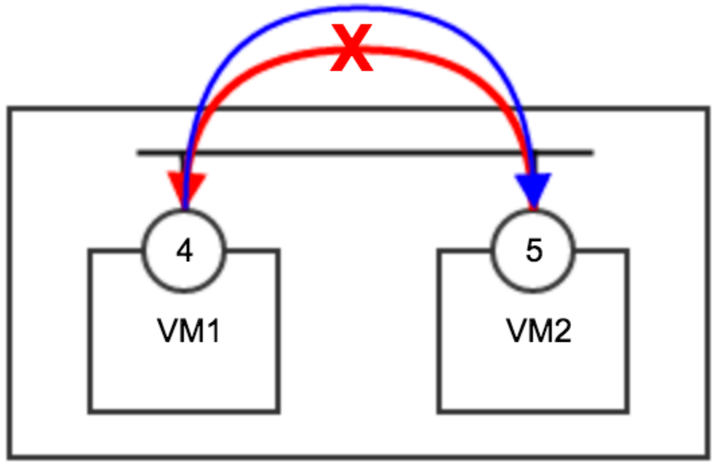


Ref: http://openvswitch.org/support/ovscon2014/17/1030-conntrack_nat.pdf

OVS Extension Dev Env

- Kernel 4.3.0 and above
- OVS 2.5 and above
- conntrack execution: modprobe nf_conntrack_ipv4
- conntrack feature check: sudo ovs-appctl dpctl/dump-conntrack

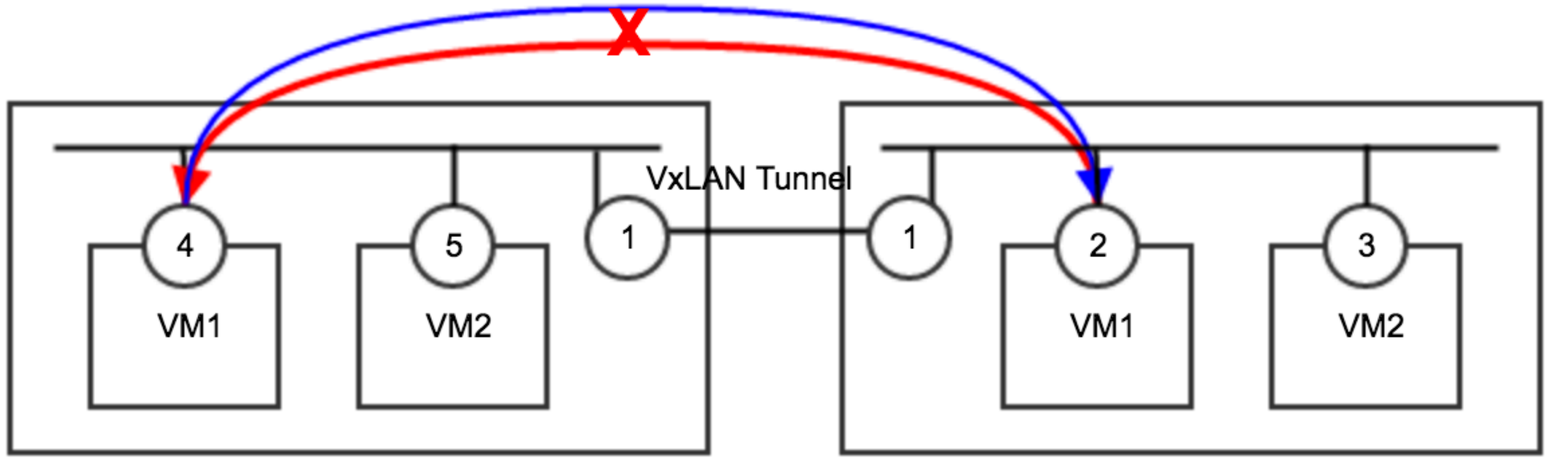
Test I




```
table=0,priority=100,ip,ct_state=-trk,action=ct(table=1)
table=1,in_port=4,ip,ct_state=+trk+new,action=ct(commit),normal
table=1,in_port=4,ip,ct_state=+trk+est,action=5
table=1,in_port=5,ip,ct_state=+trk+new,action=drop
table=1,in_port=5,ip,ct_state=+trk+est,action=4
```

```
sudo ovs-appctl dpctl/dump-conntrack
icmp,orig=(src=10.10.0.12,dst=10.10.0.13,id=18945),reply=(src=10.10.0.13,dst=10.10.0.12,id=18945)
```

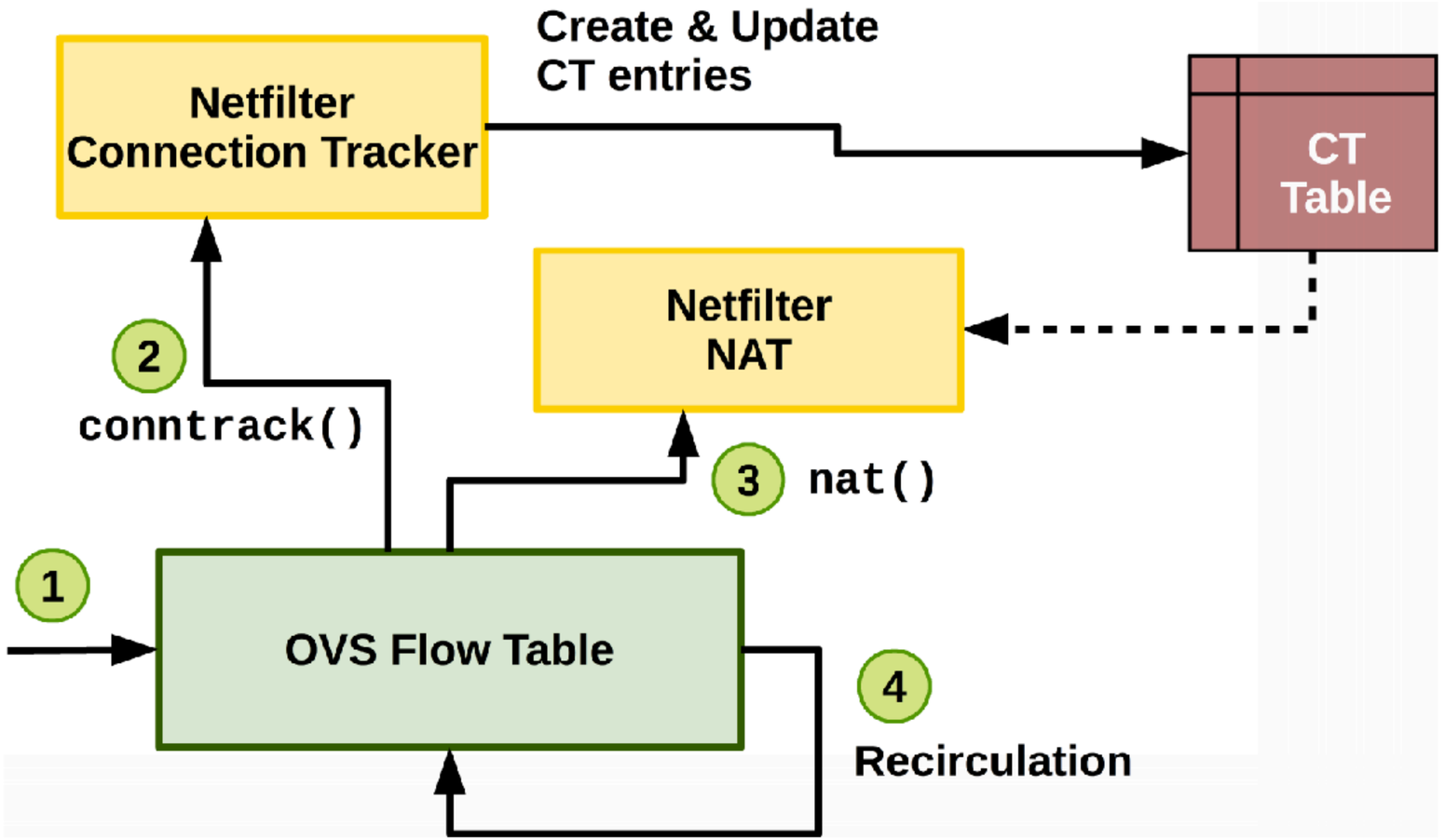
Test II




```
table=3,priority=100,ip,ct_state=-trk,action=ct(table=4)
table=4,in_port=4,ip,ct_state=+trk+new,nw_dst=10.10.0.13/32,action=ct(commit),normal
table=4,in_port=4,ip,ct_state=+trk+new,nw_dst=10.10.0.11/32,action=ct(commit),set_field:0x402-
>tun_id,set_field:10.0.0.166->tun_dst,1
table=4,in_port=4,ip,nw_dst=10.10.0.13/32,ct_state=+trk+est,action=5
table=4,in_port=4,ip,nw_dst=10.10.0.11/32,ct_state=+trk+est,action=set_field:0x402->tun_id,set_field:
10.0.0.166->tun_dst,1
table=4,in_port=5,ip,ct_state=+trk+new,action=drop
table=4,in_port=5,ip,nw_dst=10.10.0.12/32,ct_state=+trk+est,action=4
table=4,in_port=1,ip,nw_dst=10.10.0.12/32,ct_state=+trk+est,action=4
```

```
sudo ovs-appctl dpctl/dump-conntrack
udp,orig=(src=10.0.0.165,dst=10.0.0.166,sport=34209,dport=4789),reply=(src=10.0.0.166,dst=10.0.0.165,spo
t=4789,dport=34209)
icmp,orig=(src=10.10.0.12,dst=10.10.0.11,id=25089),reply=(src=10.10.0.11,dst=10.10.0.12,id=25089)
udp,orig=(src=10.0.0.166,dst=10.0.0.165,sport=55335,dport=4789),reply=(src=10.0.0.165,dst=10.0.0.166,spo
t=4789,dport=55335)
```

OVS NAT


Create & Update
CT entries
Netfilter
Connection Tracker
CT
Table
Netfilter
NAT
2
conntrack()
3
nat()
1
OVS Flow Table
4
Recirculation

OVS NAT Dev Env

- OVS 2.6 and above
- Kernel 4.6.0 and above

OVS NAT Rules

```
table=0,ip,in_port=5 actions=ct(commit,zone=1,nat(src=192.168.10.103-192.168.10.115,random)),output:6
table=0,in_port=6,ct_state=-trk,ip,action=ct(table=0,zone=1,nat)
table=0,in_port=6,ct_state=+trk,ip,action=5
```

```
$sudo ovs-appctl dpctl/dump-conntrack  | grep 192
tcp,orig=(src=10.0.0.163,dst=10.0.0.162,sport=56192,dport=9876),reply=(src=10.0.0.162,dst=10.0.0.163,
sport=9876,dport=56192),protoinfo=(state=ESTABLISHED)
icmp,orig=(src=10.0.0.163,dst=192.168.10.2,id=2637,type=8,code=0),reply=(src=192.168.10.2,dst=192.168
.10.113,id=0,type=0,code=0),zone=1
icmp,orig=(src=10.0.0.163,dst=192.168.10.2,id=2637,type=8,code=0),reply=(src=192.168.10.2,dst=10.0.0.
163,id=2637,type=0,code=0)
```

OVS NAT Check

```
$ sudo tcpdump -i any icmp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on any, link-type LINUX_SLL (Linux cooked), capture size 65535 bytes
15:18:24.720686 IP onos02 > 192.168.10.2: ICMP echo request, id 2750, seq 2, length 64
15:18:24.720718 IP 192.168.10.113 > 192.168.10.2: ICMP echo request, id 0, seq 2, length 64
15:18:25.728610 IP onos02 > 192.168.10.2: ICMP echo request, id 2750, seq 3, length 64
15:18:25.728623 IP 192.168.10.113 > 192.168.10.2: ICMP echo request, id 0, seq 3, length 64
15:18:26.736648 IP onos02 > 192.168.10.2: ICMP echo request, id 2750, seq 4, length 64
15:18:26.736670 IP 192.168.10.113 > 192.168.10.2: ICMP echo request, id 0, seq 4, length 64
15:18:27.744655 IP onos02 > 192.168.10.2: ICMP echo request, id 2750, seq 5, length 64
15:18:27.744686 IP 192.168.10.113 > 192.168.10.2: ICMP echo request, id 0, seq 5, length 64
```