iproute2 and iptables packet

Neven Miculinić

University of Zagreb
Faculty of Electrical Engineering and Computing
Seminar for Computer Forensics class

neven.miculinic@fer.hr

January, 2018

Overview

1. iptables
   - Rules
   - Chains
   - Tables
2. ip route

iptables

- Rules
- Chains
- Tables

Rule

Rule

If-then constructs

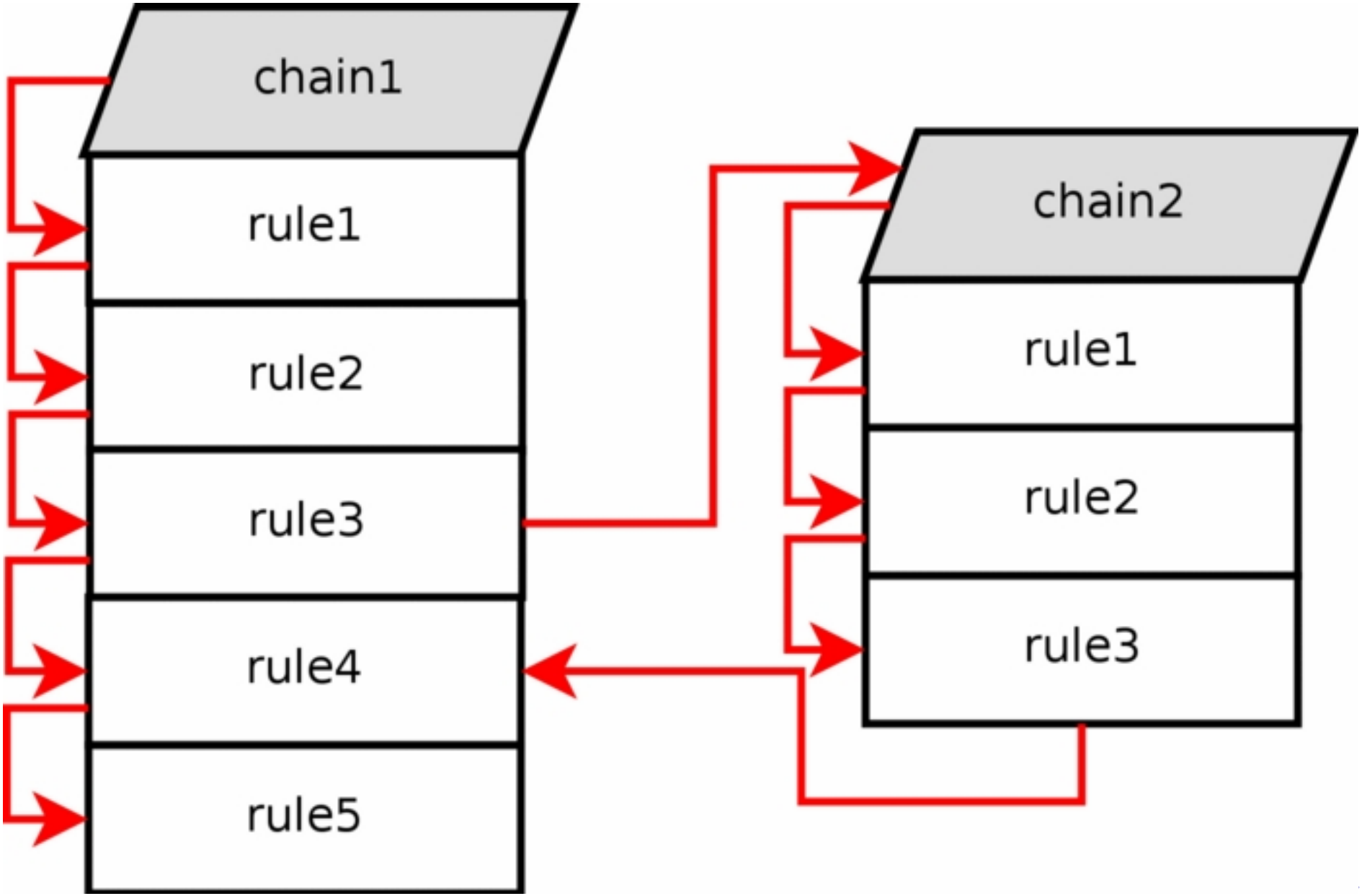
Example (Filter rule)

iptables -A INPUT -s 65.55.44.100 -j DROP

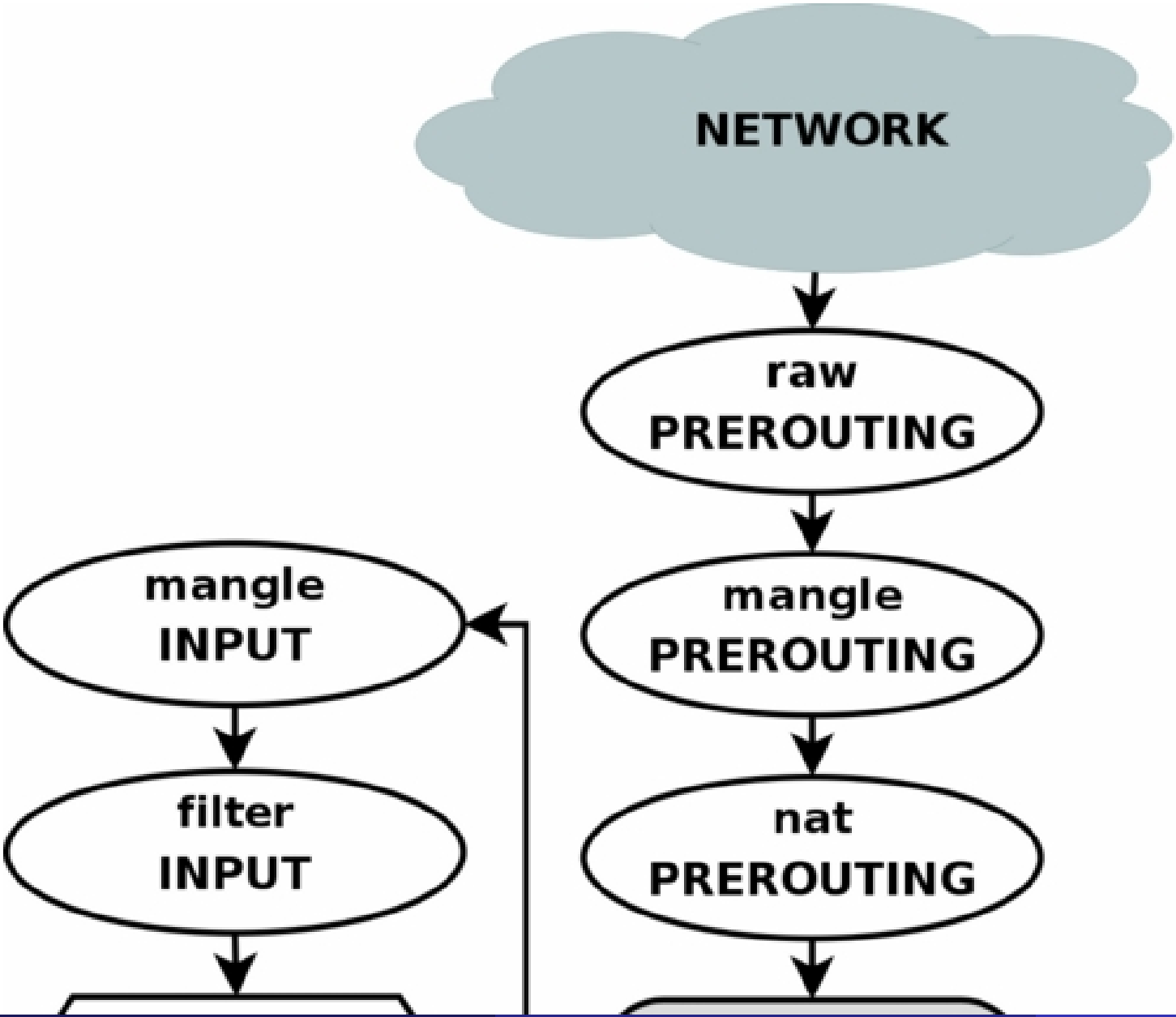
Example (NAT rule)

iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE

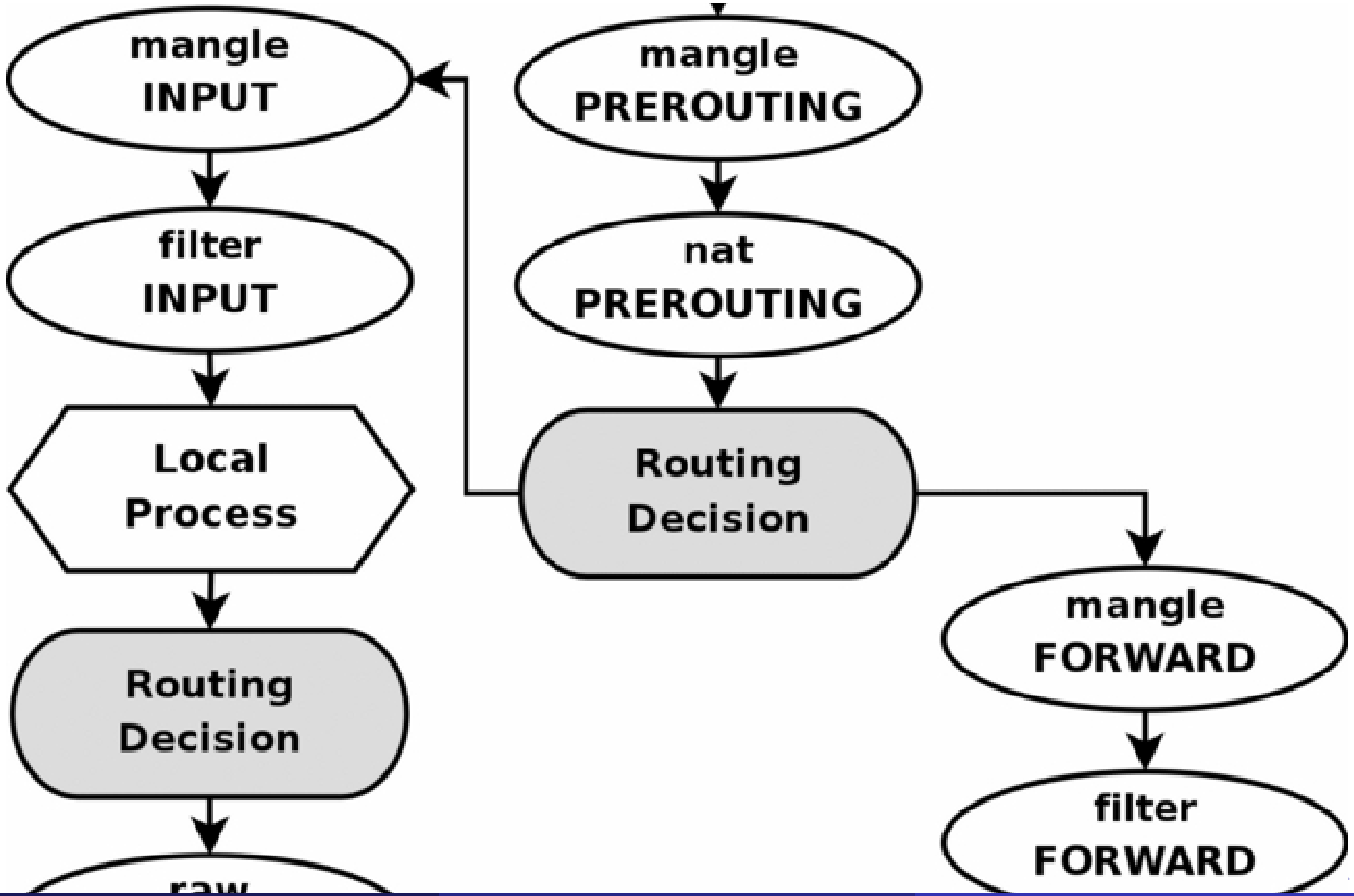
Chains


chain1
rule1
rule2
rule3
rule4
rule5
chain2
rule1
rule2
rule3

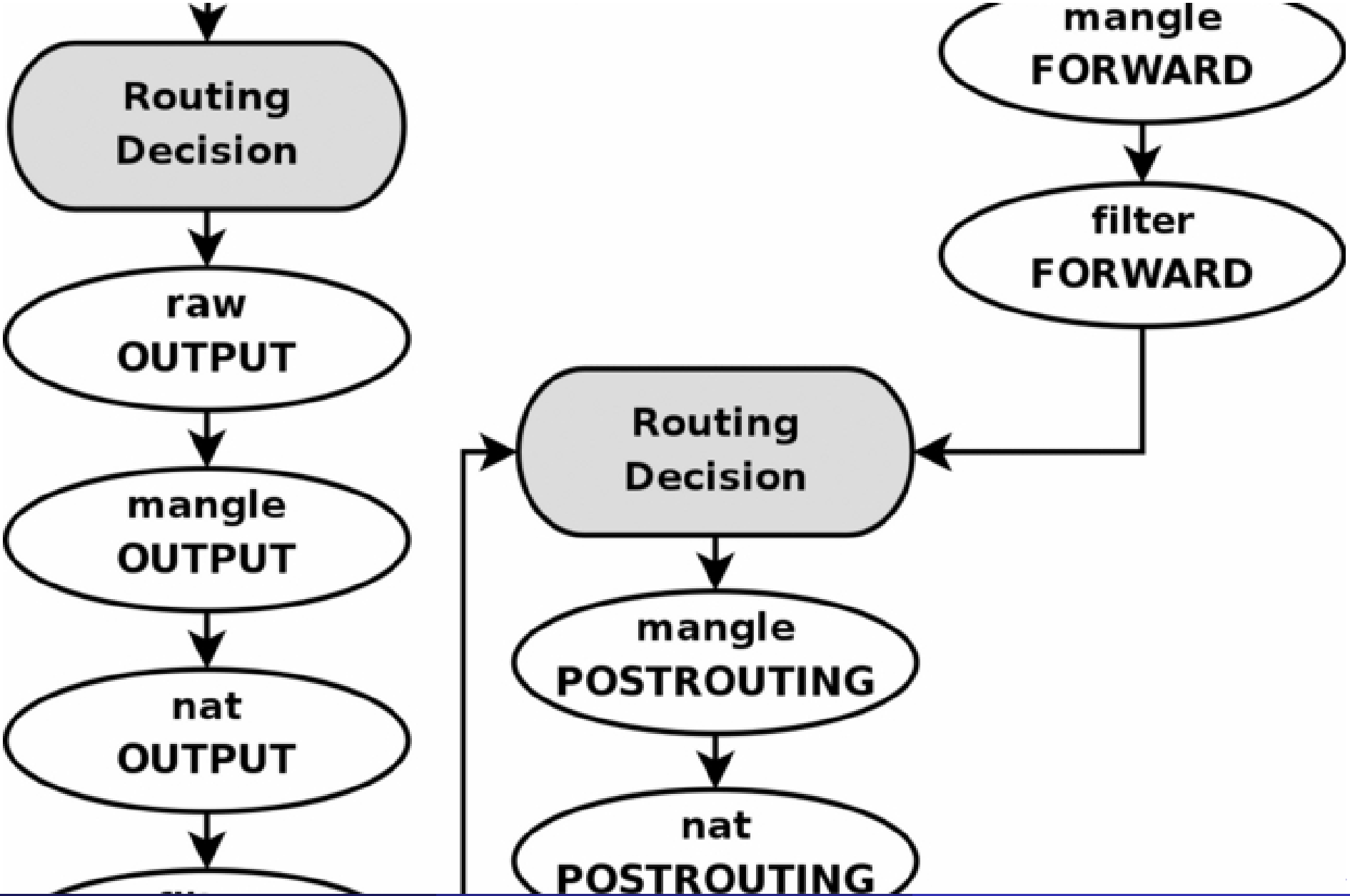
PREROUTING chains



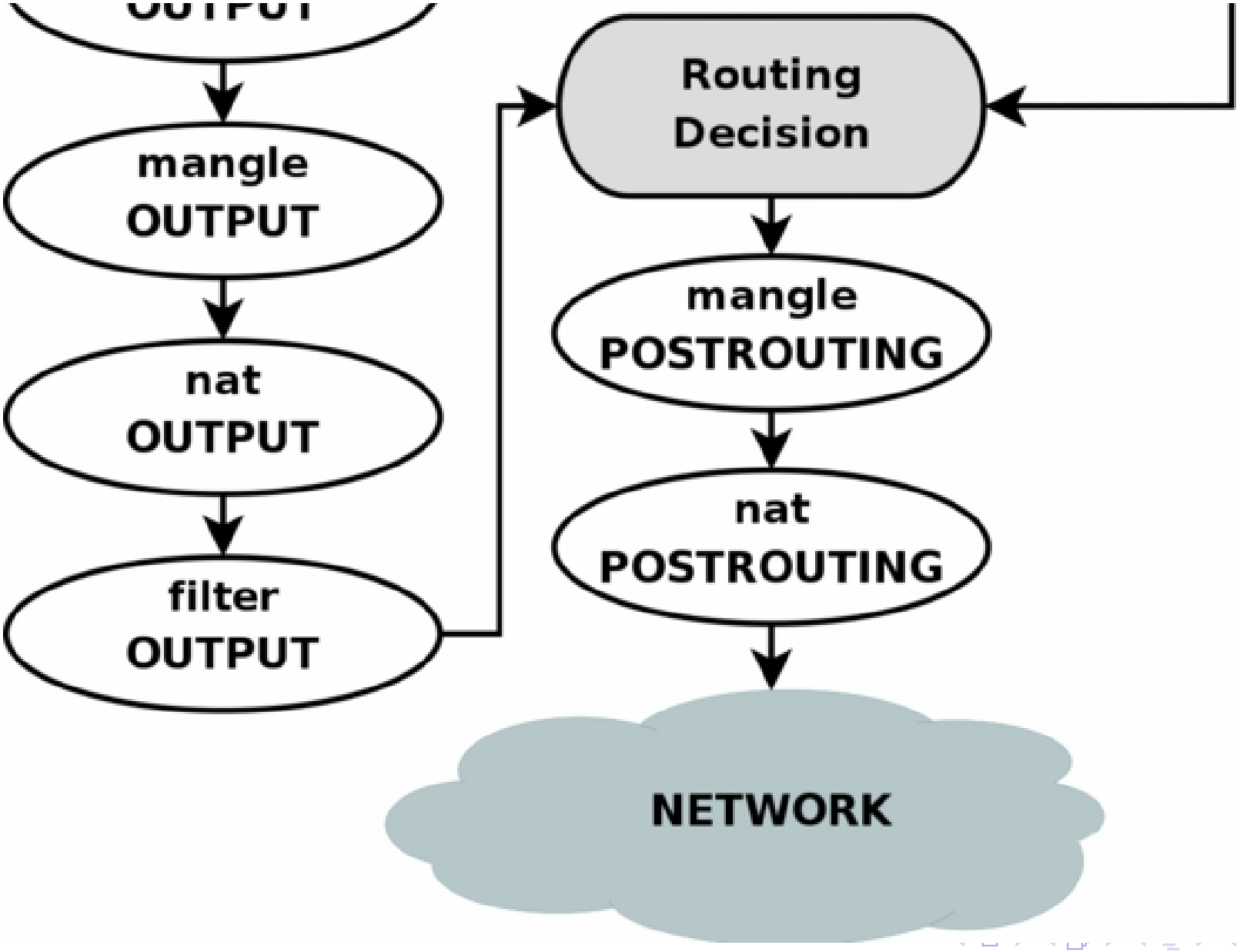
INPUT & FORWARD chains



OUTPUT chain



POSTROUTING chain



tables

- raw
- mange
- filter
- NAT
- security

ip route

ip route

Part of iproute2 package with useful routing user-space utilities

Example (Show routes)

ip route show

Example (Output)

```
default via 192.168.121.1 dev wlp1s0 proto dhcp metric 600
172.17.0.0/16 dev docker0 proto kernel scope
    link src 172.17.0.1
172.18.0.0/16 dev br-8fd3cee01eeb proto kernel scope
    link src 172.18.0.1 linkdown
192.168.121.0/24 dev wlp1s0 proto kernel scope link
    src 192.168.121.194 metric 600
```

Common ip route operations

Example (Add new route)

```
ip route add 192.0.2.0/25 dev eth0
ip route add default dev eth0
ip route add 0.0.0.0/0 dev eth0
ip route add 192.0.2.128/25 via 192.0.2.1
```

Example (Delete route)

```
ip route delete 10.0.1.0/25 via 10.0.0.1
ip route delete default dev ppp0
```

References

Netfilter

- http://www.netfilter.org/

Iptables Tutorial 1.2.2

- https://www.frozentux.net/iptables-tutorial/iptables-tutorial.html

iproute2 cheat sheet

- http://baturin.org/docs/iproute2/

iproute2 source

- https://github.com/shemminger/iproute2

The End