NAT MEHANIZAM NA LINUX OS-U

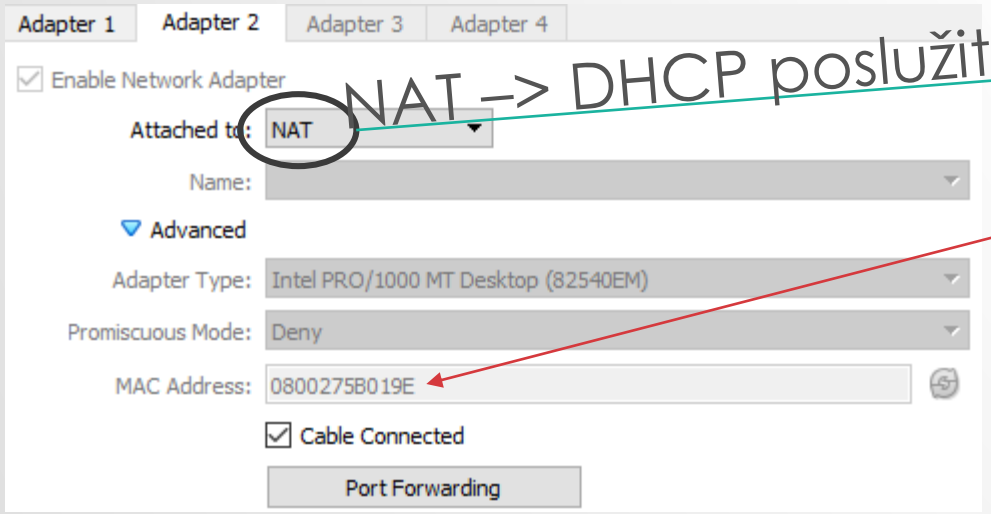
maskiranje

Mirko Jambrošić, mag. ing. inf. et comm. techn.

```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode DEFAULT group default qlen 10
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: enp0s3: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN mode DEFAULT group default qlen 1000
    link/ether 08:00:27:28:c0:73 brd ff:ff:ff:ff:ff:ff
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP mode DEFAULT group defau
    link/ether 08:00:27:5b:01:9e brd ff:ff:ff:ff:ff:ff
```

INFORMATIVKA

- omogućavanje sučelja
  - `sudo ifconfig enp0s3 up`
- određivanje sučelja na VirtualBoxu



NAT –> DHCP poslužitelj!

```
mirko@mint-virtualbox:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet6 fe80::a00:27ff:fe28:c073  prefixlen 64  scopeid 0x
        ether 08:00:27:28:c0:73  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 29  bytes 3389 (3.3 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions

enp0s8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.3.15  netmask 255.255.255.0  broadcast 10.0.3.
        inet6 fe80::e51d:398:4e30:d98b  prefixlen 64  scopeid 0x
        ether 08:00:27:5b:01:9e  txqueuelen 1000  (Ethernet)
        RX packets 341  bytes 32584 (32.5 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 390  bytes 36569 (36.5 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 132  bytes 11543 (11.5 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 132  bytes 11543 (11.5 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions
```

POSTAVLJANJE IP ADRESE NA „LOKALNO" SUČELJE

- sučelje koje je spojeno na *internal network*
  - enp0s3 u ovom slučaju
  - podmreža 192.168.1.0/24
- CHR u istom *internal networku*
  - adresa: 192.168.1.40/24
  - pingabilno?
  - zašto ne radi?

```
mirko@mint-virtualbox:~$ sudo ifconfig enp0s3 192.168.1.100 netmask 255.255.2
mirko@mint-virtualbox:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.100  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::a00:27ff:fe28:c073  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:28:c0:73  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 40  bytes 5119 (5.1 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

```
[admin@MikroTik] > ping 192.168.1.100
  SEQ HOST                                     SIZE TTL TIME  STATUS
    0 192.168.1.100                              56  64 0ms
    sent=1 received=1 packet-loss=0% min-rtt=0ms avg-rtt=0ms max-rtt=0ms
```

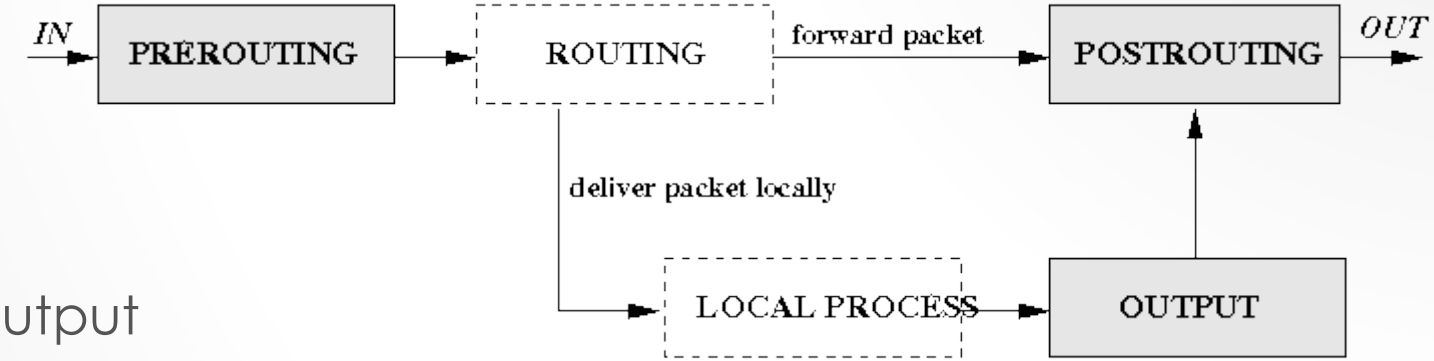
```
[admin@MikroTik] > ping net.hr
invalid value for argument address:
    invalid value of mac-address, mac address required
    invalid value for argument ipv6-address
    while resolving ip-address: could not get answer from dns server
[admin@MikroTik] > _
```

IPTABLES

- implementacija vatrozida
- otvorenog kôda
- namijenjen Linux operacijskim sustavima
- *table*
  - tablice određenih tipova pravila
  - filter, nat, mangle, ...
- *chain*
  - put paketa
- *rule*
  - pravila u tablicama i/ili lancima

UGRAĐENI LANCI

- filter tablica
  - input, forward, output
- nat tablica
  - prerouting, postrouting, output
- mangle tablica
  - prerouting, output
- **omogućavanje (pre)usmjeravanja**
  - npr korištenje NAT-a (inicijalno onemogućeno!)
  - `sudo sysctl -w net.ipv4.ip_forward=1`
    - -w = zapiši (engl. *write*)



NAT sekvenca

KREIRANJE PRAVILA

- pregled pravila
  - `iptables –L -v –line-numbers`
- brisanje pravila
  - `sudo iptables -D LANAC broj_retka`
- potrebno je odrediti tablicu
  - `-t ime_tablice`
  - podrazumjeva se tablica *filter*
  - u suprotnom, potrebno je navoditi ime tablice
- operaciju
  - -A dodavanje
  - -D brisanje
  - -R zamjena
  - -I ubacivanje

```
mirko@mint-virtualbox:~$ sudo iptables -L --line-numbers
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination
1    DROP       icmp --  anywhere             192.168.1.40

Chain FORWARD (policy ACCEPT)
num  target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
num  target     prot opt source               destination
mirko@mint-virtualbox:~$ sudo iptables -D INPUT 1
mirko@mint-virtualbox:~$ sudo iptables -L --line-numbers
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
num  target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
num  target     prot opt source               destination
mirko@mint-virtualbox:~$
```

KREIRANJE PRAVILA

- uzorak
  - -p protokol (TCP, UDP, ICMP, ...)
  - -s izvorišna adresa
  - -d odredišna adresa
  - -i ulazni uređaj
  - -o izlazni uređaj
  - --dport odredišna vrata
  - --sport izvorišna vrata
  - ! negacija
- akciju
  - -j ACCEPT, DROP, REJECT, MASQUERADE, LOG, ...

PRIMJER BLOKIRANJE ICMP

- CHR 192.168.1.40, Linux 192.168.1.100
- `sudo iptables -A INPUT -p ICMP -i enp0s3 -j DROP`
  - za sve ICMP pakete koji ulaze *u linux* kroz sučelje enp0s3 -> akcija = odbaci
  - podrazumjeva se tablica *filter*

```
[admin@MikroTik] > ping 192.168.1.100
  SEQ HOST                                     SIZE TTL TIME
    0 192.168.1.100                              56  64 0ms
    1 192.168.1.100                              56  64 0ms
    sent=2 received=2 packet-loss=0% min-rtt=0ms avg-rtt=0ms
[admin@MikroTik] >
```

```
mirko@mint-virtualbox:~$ ping 192.168.1.40
PING 192.168.1.40 (192.168.1.40) 56(84) bytes of data.
64 bytes from 192.168.1.40: icmp_seq=1 ttl=64 time=0.290 ms
64 bytes from 192.168.1.40: icmp_seq=2 ttl=64 time=0.297 ms
64 bytes from 192.168.1.40: icmp_seq=3 ttl=64 time=0.289 ms
^C
--- 192.168.1.40 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2046ms
rtt min/avg/max/mdev = 0.289/0.292/0.297/0.003 ms
mirko@mint-virtualbox:~$
```

```
mirko@mint-virtualbox:~$ sudo iptables -A INPUT -p ICMP -i enp0s3 -j DROP
mirko@mint-virtualbox:~$ sudo iptables -L -v --line-numbers
Chain INPUT (policy ACCEPT 1 packets, 328 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1        0     0 DROP       icmp --  enp0s3 any     anywhere             anywhere

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source               destination
```

MASKIRANJE

- linux ima dva sučelja
  - testno, pripazi na imena sučelja!
  - enp0s3 – lokalno, *spojeno s* CHR-om
  - enp0s8 – javno, spojeno na NAT sučelje na virtualboxu
  - enp0s8 ima uključen DHCP klijent
  - postoji *defaultna* ruta
  - može se pingati neko javno računalo

```
mirko@mint-virtualbox:~$ ping 1.1.1.1
PING 1.1.1.1 (1.1.1.1) 56(84) bytes of data.
64 bytes from 1.1.1.1: icmp_seq=1 ttl=54 time=8.06 ms
64 bytes from 1.1.1.1: icmp_seq=2 ttl=54 time=7.58 ms
64 bytes from 1.1.1.1: icmp_seq=3 ttl=54 time=8.30 ms
^C
--- 1.1.1.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 7.589/7.987/8.307/0.307 ms
mirko@mint-virtualbox:~$
```

```
mirko@mint-virtualbox:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.100  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::a00:27ff:fe28:c073  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:28:c0:73  txqueuelen 1000  (Ethernet)
        RX packets 498  bytes 141678 (141.6 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 67  bytes 7338 (7.3 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

enp0s8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.3.15  netmask 255.255.255.0  broadcast 10.0.3.255
        inet6 fe80::e51d:398:4e30:d98b  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:5b:01:9e  txqueuelen 1000  (Ethernet)
        RX packets 609  bytes 57268 (57.2 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 665  bytes 59376 (59.3 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 171  bytes 15492 (15.4 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 171  bytes 15492 (15.4 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

mirko@mint-virtualbox:~$ ip route
default via 10.0.3.2 dev enp0s8 proto dhcp metric 100
10.0.3.0/24 dev enp0s8 proto kernel scope link src 10.0.3.15 metric 100
169.254.0.0/16 dev enp0s8 scope link metric 1000
192.168.1.0/24 dev enp0s3 proto kernel scope link src 192.168.1.100
mirko@mint-virtualbox:~$
```

MASKIRANJE

- sve što *izlazi* kroz enp0s8 -> maskiraj
- prema NAT sekvenci chain je POSTROUTING
- `sudo iptables -t nat –A POSTROUTING –j MASQUERADE –o enp0s8`

```
mirko@mint-virtualbox:~$ sudo iptables -t nat -A POSTROUTING -j MASQUERADE -o enp0s8
```

```
mirko@mint-virtualbox:~$ sudo iptables -t nat -L -v --line-numbers
Chain PREROUTING (policy ACCEPT 2 packets, 194 bytes)
num   pkts bytes target     prot opt in     out     source               destination

Chain INPUT (policy ACCEPT 1 packets, 138 bytes)
num   pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 6 packets, 456 bytes)
num   pkts bytes target     prot opt in     out     source               destination

Chain POSTROUTING (policy ACCEPT 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1        7   512 MASQUERADE  all  --  any    enp0s8  anywhere             anywhere
```