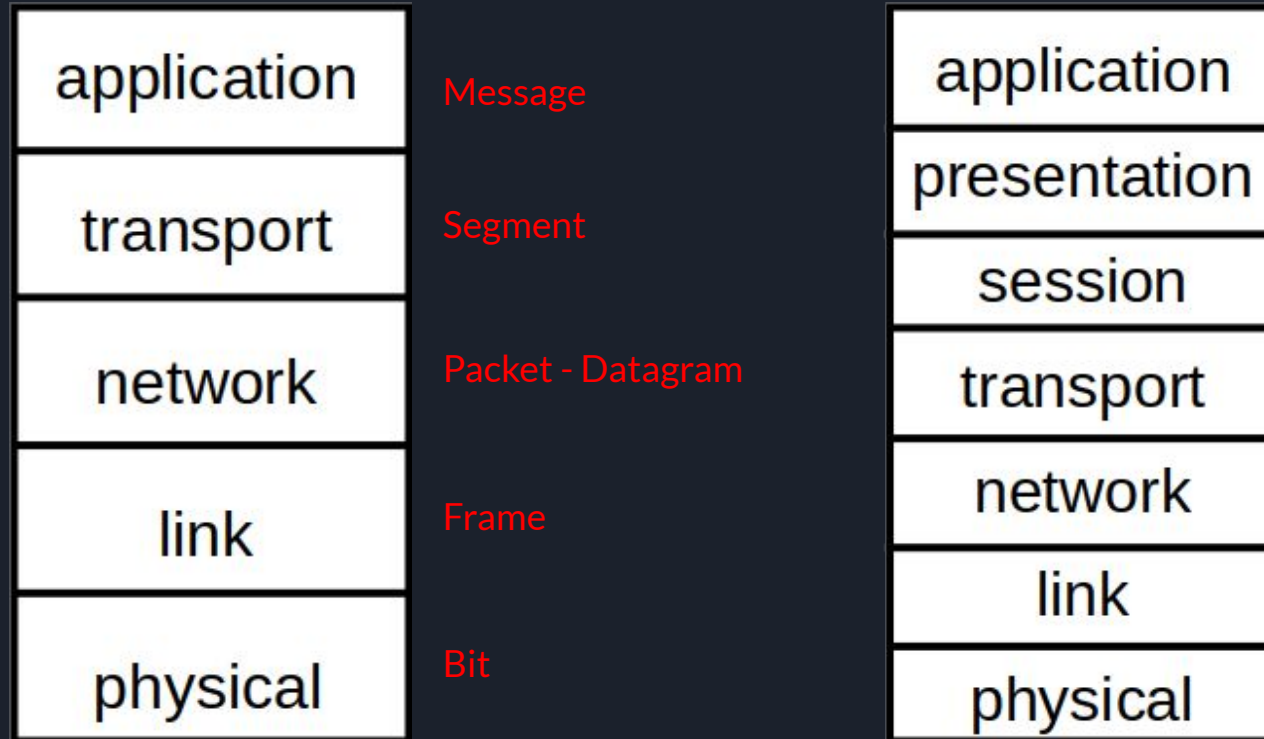




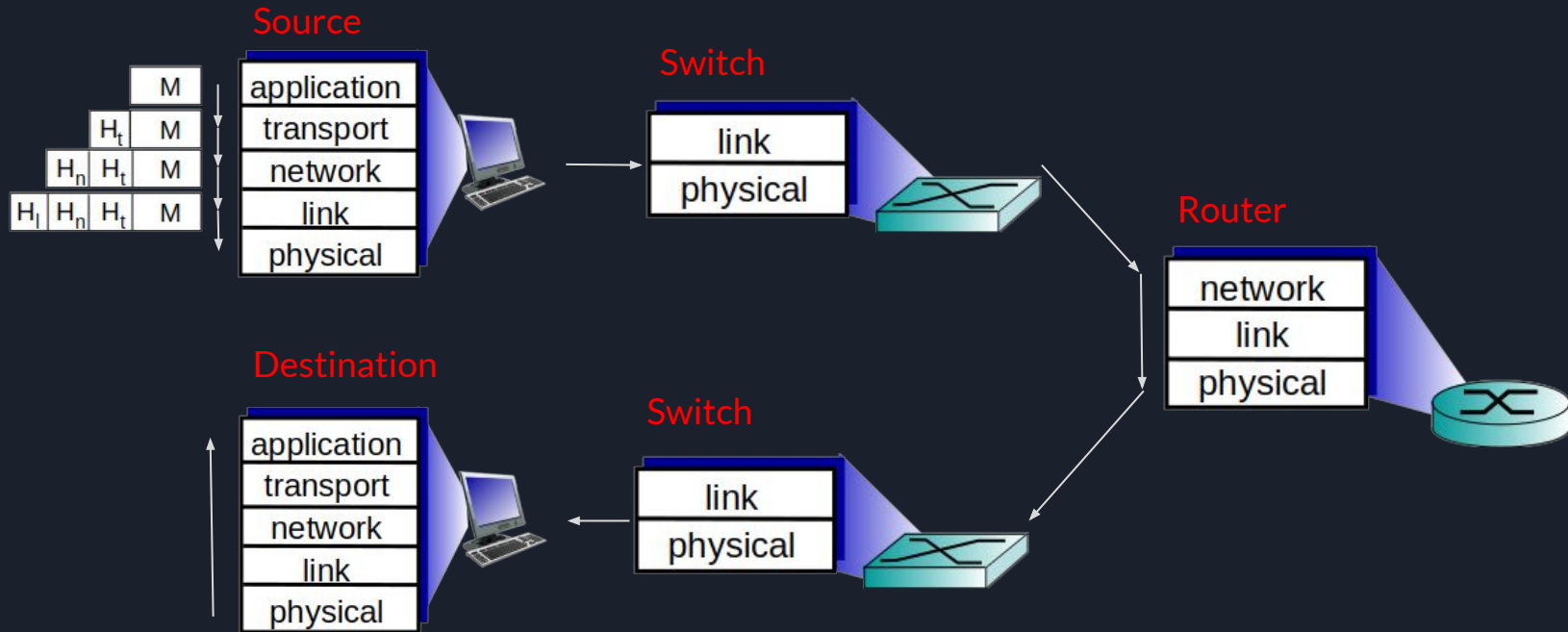
Network



A little bit of academy



A little bit of academy





Dive in to Linux

- IProute
- IPtables

IProute

iproute = arp + ifconfig + route

Let's go to terminal

```
root@Roohi-LP:~# ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
```

```
root@Roohi-LP:~# ip route
default via 192.168.0.1 dev wlo1 proto dhcp metric 600
10.0.100.0/24 dev ppp0 scope link
10.11.12.0/24 via 172.16.113.193 dev tun0
10.21.232.0/27 dev ppp0 scope link
10.22.224.8/29 dev ppp0 scope link
10.22.224.16/29 dev ppp0 scope link
10.22.232.0/28 dev ppp0 scope link
10.30.16.224/27 dev ppp0 scope link
10.168.0.0/16 dev ppp0 scope link
77.238.120.132 via 192.168.0.1 dev wlo1
169.254.0.0/16 dev wlo1 scope link metric 1000
169.254.2.1 dev ppp0 proto kernel scope link src 10.20.17.118
172.16.0.0/12 dev ppp0 scope link
172.16.10.0/24 via 172.16.113.193 dev tun0
172.16.113.0/24 via 172.16.113.193 dev tun0
172.16.113.193 dev tun0 proto kernel scope link src 172.16.113.194
172.17.0.0/16 dev docker0 proto kernel scope link src 172.17.0.1 linkdown
172.30.90.2 dev ppp0 scope link
172.31.0.0/20 via 172.16.113.193 dev tun0
192.168.0.0/20 dev wlo1 proto kernel scope link src 192.168.0.97 metric 600
192.168.60.122 dev ppp0 scope link
192.168.60.141 dev ppp0 scope link
192.168.60.230 dev ppp0 scope link
```

```
root@Roohi-LP:~#
```

```
root@Roohi-LP:~# ifconfig
docker0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    inet 172.17.0.1 netmask 255.255.0.0 broadcast 172.17.255.255
```

```
root@Roohi-LP:~# route -n
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
0.0.0.0 192.168.0.1 0.0.0.0 UG 600 0 0 wlo1
10.0.100.0 0.0.0.0 255.255.255.0 U 0 0 0 ppp0
10.11.12.0 172.16.113.193 255.255.255.0 UG 0 0 0 tun0
10.21.232.0 0.0.0.0 255.255.255.224 U 0 0 0 ppp0
10.22.224.8 0.0.0.0 255.255.255.248 U 0 0 0 ppp0
10.22.224.16 0.0.0.0 255.255.255.248 U 0 0 0 ppp0
10.22.232.0 0.0.0.0 255.255.255.240 U 0 0 0 ppp0
10.30.16.224 0.0.0.0 255.255.255.224 U 0 0 0 ppp0
192.168.0.0 0.0.0.0 255.255.0.0 U 0 0 0 ppp0
172.16.0.0 0.0.0.0 255.0.0.0 U 1000 0 0 wlo1
172.16.10.0 172.16.113.193 255.255.255.0 UH 0 0 0 ppp0
172.16.113.0 0.0.0.0 255.240.0.0 U 0 0 0 ppp0
172.16.113.193 172.16.113.193 255.255.255.0 UG 0 0 0 tun0
172.16.113.193 0.0.0.0 255.255.255.255 UH 0 0 0 tun0
172.17.0.0 0.0.0.0 255.255.0.0 U 0 0 0 docker0
172.30.90.2 0.0.0.0 255.255.255.255 UH 0 0 0 ppp0
172.31.0.0 172.16.113.193 255.255.240.0 UG 0 0 0 tun0
192.168.0.0 0.0.0.0 255.255.240.0 U 600 0 0 wlo1
192.168.60.122 0.0.0.0 255.255.255.255 UH 0 0 0 ppp0
192.168.60.141 0.0.0.0 255.255.255.255 UH 0 0 0 ppp0
192.168.60.230 0.0.0.0 255.255.255.255 UH 0 0 0 ppp0
```

```
root@Roohi-LP:~#
```

```
inet 172.16.113.194 netmask 255.255.255.255 destination 172.16.113.193
    inet fe80::e81:f04e:1ad0:a1ad prefixlen 64 scopeid 0x20<link>
    unspec 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00 txqueuelen 500 (UNSPEC)
    RX packets 19424 bytes 9213560 (9.2 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 9313 bytes 1384027 (1.3 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

wlo1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.0.97 netmask 255.255.240.0 broadcast 192.168.15.255
    inet6 fe80::f795:6161:5604:2f36 prefixlen 64 scopeid 0x20<link>
    ether 8c:00:7e:25:c2:e5 txqueuelen 1000 (Ethernet)
    RX packets 393816B bytes 1275297747 (1.2 GB)
    RX errors 0 dropped 106 overruns 0 frame 0
    TX packets 481842 bytes 224099426 (224.0 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
root@Roohi-LP:~#
```



IPtables

Organized into:

- Tables
- Chains
- Targets

Table 1:

- Chain 1:
 - Rule 1 → Target 1
 - Rule 2 → Target 2
- Chain 2:
 - Rule 1 → Target 1
 - Rule 2 → Target 2
- ...

Table 2:

- Chain 1:
 - Rule 1 → Target 1
 - Rule 2 → Target 2
- Chain 2:
 - Rule 1 → Target 1
 - Rule 2 → Target 2
- ...

Table n:

- Chain 1:
 - Rule 1 → Target 1
 - Rule 2 → Target 2
- Chain 2:
 - Rule 1 → Target 1
 - Rule 2 → Target 2
- ...



IPtables

Chains:

- Each of these tables are composed of a few default chains
- These chains allow you to filter packets at various points
 - PREROUTING
 - INPUT
 - OUTPUT
 - FORWARD
 - POSTROUTING

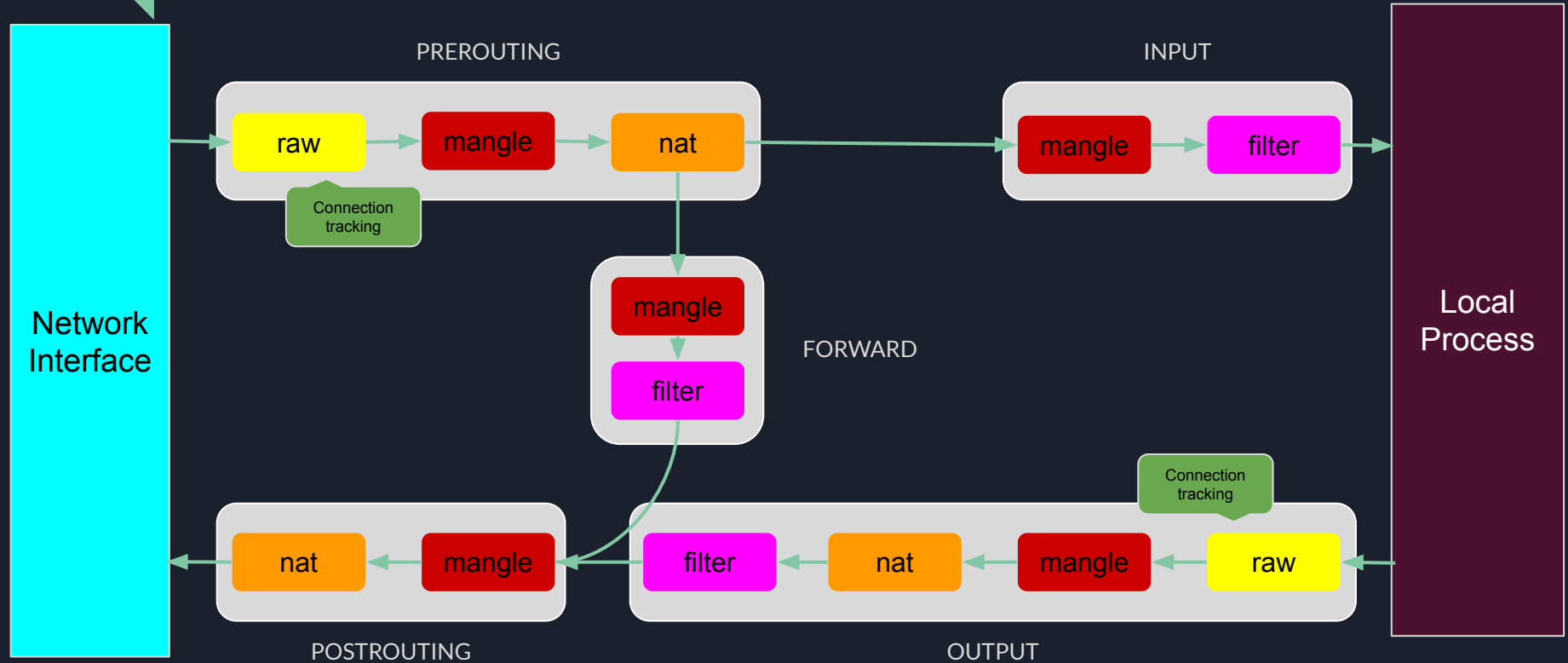


IPtables

Tables:

- A table is something that allows you to process packets in specific ways
- The default table is the filter table, although there are other tables too:
 - Filter
 - Nat
 - Mangle
 - Raw
 - Some kernels: Security → SELinux

IPtables





IPtables

Targets:

- Default policy
 - For each chain
 - Defined as a target
- Types of targets:
 - Terminating
 - ACCEPT
 - DROP
 - REJECT
 - Non-Terminating
 - LOG

Let's go to terminal

Useful Network Command

- mtr
- nc
- conntrack

```
My traceroute [v0.95]
Roohi-LP (192.168.100.129) -> google.com (142.250.201.142) 2023-06-01T08:26:06+0330
Keys: Help Display mode Restart statistics Order of fields quit

          Packets
Host      Loss%  Snt   Last  Avg  Best  Wrst StDev
1. _gateway 0.0%   19    1.0    1.0   0.8    1.3   0.1
2. 2.177.128.1 0.0%   18    2.8    3.4   2.8    6.3   0.8
3. 93.118.125.41 33.3%  18    3.8    5.4   3.6   19.7   4.6
4. 10.22.27.41 41.2%  18    3.6    4.9   3.2   12.7   3.2
5. 5.239.247.25 70.6%  18    6.6    5.4   3.6    9.0   2.4
6. 10.21.252.18 88.2%  18    3.3    3.3   3.2    3.3   0.1
7. 10.202.7.102 0.0%   18    3.9    3.8   3.5    4.3   0.2
8. 10.21.21.10 0.0%   18    3.7    3.9   3.6    4.8   0.3
9. 134.0.220.188 76.5%  18   38.5   38.5  36.9   40.0   1.3
10. 213.202.5.239 94.1%  18   40.3   40.3  40.3   40.3   0.0
11. 216.239.48.87 0.0%   18   38.0   38.4  38.0   39.0   0.3
12. 74.125.253.75 0.0%   18   35.6   36.6  35.6   48.8   3.0
13. mct01s21-in-f14.1e100.net 0.0%   18   38.0   38.3  37.9   39.2   0.3
```

```
roohi@Roohi-LP:~$ conntrack
Command 'conntrack' not found, but can be installed with:
sudo apt install conntrack
roohi@Roohi-LP:~$ mtr -P 443 google.com
roohi@Roohi-LP:~$ nc -vz google.com 443
Connection to google.com (142.250.201.142) 443 port [tcp/https] succeeded!
roohi@Roohi-LP:~$ conntrack -d 8.8.8.8 -E
mnl_socket_bind: Operation not permitted
conntrack v1.4.6 (conntrack-tools): Can't open netlink socket
roohi@Roohi-LP:~$ sudo !!
sudo conntrack -d 8.8.8.8 -E
[sudo] password for roohi:
[NEW] icmp      1 30 src=192.168.100.129 dst=8.8.8.8 type=8 code=0 id=2 [UNREPLIED] src=8.8.8.8 dst=192.168.100.129 type=0 code=0 id=2
[UPDATE] icmp   1 30 src=192.168.100.129 dst=8.8.8.8 type=8 code=0 id=2 src=8.8.8.8 dst=192.168.100.129 type=0 code=0 id=2
```