

# LINUX kā maršrutētājs



Ilvars Tauriņš

2006. gada novembris

# Kas ir maršrutētājs?

Maršrutētājs ir ierīce, kura savieno divus dažādus datortīklus, un tā ir diezgan komplicēta ierīce ar plašām iespējām.



# Ko mums vajag?

- Divas tīkla kartes

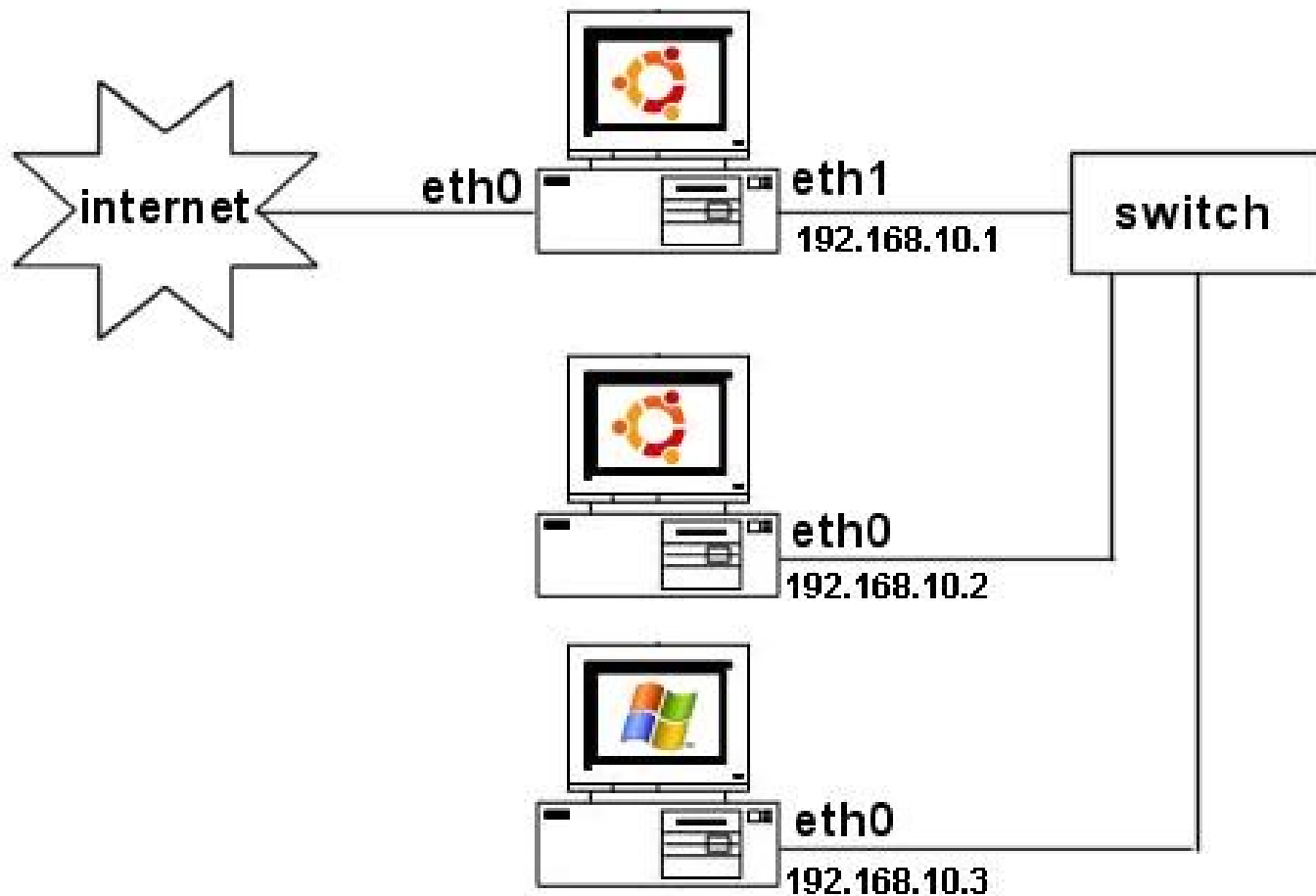
**eth1** - datortīkla karte uz iekšējo datortīklu

**eth0** - datortīkla karte uz Internet

**192.168.10.0/24** - iekšējā tīkla IP adreses



# Maršrutētāja OS Ubuntu 6.06





# Adrešu maršrutēšana

- `iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j DNAT --to-destination 192.168.10.2:8080` web serveris
- `iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 21 -j DNAT --to-destination 192.168.10.3:21` FTP serveris



# Starp WAN un maršrutētāju

- Aizliegt no Interneta pingot maršrutētāju  
`iptables -A INPUT -p icmp -i eth0 -j DROP`
- Aizliegt visus portus  
`iptables -A INPUT -p ALL -i eth0 -j DROP`



# Adrešu filtrs

- **Iptables -t nat -A PREROUTING -i eth1 -p tcp --dport 80 -d 207.46.199.60 -j DROP** Aizliedz pieeju [www.microsoft.com](http://www.microsoft.com)

# Portu filtrs

- **Iptables -t nat -A PREROUTING -i eth1 -p tcp --dport 21 -j DROP** Aizliedz pieeju caur 21 portu



# Ātrumu ierobežošana jeb Traffic shaping

- **iptables -t mangle -A POSTROUTING -s 192.168.10.2 -j CLASSIFY --set-class 1:2**  
**iptables -t mangle -A POSTROUTING -d 192.168.10.2 -j CLASSIFY --set-class 2:2**  
klasificējam IP adresi
- **tc qdisc add dev eth0 root handle 1: htb r2q 3 default 15**  
**tc qdisc add dev eth1 root handle 2: htb r2q 8 default 15**  
Definējam "root queueing discipline"  
r2q aprēķina pēc formulas mazākais ātrums (B) / MTU (1500 B) > r2q lielākais veselais sk.
- **tc class add dev eth0 parent 1: classid 1:10 htb rate 220Kbit ceil 220Kbit**  
**tc class add dev eth1 parent 2: classid 2:10 htb rate 510Kbit ceil 510Kbit**  
Definējam katrai tīkla kartei klasi ar lielāko ātrumu, kāds ir iespējams
- **tc class add dev eth0 parent 1:10 classid 1:2 htb rate 44Kbit ceil 220Kbit**  
**tc class add dev eth1 parent 1:10 classid 2:2 htb rate 102Kbit ceil 510Kbit**  
Definējam katrai IP klasi ar lielāko ātrumu, kāds ir iespējams
- **tc qdisc add dev eth0 parent 1:11 handle 111: sfq perturb 10**  
**tc qdisc add dev eth1 parent 2:11 handle 211: sfq perturb 10**  
Definējam godīgu brīvo interneta sadali



# Lai viss pēc restarta strādātu

- Uzrakstam skriptu un iekopejam to mapē /etc/init.d
- Uzliekam failiem executable(izpildīšanās) tiesības, konsolē ierakstot: **chmod +x**
- Ierakstam failā /etc/rc.local ceļus pie skriptiem pirms exit 0.



# Firewall.sh

```
#!/bin/sh
```

```
#Ceļi
```

```
IPTABLES='/sbin/iptables'
```

```
#deklarēsim dažas konstantes
```

```
EXT_IF='eth0'
```

```
INT_IF='eth1'
```

```
# Definēsim lietotājus
```

```
PC1='192.168.10.11'
```

```
PC2='192.168.10.12'
```

```
PC3='192.168.10.13'
```

```
PC4='192.168.10.14'
```



```
$IPTABLES -F
$IPTABLES -t nat -F
$IPTABLES -X
$IPTABLES -t nat -X
$IPTABLES -t nat -A POSTROUTING -o $EXT_IF -j MASQUERADE
$IPTABLES -A FORWARD -i $INT_IF -j ACCEPT
echo 1 > /proc/sys/net/ipv4/ip_forward
```

#Katra PC klasificēsim

```
$IPTABLES -t mangle -A POSTROUTING -s $PC1 -j CLASSIFY --set-class 1:11
$IPTABLES -t mangle -A POSTROUTING -d $PC1 -j CLASSIFY --set-class 2:11
$IPTABLES -t mangle -A POSTROUTING -s $PC2 -j CLASSIFY --set-class 1:12
$IPTABLES -t mangle -A POSTROUTING -d $PC2 -j CLASSIFY --set-class 2:12
$IPTABLES -t mangle -A POSTROUTING -s $PC3 -j CLASSIFY --set-class 1:13
$IPTABLES -t mangle -A POSTROUTING -d $PC3 -j CLASSIFY --set-class 2:13
$IPTABLES -t mangle -A POSTROUTING -s $PC4 -j CLASSIFY --set-class 1:14
$IPTABLES -t mangle -A POSTROUTING -d $PC4 -j CLASSIFY --set-class 2:14
```

```
exit 0
```



# Traffic\_shaper.sh

```
#!/bin/sh
#Definējam konstantes
TC='/sbin/tc'
EXT_IF='eth0'
INT_IF='eth1'
# Interneta ātrumi Kbit/s
MAX_UP='220'
MAX_DOWN='510'
EXT_ROOT_Q='1:'
INT_ROOT_Q='2:'
EXT_ROOT_C='1:10'
INT_ROOT_C='2:10'
# Maršrutētāja qdisc
$TC qdisc add dev $EXT_IF root handle $EXT_ROOT_Q htb r2q 3 default 10
$TC qdisc add dev $INT_IF root handle $INT_ROOT_Q htb r2q 8 default 10
# Maršrutētāja klase
$TC class add dev $EXT_IF parent $EXT_ROOT_Q classid $EXT_ROOT_C htb rate
    ${MAX_UP}Kbit ceil ${MAX_UP}Kbit
$TC class add dev $INT_IF parent $INT_ROOT_Q classid $INT_ROOT_C htb rate
    ${MAX_DOWN}Kbit ceil ${MAX_DOWN}Kbit
```



# Download un Upload klases

# PC1

```
$TC class add dev $EXT_IF parent $EXT_ROOT_C classid ${EXT_ROOT_Q}11  
htb rate ($MAX_UP/5)Kbit ceil ${MAX_UP}Kbit
```

```
$TC class add dev $INT_IF parent $INT_ROOT_C classid ${INT_ROOT_Q}11  
htb rate (MAX_DOWN/5)Kbit ceil ${MAX_DOWN}Kbit
```

# PC2

```
$TC class add dev $EXT_IF parent $EXT_ROOT_C classid ${EXT_ROOT_Q}12  
htb rate ($MAX_UP/5)Kbit ceil ${MAX_UP}Kbit
```

```
$TC class add dev $INT_IF parent $INT_ROOT_C classid ${INT_ROOT_Q}12  
htb rate (MAX_DOWN/5)Kbit ceil ${MAX_DOWN}Kbit
```

#PC3

```
$TC class add dev $EXT_IF parent $EXT_ROOT_C classid ${EXT_ROOT_Q}13  
htb rate ($MAX_UP/5)Kbit ceil ${MAX_UP}Kbit
```

```
$TC class add dev $INT_IF parent $INT_ROOT_C classid ${INT_ROOT_Q}13  
htb rate (MAX_DOWN/5)Kbit ceil ${MAX_DOWN}Kbit
```

#PC4

```
$TC class add dev $EXT_IF parent $EXT_ROOT_C classid ${EXT_ROOT_Q}14  
htb rate ($MAX_UP/5)Kbit ceil ${MAX_UP}Kbit
```

```
$TC class add dev $INT_IF parent $INT_ROOT_C classid ${INT_ROOT_Q}14  
htb rate ($MAX_DOWN/5)Kbit ceil ${MAX_DOWN}Kbit
```

# Default, priekš cita

```
$TC class add dev $EXT_IF parent $EXT_ROOT_C classid ${EXT_ROOT_Q}15  
htb rate ($MAX_UP/5)Kbit ceil ${MAX_UP}Kbit
```

```
$TC class add dev $INT_IF parent $INT_ROOT_C classid ${INT_ROOT_Q}15  
htb rate (MAX_DOWN/5)Kbit ceil ${MAX_DOWN}Kbit
```

**# dalīt godīgi brīvo internetu**

**# PC1**

**\$TC qdisc add dev \$EXT\_IF parent \${EXT\_ROOT\_Q}11 handle 111: sfq perturb 10**

**\$TC qdisc add dev \$INT\_IF parent \${INT\_ROOT\_Q}11 handle 211: sfq perturb 10**

**# PC2**

**\$TC qdisc add dev \$EXT\_IF parent \${EXT\_ROOT\_Q}12 handle 112: sfq perturb 10**

**\$TC qdisc add dev \$INT\_IF parent \${INT\_ROOT\_Q}12 handle 212: sfq perturb 10**

**# PC3**

**\$TC qdisc add dev \$EXT\_IF parent \${EXT\_ROOT\_Q}13 handle 113: sfq perturb 10**

**\$TC qdisc add dev \$INT\_IF parent \${INT\_ROOT\_Q}13 handle 213: sfq perturb 10**

**# PC4**

**\$TC qdisc add dev \$EXT\_IF parent \${EXT\_ROOT\_Q}14 handle 114: sfq perturb 10**

**\$TC qdisc add dev \$INT\_IF parent \${INT\_ROOT\_Q}14 handle 214: sfq perturb 10**

**# Default, priekš cita**

**\$TC qdisc add dev \$EXT\_IF parent \${EXT\_ROOT\_Q}15 handle 115: sfq perturb 10**

**\$TC qdisc add dev \$INT\_IF parent \${INT\_ROOT\_Q}15 handle 215: sfq perturb 10**

**exit 0**

