# Linux - správa síťového prostředí

Roman Pavelka

# Obsah

- Konfigurace síťových služeb
- Diagnostika síťového provozu
- Použití snifferu
- Linux jako router
- Firewall iptables
- NAT v Linuxu
- Konfigurace DHCP a DNS brány
- IPv6
- Konfigurace serveru
- Sdílení souborů pro Windows pomocí serveru SAMBA

# Konfigurace síťových služeb

- Pomocí distribučních utilit
- Pomocí utility ip
- Ruční konfigurace v režimu rescue
- Použití DHCP klienta

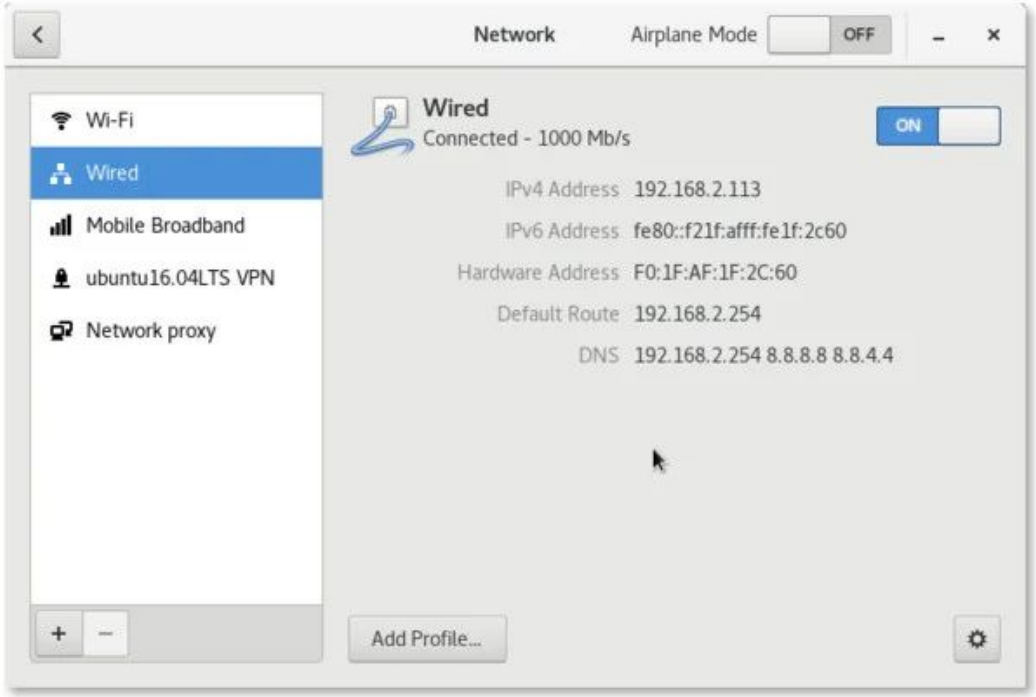
# Konfigurace síťových služeb

**Pomocí distribučních utilit**

NetworkManager daemon

+

GUI frontend



# Konfigurace síťových služeb

## Pomocí utility ip

```
systemctl stop NetworkManager

ip addr

ip addr add/del 192.0.2.11/24 dev eth0

ip link set X up/down

ip route get/add

ss -nltu
```

dříve `netstat -tulnp`

# Konfigurace síťových služeb

## DHCP (virtualbox: NAT networking)

```
dhclient enp0s3

ip route

ping 8.8.8.8

ip route get 8.8.8.8
```

**Host:** `netcat -l 0.0.0.0 8888`
**VM:** `curl <>:8888`

# Konfigurace síťových služeb

**Manuální konfigurace:**

```
ip addr add <IP>/<NET> dev <INTERFACE>

ip route add default via <IP>

ping 8.8.8.8
```

# Diagnostika síťového provozu

## Diagnostika síťového připojení

`ip addr`

`ping`

`ip route get`

## Nástroje na monitorování sítě

`nmap`

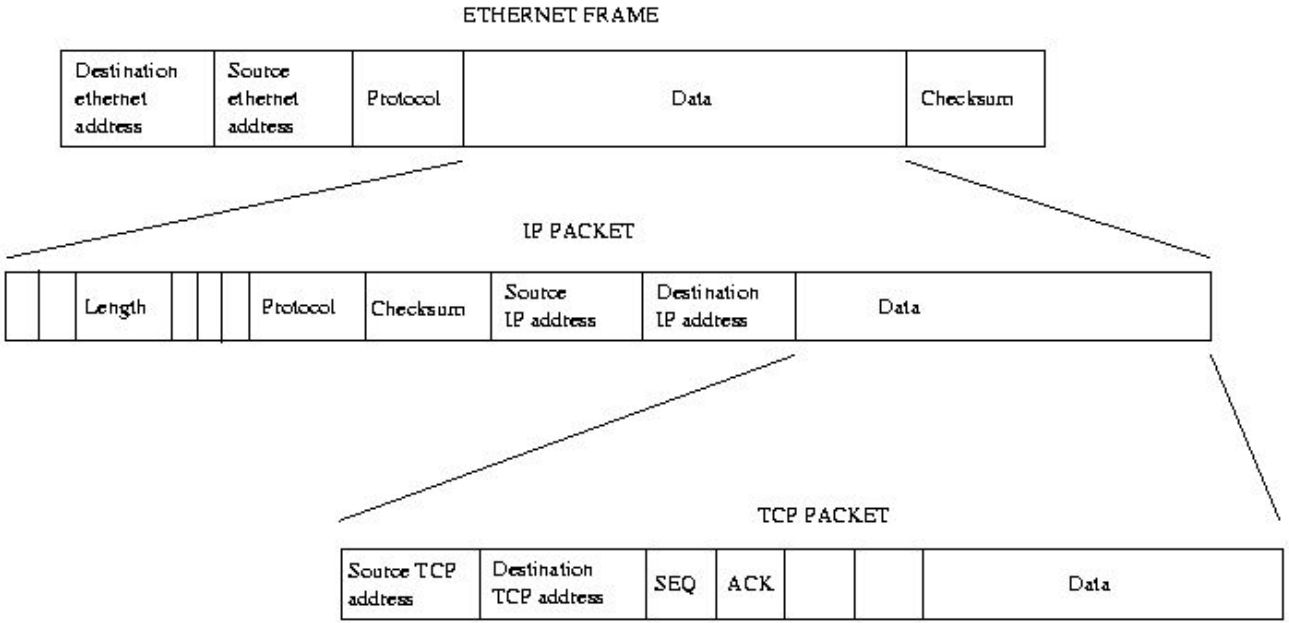
`traceroute`

# Použití snifferu

- Koncept zapouzdření síťového provozu
- Principy protokolů TCP, UDP, IP
- Význam ethernetové hlavičky, protokol ARP
- Tcpdump
- Wireshark
- Interpretace výsledků

# Použití snifferu

**Koncept zapouzdření síťového provozu** **zdroj obrázku:** https://tldp.org/LDP/tlk/net/net.html



# Použití snifferu

**Principy protokolů TCP, UDP, IP**

https://en.wikipedia.org/wiki/Transmission_Control_Protocol#TCP_segment_structure

https://en.wikipedia.org/wiki/User_Datagram_Protocol#UDP_datagram_structure

https://en.wikipedia.org/wiki/File:IPv4_Packet-en.svg

# Použití snifferu

Význam ethernetové hlavičky

https://en.wikipedia.org/wiki/Ethernet_frame#Ethernet_II

Address Resolution Protocol

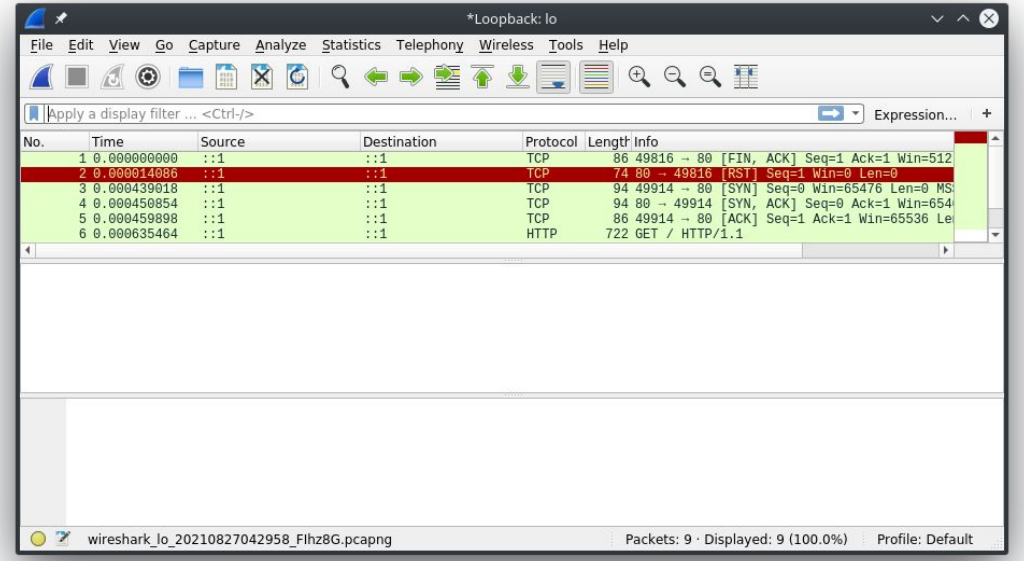
- IP -> MAC
- Resolved or broadcasted

# Použití snifferu

## Tcpdump, Wireshark, Interpretace výsledků

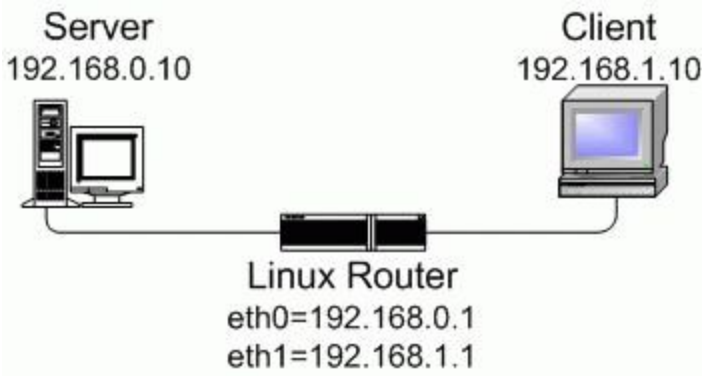
```
tcpdump -i lo -v -n -l | egrep -i "POST /|GET /|Host:"
```

```
tcpdump -i lo -vvAl | grep 'User-Agent:'
```
(Zdroj)



# Linux jako router

Konfigurace Linuxu pro routování mezi dvěma sítěmi




Zdroj, Obrázek

# Linux jako router

### 1. Static IPs

```
$ sudo nano /etc/network/interfaces
# Defining the first interface
auto <interface_name>
iface <interface_name> inet static
address 192.168.0.1
netmask 255.255.255.0

# Defining the second interface
auto <interface_name>
iface <interface_name> inet static
address 192.168.1.1
netmask 255.255.255.0
```

# Linux jako router

## 2. Routing

```
ip route add 192.168.1.0/24 via 192.168.0.1
ip route add 192.168.0.0/24 via 192.168.1.1
```

## 3. Packet forwarding

```
nano /etc/sysctl.conf

...
net.ipv4.ip_forward=1

...

sysctl -p
```

# Firewall iptables

**Firewall:** blocks some traffic

**Filters:** INPUT / FORWARD / OUTPUT

**Targets:** ACCEPT / DROP / RETURN / <chain>

**List all rules:** `sudo iptables -L -v`

# Firewall iptables

**Smazat vše**

```
sudo iptables -F
```

**Povolíme jedinou adresu na portu 80**

```
sudo iptables -A INPUT -s 192.168.1.3 -p tcp --dport 22 -j ACCEPT
```

```
sudo iptables -A INPUT -j DROP
```

**Uložit vše**

```
sudo /sbin/iptables-save
```

(Zdroj)

# NAT v Linuxu

**NAT** = Změna IP source a/nebo IP destination průchozích paketů

Konfigurace NAT pomocí IPTables

1. **Maškaráda (vnitřní počítače mají IP toho vnějšího):**

   ```
   iptables -t nat -A POSTROUTING -o eth0 -s 10.0.0.0/24 -j MASQUERADE
   ```

2. **SNAT (nastavitelná IP)**

   ```
   iptables -t nat -A POSTROUTING -o eth0 -s 10.0.0.0/24 -j SNAT --to-source 123.123.123.1
   ```

(Zdroj)

# Konfigurace DHCP a DNS brány

## DNS

```
apt-get install bind9

ls  /etc/bind/

cat /etc/bind/named.conf.local
```

(Zdroj)

Lokálně: `/etc/hosts`

# Konfigurace DHCP a DNS brány

## DHCP

```
sudo apt install isc-dhcp-server

nano /etc/dhcp/dhcpd.conf
...
option domain-name-servers 10.1.1.1, 8.8.8.8;
...
```

(Zdroj)

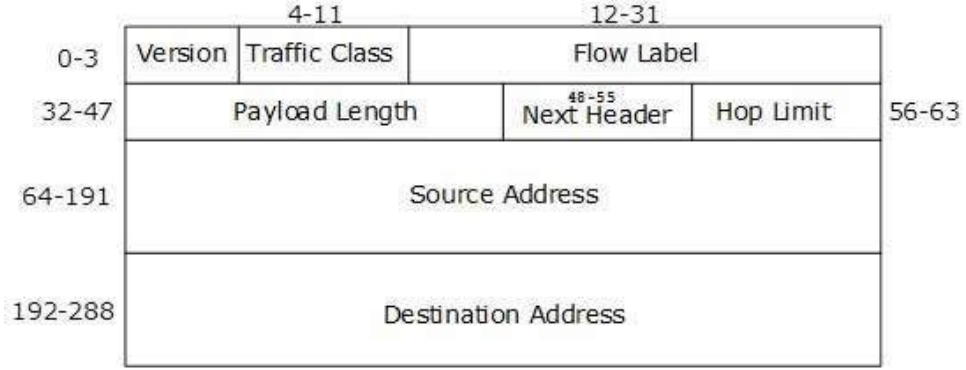
# IPv6

IPv6 v Linuxu

2001:0db8:3042:0002:5a55:caff:fef6:bdbf

Základní pojmy IPv6

::/0 default, ::1/128 defalt




Konfigurace IPv6 v Linuxu

```
ip -6 addr add 2001:db8:1:1:204:76ff:fe47:c/64 dev eth0
ip -6 route show
```

Link local adresy

(Zdroj obrázku, CZ zdroj, TLDP zdroj)

# Konfigurace serveru

**Základní konfigurace webového serveru Apache s PHP a MySQL (LAMP)**

```
sudo apt install php libapache2-mod-php php-mysql mariadb
```

```
/etc/apache2/sites-available/
```

(Zdroj)

# Konfigurace serveru

## Zprovoznění FTP

```
sudo apt install vsftpd
```

```
/etc/vsftpd.conf
/etc/vsftpd.userlist
```

```
sudo systemctl restart vsftpd
```

(Zdroj)

# Sdílení souborů pro Windows pomocí serveru SAMBA

```
sudo apt install samba

mkdir /home/username/sambashare

/etc/samba/smb.conf:
[sambashare]
    comment = Samba on Ubuntu
    path = /home/username/sambashare
    read only = no
    browsable = yes

sudo service smbd restart

sudo smbpasswd -a username

Windows: \\ip-address\sambashare (Zdroj)
```