

# *Linux jako broadband router (1)*



Ondřej Caletka

O.Caletka@sh.cvut.cz  
<http://www.pslib.cz/caletka>



# *Linux jako broadband router*

- Volíme adresní rozsah
  - Sítování z příkazového řádku
  - Konfigurace NATu
  - DHCP server
  - *DNS server (forwarder)*
  - *Provázání DHCP a DNS*
- 
-

# Pro a proti

- Pro PC Router:
  - vyšší konfigurovatelnost
  - stabilita
  - možnost omezování šířky pásma
  - rozšiřitelnost o VPN, HTTP Cache, Apache...
  - cena HW
- Pro HW Router:
  - spotřeba elektřiny
  - nízká hlučnost
  - nenáročnost konfigurace



# Volíme adresní rozsah

- Máme vlastně tři možnosti

- a) 10.0.0.0 - 10.255.255.255 (10/8 prefix)
- b) 172.16.0.0 - 172.31.255.255 (172.16/12 prefix)
- c) 192.168.0.0 - 192.168.255.255 (192.168/16 prefix)

- Pozor na standardní masku

- Není dobré vybírat si „provažené“ rozsahy jako 10.0.0.0/8,24; 192.168.0.0/24; 192.168.1.0/24

# Rychlokurz síťování

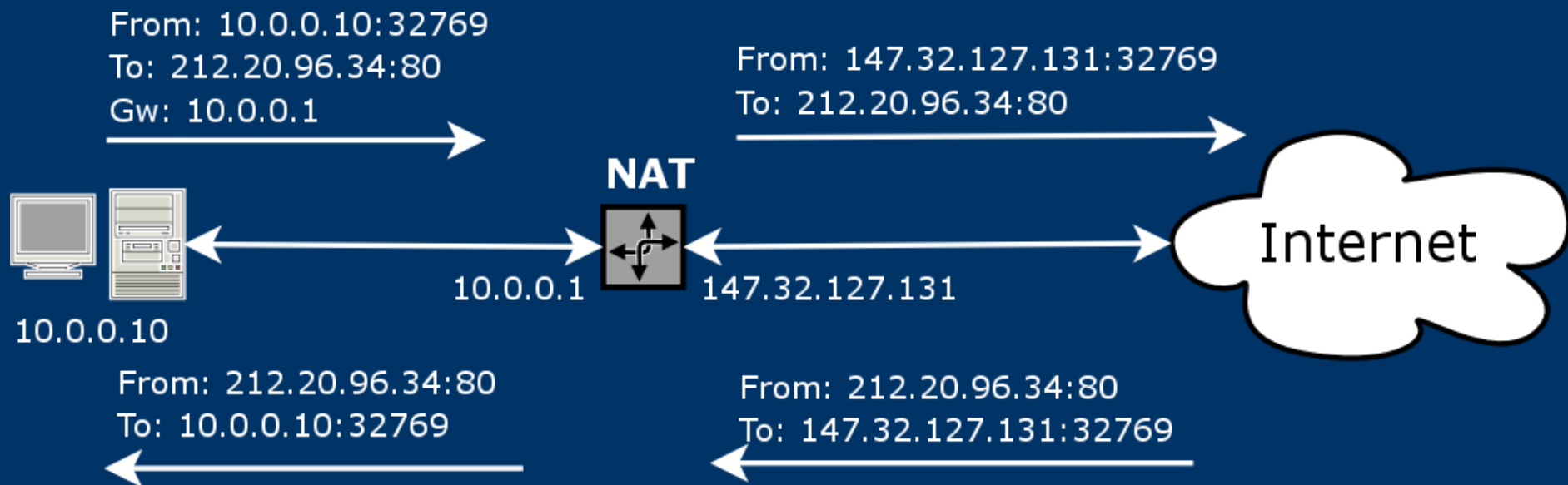
- Nastavení z DHCP: *dhcpcd eth0*
- Ruční nastavení:

```
ip addr add dev eth0 192.168.0.25/24  
ip route add default via 192.168.0.1
```

- Nebo postaru:

```
ifconfig eth0 up 192.168.0.25 netmask \  
255.255.255.0  
route add default gw 192.168.0.1
```

# NAT – překlad síťových adres



# Rozjetí NATu v iptables

- Nastavení pravidla pro SNAT:

```
iptables -t nat -A POSTROUTING -s 10.0.0.0/24 \  
-d \! 10.0.0.0/24 -j SNAT --to-source 147.32.127.131
```

- Povolení forwardování paketů

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

- Port forwarding

```
iptables -t nat -A PREROUTING -p tcp --dport 10022 \  
-j DNAT --to-destination 10.0.0.10:22
```



# Jak uložit nastavení trvale?

- Vytvořit ze sady pravidel initskript – nedoporučuje se používat jiné než číselné názvy
  - Příkazem *iptables-save*:
    - Uloží na std. výstup (!) stav netfiltru ve formě sekvence argumentů příkazu *iptables*, kterými se do prázdného netfiltru současný stav replikuje
    - Tento výstup je také vhodný pro zjištění stavu netfilteru.
    - Stav netfilteru se obnoví příkazem *iptables-restore*
    - Distribuce to obvykle automatizují */etc/init.d/iptables save*
- 
-



# Testování

- Sledování provozu na rozhraních – tcpdump:
    - tcpdump -i eth0
    - tcpdump -i eth0 host 192.168.125.1
  - Trasování cesty k cíli – traceroute; mtr:
    - mtr 147.32.127.240
  - Podmínky průchodu paketu routerem:
    1. iptable filter, chain FORWARD
    2. /proc/sys/net/ipv4/ip\_forward = 1
    3. správně nastavená iptable nat
    4. nepřekrývající se adresní rozsahy síťových rozhraní
- 
-

# DHCP Server

- Přiděluje automaticky IP adresy
- Nejrozšířenější je od ISC – dhcpd
- Konfiguruje se souborem */etc/dhcp/dhcpd.conf*

```
option domain-name "doma.net";  
option domain-name-servers 147.32.127.241;  
default-lease-time 600;  
max-lease-time 7200;
```

```
authoritative;
```

```
subnet 147.32.114.0 netmask 255.255.255.0 {  
}
```

# *DHCP Server*

```
subnet 192.168.9.0 netmask 255.255.255.0 {  
    range 192.168.9.10 192.168.9.20;  
    option routers 192.168.9.1;  
}
```

```
host evo {  
    hardware ethernet 00:d0:59:82:01:74;  
    fixed-address 192.168.9.2;  
}
```



# Závěr

- Pěkný návod o síťování v linuxu na <http://www.pslib.cz/ke/manuals/linux/network/index.phtml>
  - O (statické) DNS je hodně v LDP: <http://knihy.cpress.cz/DataFiles/Book/00000675/Download/K0819.pdf>
  - Seriál na rootovi: <http://www.root.cz/serialy/linux-jako-internetova-gateway/>
  - Diskuze
- 
-

# *Kdo obrací Metro na Dejvické?*



# Režim Bezobslužného Obratu

- Nová funkce Liniového Zabezpečovače pro trat' A
- 1. úspěšný test na Dejvické 22.9.2006 01:58
- 3x CCTV + software pro detekci nežádoucích objektů v kolejišti
- Přisvětlení 1. staniční koleje

