Számítógépes Hálózatok GY – 8.hét

Laki Sándor
ELTE-Ericsson Kommunikációs Hálózatok Laboratórium
ELTE IK - Információs Rendszerek Tanszék
lakis@elte.hu
http://lakis.web.elte.hu

Teszt – 10 kérdés 10 perc

canvas.elte.hu

Kód:

Mininet – Hálózati linkek tulajdonságai

Link csomagvesztéssel

Hálózati linkek tulajdonságai:

késleltetés (delay), csomagvesztés (loss), sávszélesség (bw)

A mininetes python scriptben:

```
linkopts = {'bw':10, 'delay':'5ms’, loss=10 }
        # bw: sávszélesség Mbps-ben
        # delay: késleltetés mértékegységgel: ms, s, us, stb.
        # loss: 0-100 közötti egész, csomagvesztés százalék
net.addLink(h1, r1, cls=TCLink, **linkopts)
```

IP címek interfészekhez rendelése

Interfészek lekérdezése

```
# ifconfig
```

IP cím interfészhez rendelése

```
# ip addr add 10.0.2.1/24 dev h1-eth0
```

vagy (régebben):

```
# ifconfig h1-eth0 10.0.2.1 netmask 255.255.255.0
```

Routing tábla

Routing tábla lekérdezése

```
# route -n
```

Default route bejegyzés hozzáadása

```
# ip route add default via 10.0.2.254
```

Routing táblabejegyzés a 10.10.0.0/16 felé

```
# ip route add 10.10.0.0/16 via 10.10.254.254
```

Routing táblabejegyzés törlése

```
# ip route del 10.10.0.0/16
```

1. Feladat

A) Vizsgáljuk meg, hogy miként hat a csomagvesztés és késleltetés a TCP alapú számológép programra, amit csináltunk.

B) Nézzük meg, hogy a gyakorlat anyagai (udp-socket-stream) között elérhető UDP alapú video streamelő alkalmazásokra milyen hatással van a késleltetés és a csomagvesztés.

2. Feladat – SSH tunnel

- Számológép szerver elérése localhostra bindolva távolról ssh tunnellel
- SSH deamon indítása egy hoszton (mininet hoszton)

```
# /usr/sbin/sshd
```

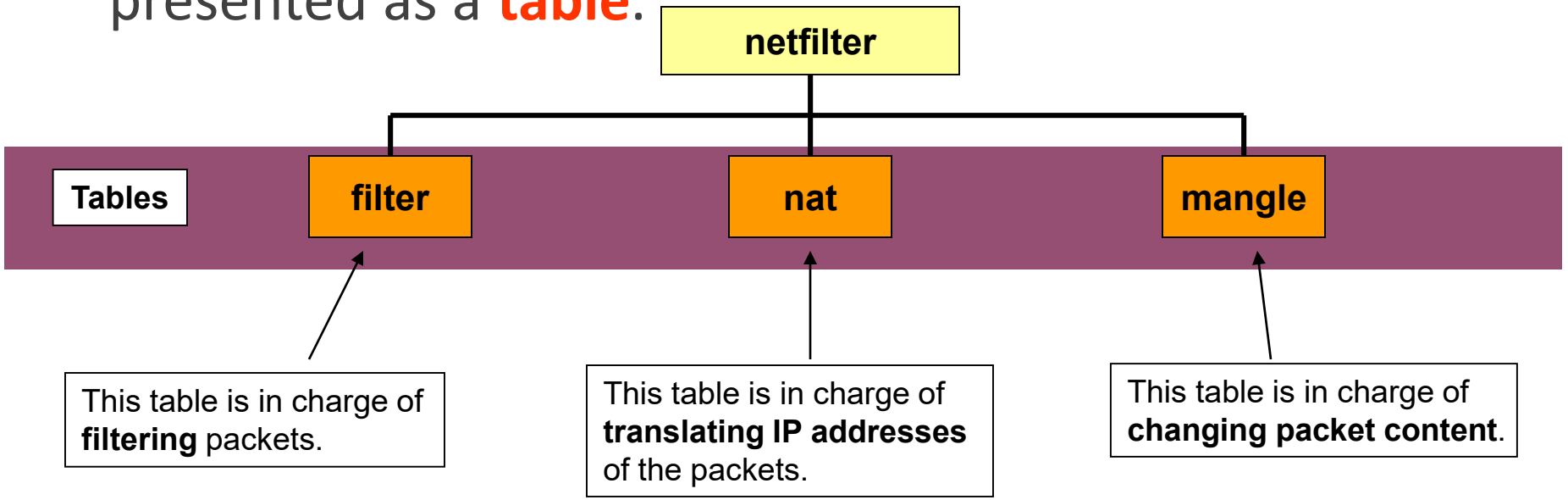
- SSH tunnel kihúzása:

```
# ssh -L 80:intra.example.com:80 gw.example.com
```

- ssh –L <localport>:<remote host>:<remote port> <gateway you can ssh in>
  - localport: a localhost ezen porján lesz elérhető a távoli szerver/szolgáltatás
  - remote host:remote port: ide csatlakozik a tunnel végpont, minden, amit a localportra küldünk ide fog továbbítódni és vissza. A gateway-ről elérhetőnek kell lennie!
  - gateway: a gép, amire be tudunk sshval lépni!

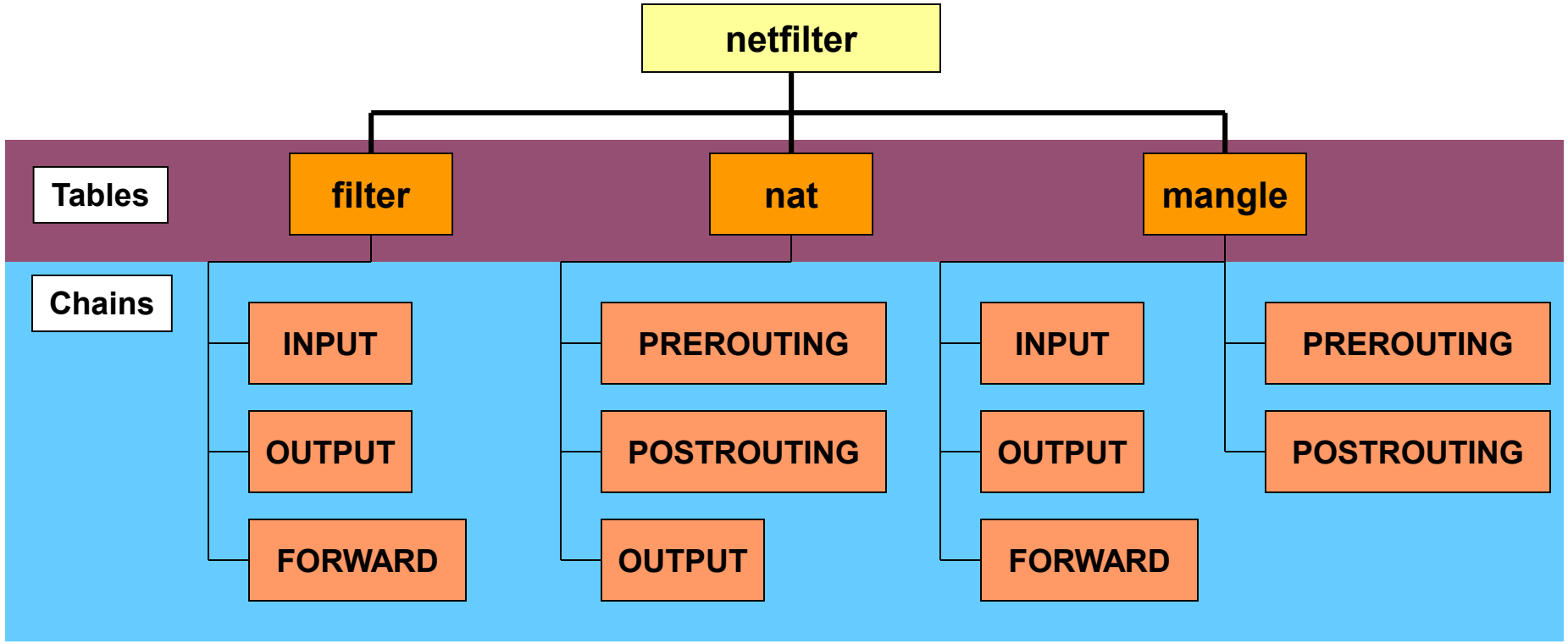
iptables – Tables and Chains

- Each function provided by the netfilter architecture is presented as a **table**.

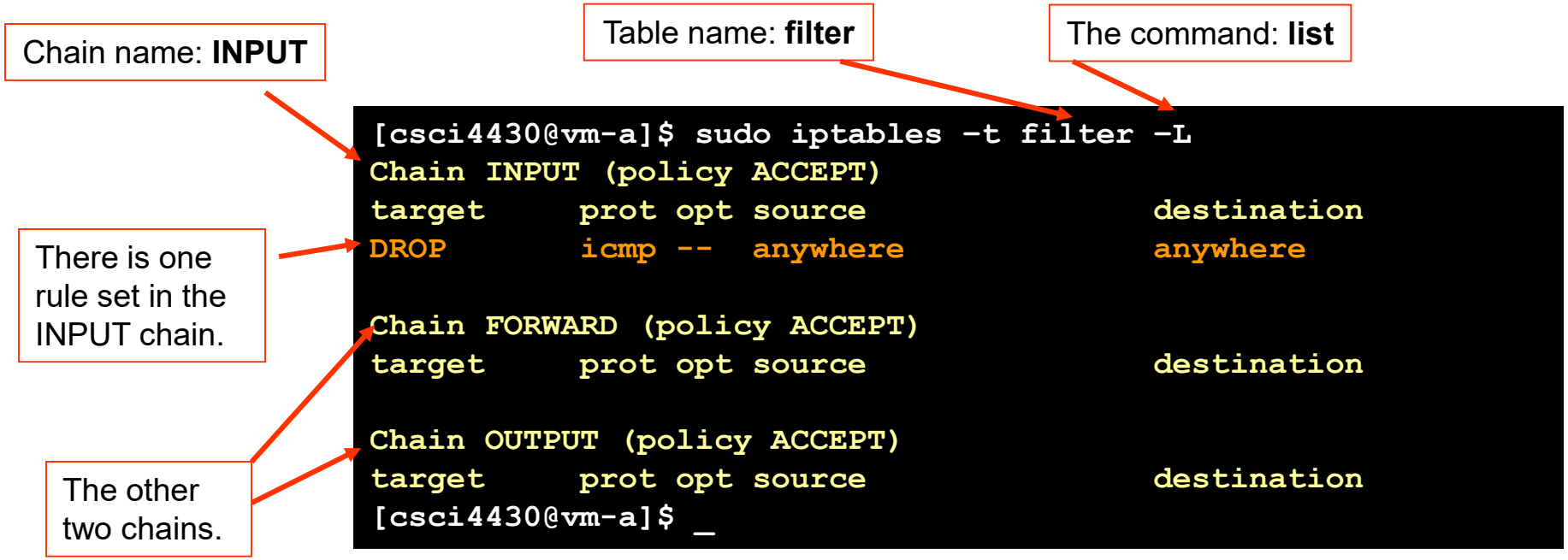


iptables – Tables and Chains

- Under each table, there are a set of **chains**.
  - Under each chain, you can assign a set of **rules**.



iptables – Tables and Chains



The rule in the INPUT chain means:

When a packet with ICMP payload passes through the **INPUT hook**, **DROP** that packets, no matter it is **from anywhere** and **to anywhere**.

iptables – Tables and Chains

```
[csci4430@vm-a]$ sudo iptables -t filter -A INPUT --protocol icmp --jump DROP
[csci4430@vm-a]$ sudo iptables -t filter -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       icmp --  anywhere             anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
[csci4430@vm-a]$ _
```

This entry shows that a new rule is added to the INPUT chain of the filter table successfully.

Add a new rule to the INPUT chain.

The **protocol** of the packets in which this rule is interested is **ICMP**.

If a packet
(1) passes through the INPUT hook, and
(2) is an ICMP packet,

then the packet **jumps to the target DROP** – **to discard the packet**.

NAT Rules Set Up

- Your private network can "access" CUHK network and itself only.

```
[csci4430@vm-a]$ sudo iptables -t nat -A POSTROUTING \
                 -s 10.0.<vm_group_id>.0/24 -d 137.189.0.0/16 \
                 -j MASQUERADE
```

- Your private network can only **use SSH** to reach the outside world!

```
[csci4430@vm-a]$ sudo iptables -t nat -A POSTROUTING \
                 -p tcp -d ! 10.0.<vm_group_id>.0/24 --dport 22 \
                 -j MASQUERADE
```

iptables – More rules

- Clear all existing rules
  - Flush all entries in the filter table
    - ❖ `iptables -t filter -F`
  - Flush all entries in the nat table
    - ❖ `iptables -t nat -F`
  - Flush all entries in the mangle table
    - ❖ `iptables -t mangle -F`
- List all entries in the nat table
  - ❖ `iptables -t nat -L`
- Always take the manual for reference.

3. Feladat - tűzfalak

Először: iptables.pdf

A) ICMP tiltás

B) TCP port forwarding

C) NAT

Vége
Köszönöm a figyelmet!