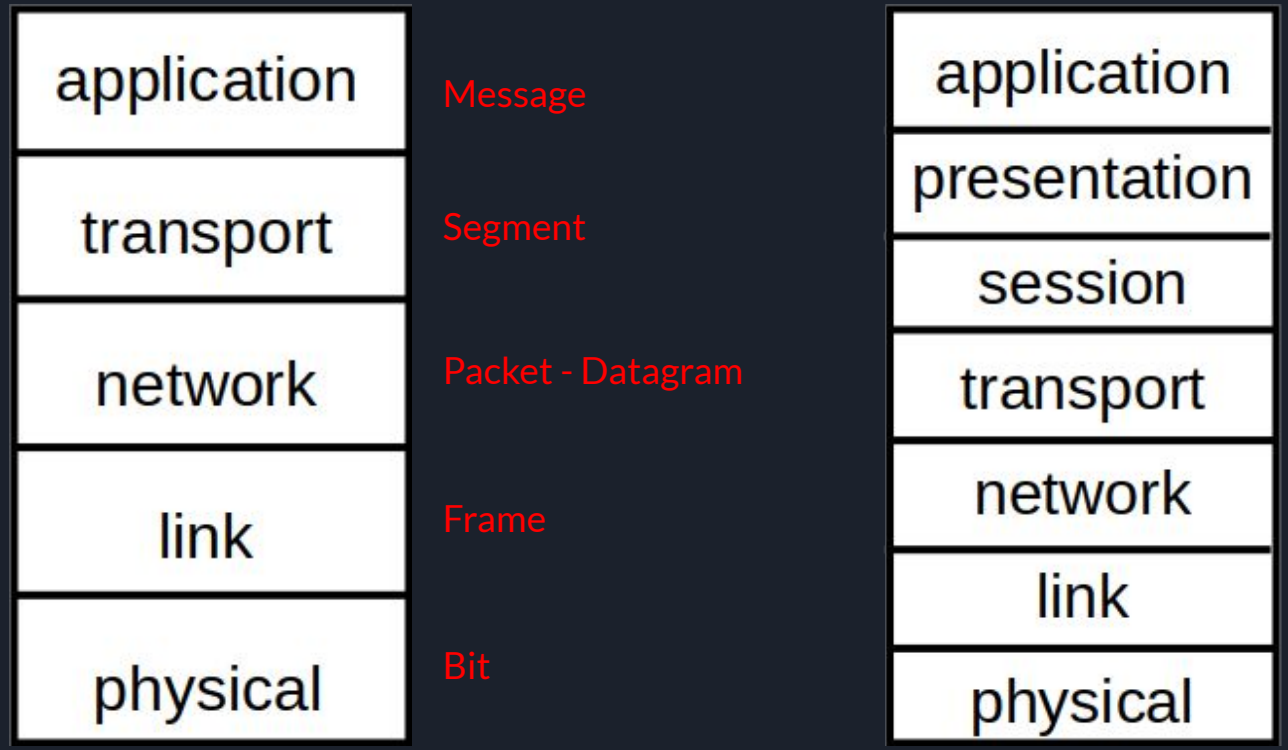
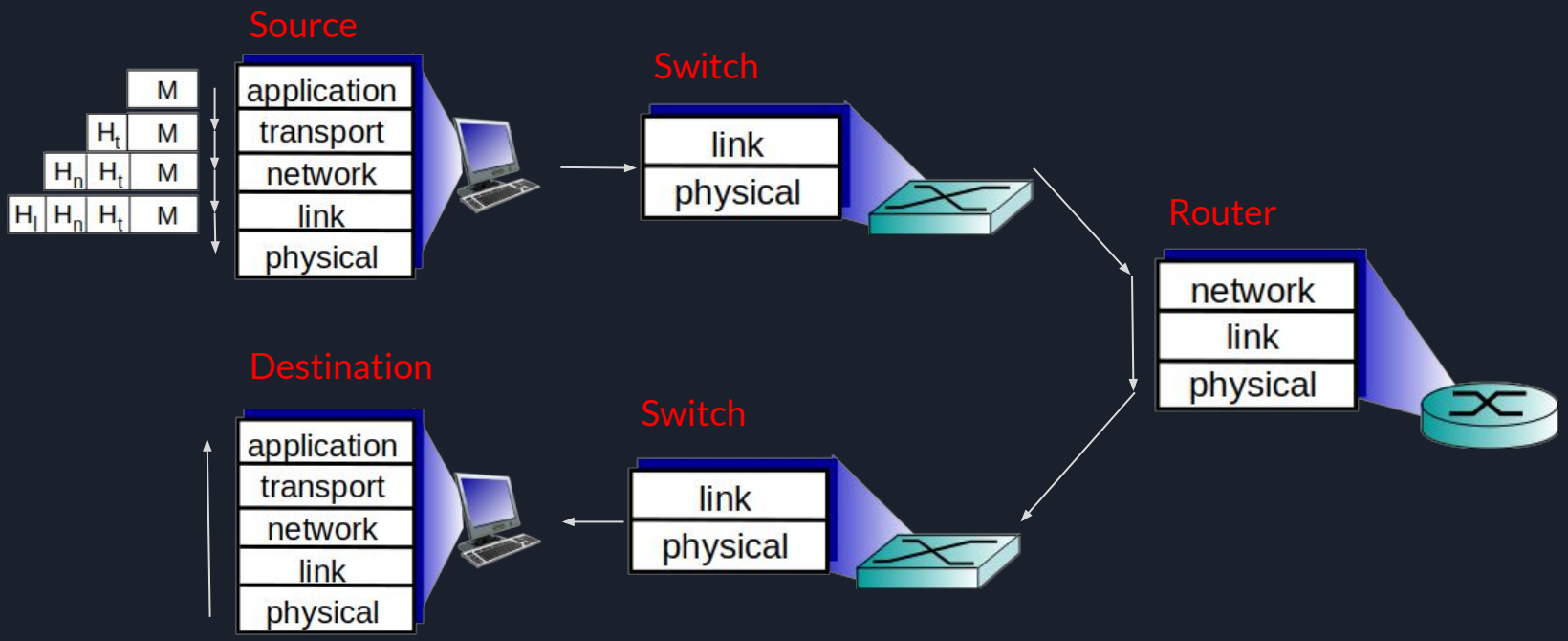
Network

A little bit of academy



A little bit of academy

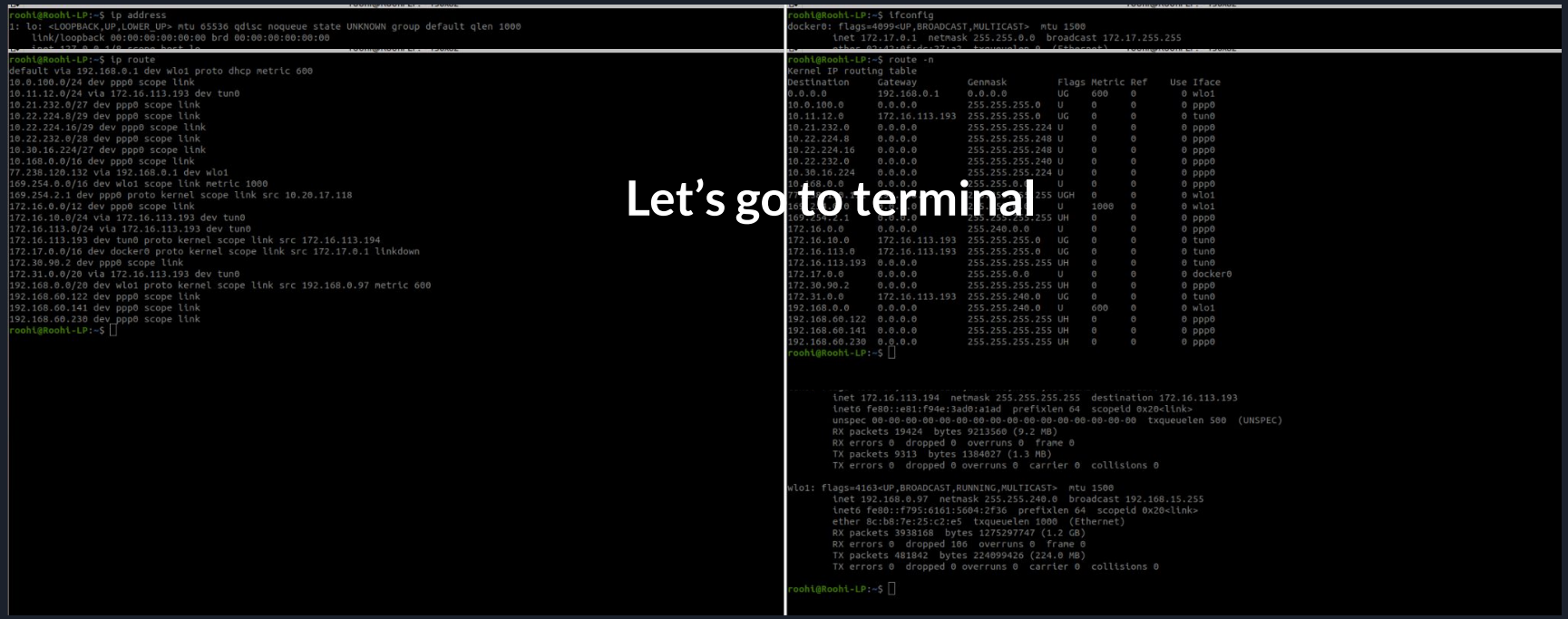


Dive in to Linux

- IProute
- IPtables

IProute

iproute = arp + ifconfig + route



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:

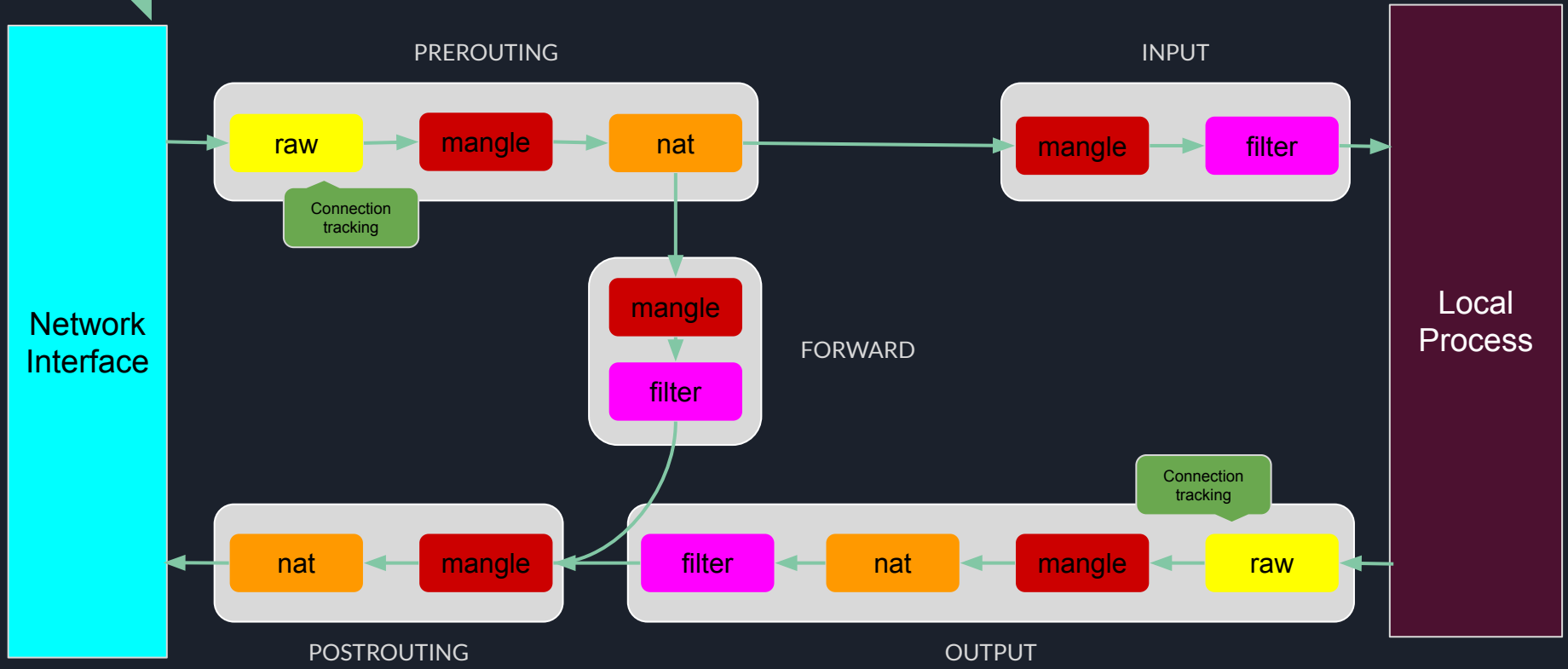
- Each of these tables are composed of a few default chains
- These chains allow you to filter packets at various points
  - PREROUTING
  - INPUT
  - OUTPUT
  - FORWARD
  - POSTROUTING

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


Network Interface
PREROUTING
raw
mangle
nat
Connection tracking
INPUT
mangle
filter
Local Process
mangle
filter
FORWARD
Connection tracking
nat
mangle
filter
nat
mangle
raw
POSTROUTING
OUTPUT

IPtables

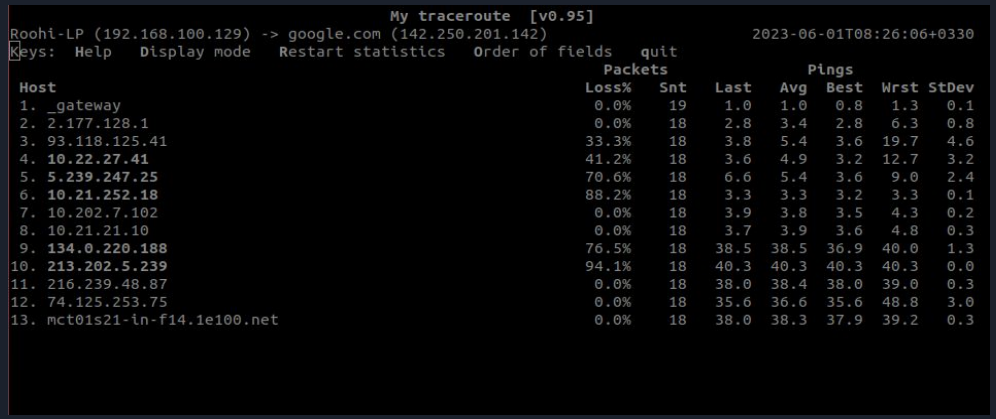
Targets:

- 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




```
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
```