FSI
LEI

2025/2026

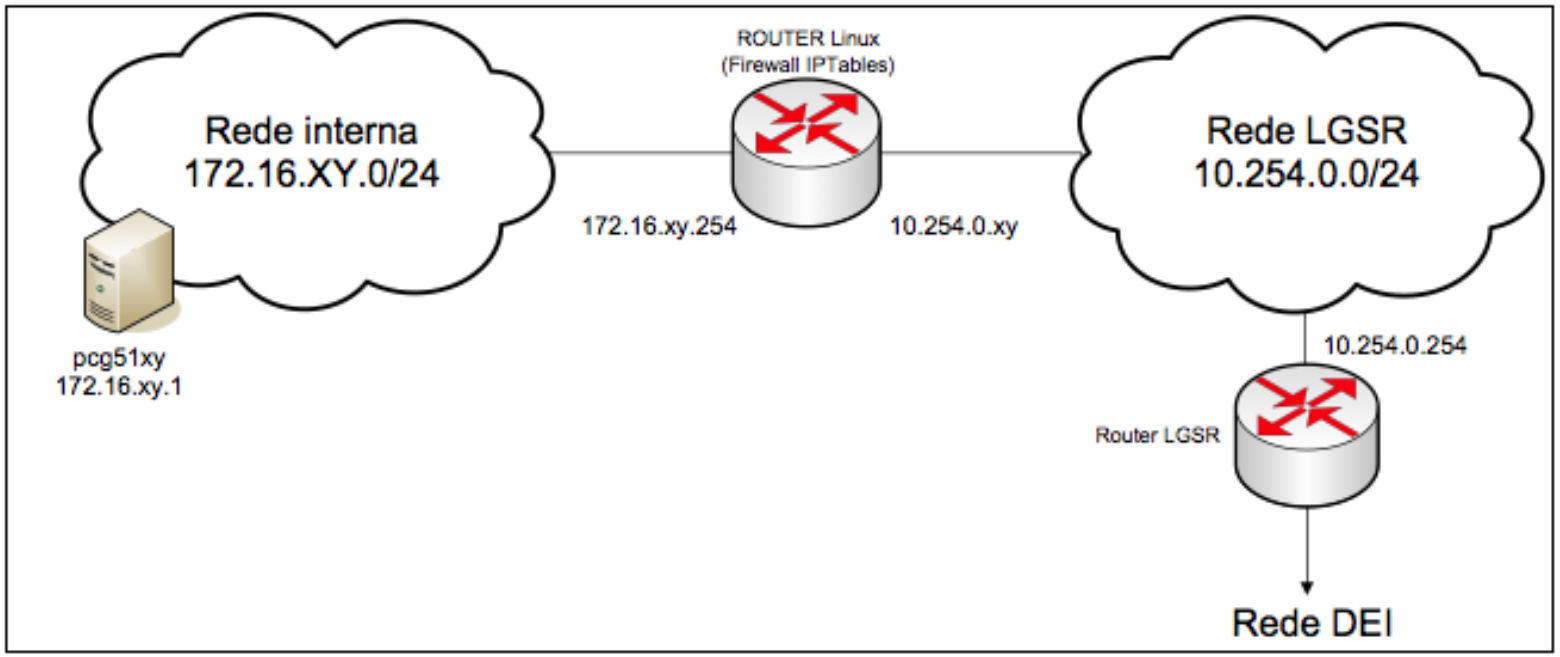
Practical class #3

- Network packet filtering and NAT with IPTables

IPTables

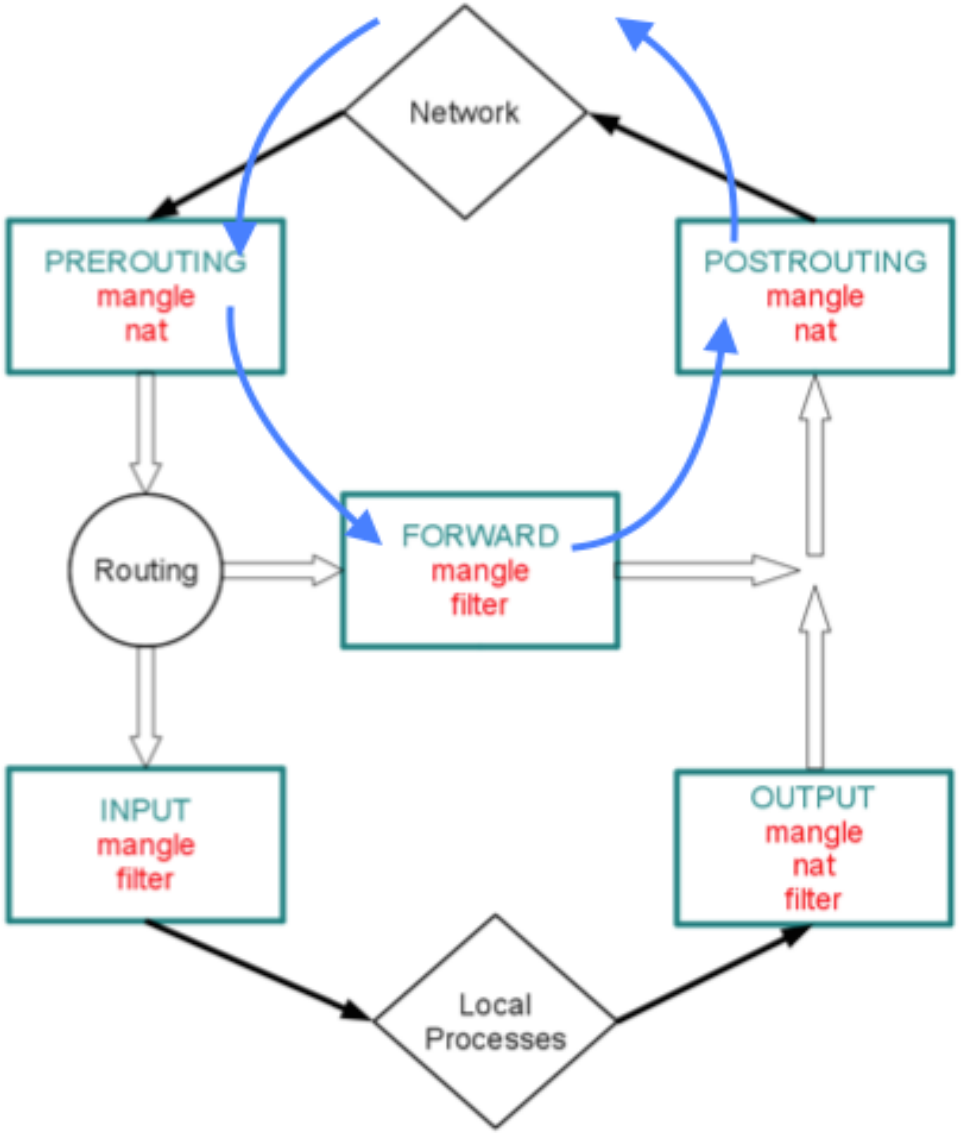
Linux as a router and network firewall:

- Packet filtering between different IP networks
- Network Address Translation (SNAT, Masquerading, DNAT, REDIRECT, …)



IPTables

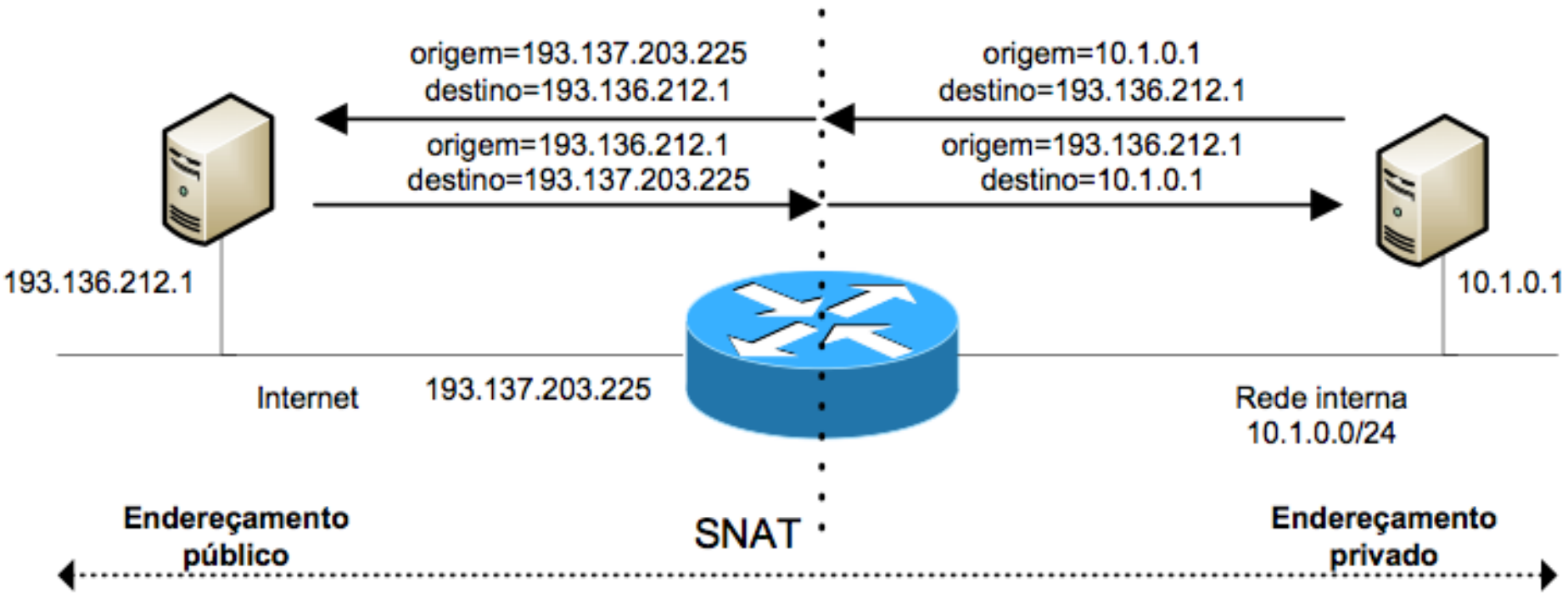
filter, **nat** and **mangle** tables:



https://cs.senecac.on.ca/~michal.heidenreich/ops335/journal.shtml

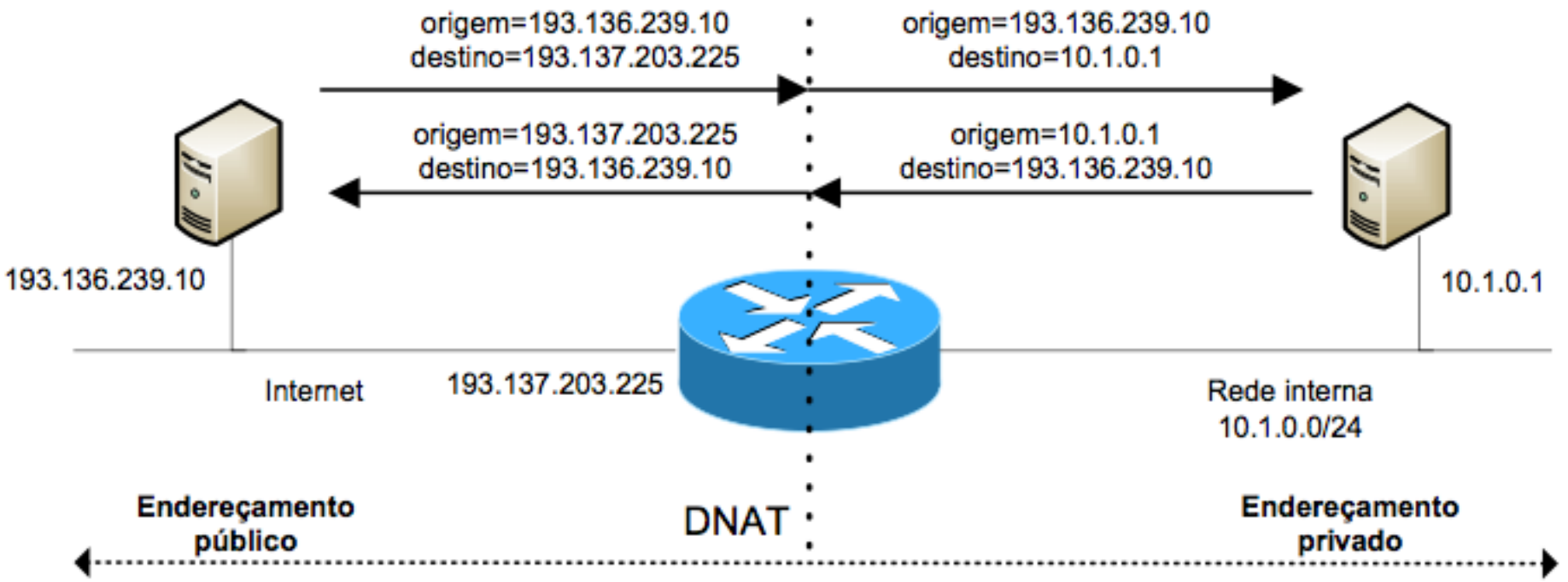
NAT (SNAT)

iptables -t nat -A POSTROUTING -s 10.1.0.0/24 -d 193.136.212.1 -j SNAT --to-source 193.137.203.225

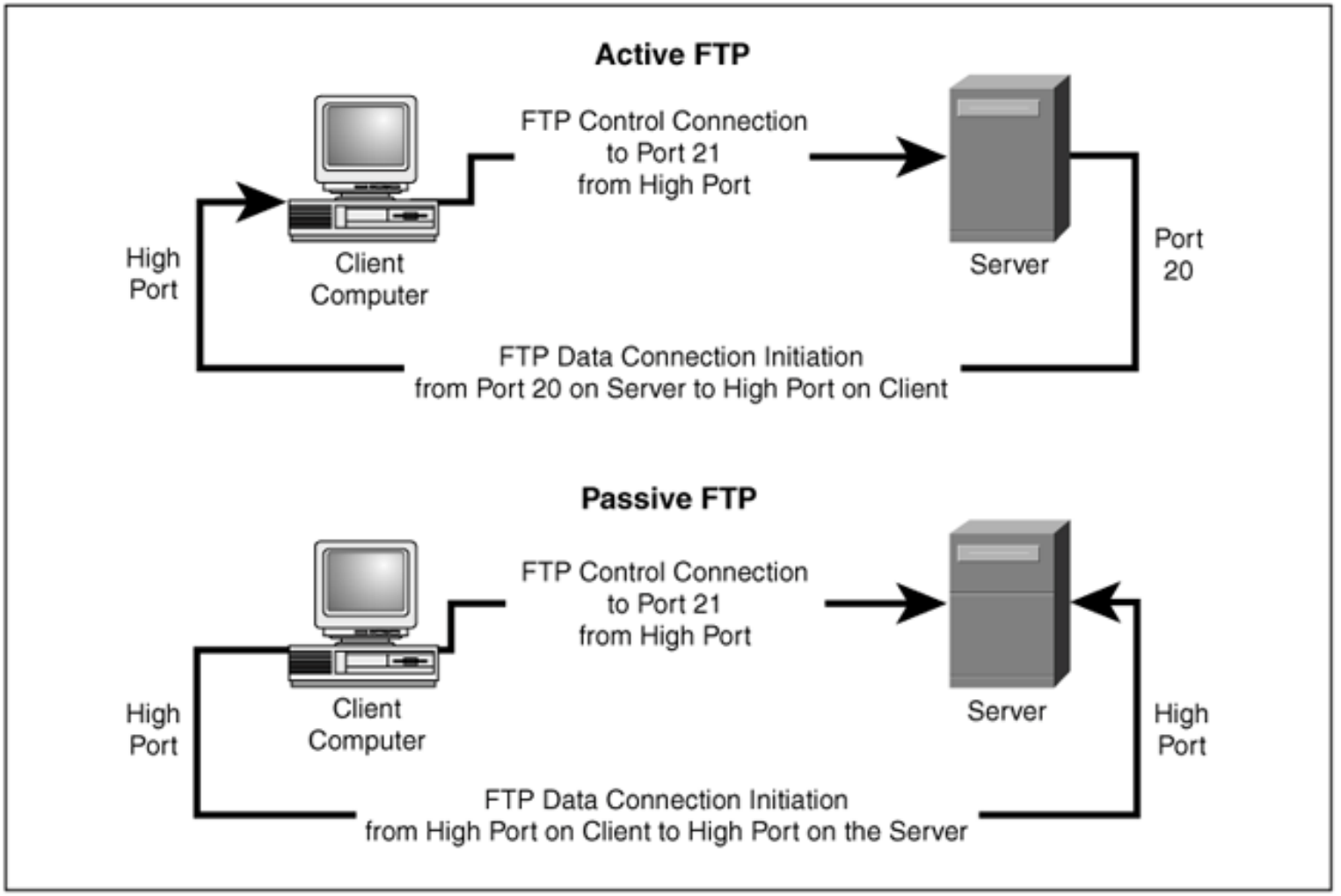


NAT (DNAT)

iptables -t nat -A PREROUTING -s 193.136.239.10 -d 193.137.203.225 -j DNAT --to-destination 10.1.0.1

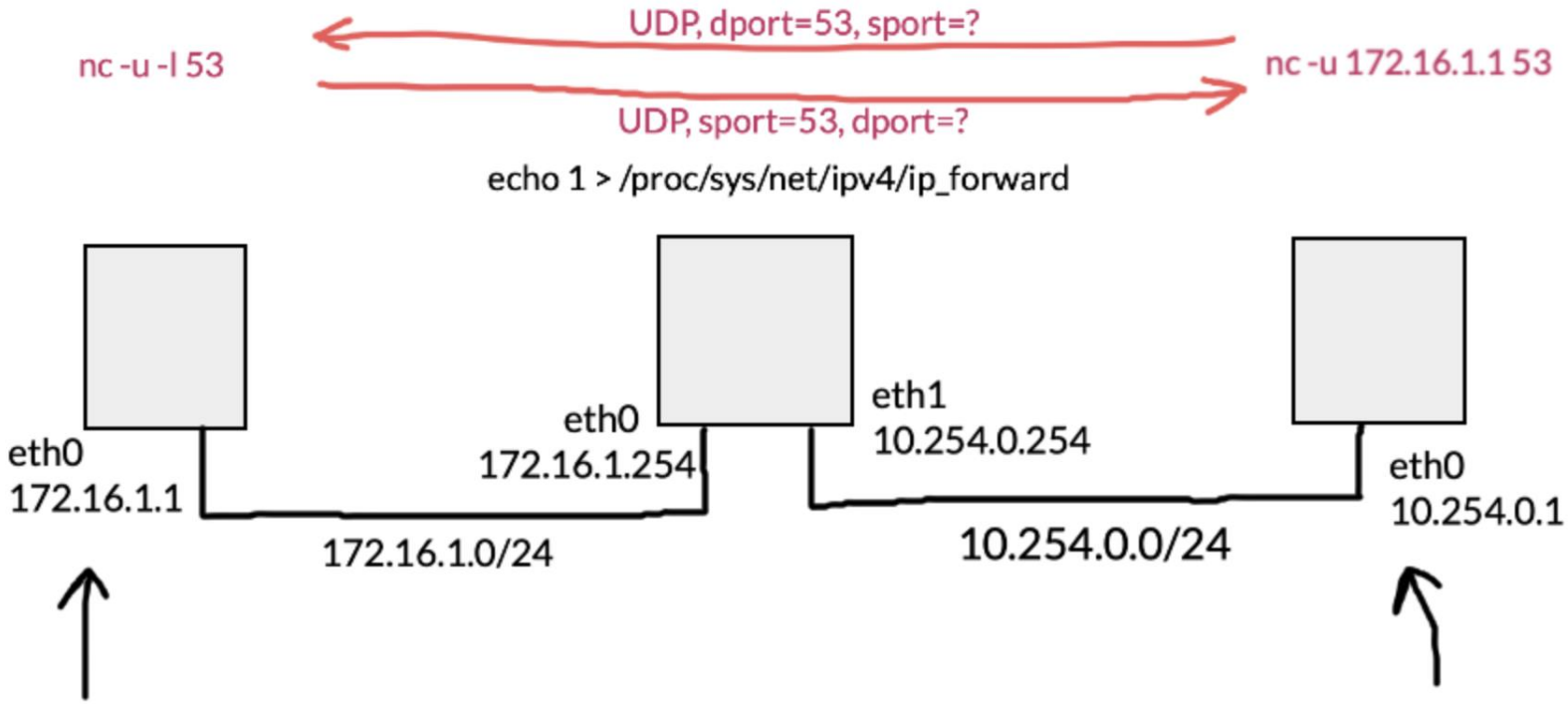


FTP (Active and Passive modes)



http://codeidol.com/unix/linux-fix/Linux-FTP-Server-Setup/FTP-Overview/

Experimental scenario (example)



route add -net 10.254.0.0/24 gw 172.16.1.254
ou
route add default gw 172.16.1.254

route add -net 172.16.1.0/24 gw 10.254.0.254
ou
route add default gw 10.254.0.254