Základní nastavení sítě

Modul 03

Sergey Kuroedov 2026

Cíle a obsah modulu

1. **Nastavení sítě** — nastavit parametry TCP/IP nástrojem `nmcli` a ověřit je příkazem `ip`
2. **Diagnostika sítě** — lokalizovat příčinu nedostupnosti nástroji `ping` a `tracepath`
3. **Systémový firewall** — přiřadit rozhraní a sítě do zón a povolit služby

3.1 Nastavení sítě

Název systému, NetworkManager, příkaz `ip` , překlad názvů

Název systému

- `hostnamectl` rozlišuje statický, přechodný a popisný název
- statický název je uložen v souboru `/etc/hostname`
- přechodný název přiděluje server DHCP, statický má přednost
- plně kvalifikovaný název (FQDN) obsahuje i doménu

```
hostnamectl set-hostname web01.example.com
hostnamectl
```

Architektura NetworkManageru

- NetworkManager je daemon, který konfiguruje rozhraní podle profilů
- `nmcli` ovládá NetworkManager z příkazového řádku
- `nmtui` nabízí stejné funkce v textovém menu
- profily jsou uloženy v `/etc/NetworkManager/system-connections/`

> **Poznámka** — Formát `ifcfg` v `/etc/sysconfig/network-scripts/` je zastaralý. Fedora ukládá profily ve formátu keyfile.

Rozhraní a profil připojení

```
$ nmcli device status
DEVICE  TYPE      STATE      CONNECTION
enp1s0  ethernet  connected  enp1s0
$ nmcli connection show
NAME    UUID                                  TYPE      DEVICE
enp1s0  5f3c1a2e-8d4b-4c1e-9a7f-2b6d0e3c8a11  ethernet  enp1s0
```

- rozhraní (device) je síťová karta, fyzická nebo virtuální
- profil (connection) je uložená sada parametrů rozhraní
- aktivace profilu použije jeho parametry na rozhraní
- na rozhraní je současně aktivní nejvýše jeden profil

Zjištění stavu příkazem `ip`

Příkaz	Účel
`ip link show`	vypíše rozhraní a stav jejich linky
`ip address show`	vypíše adresy přiřazené rozhraním
`ip -brief address`	vypíše adresy po jednom řádku na rozhraní
`ip route show`	vypíše routovací tabulku
`ip neighbour show`	vypíše sousedy zjištěné protokolem ARP

> **Poznámka** — Nástroje `ifconfig`, `route` a `arp` z balíčku `net-tools` jsou zastaralé a Fedora je ve výchozí instalaci neobsahuje.

Rozhraní a adresy ve výpisu `ip`

```
$ ip address show enp1s0
2: enp1s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 …
    link/ether 52:54:00:3a:1f:7c brd ff:ff:ff:ff:ff:ff
    inet 192.168.10.20/24 brd 192.168.10.255 scope global …
    inet6 fe80::5054:ff:fe3a:1f7c/64 scope link …
```

- příznak `UP` označuje administrativně zapnuté rozhraní
- příznak `LOWER_UP` označuje navázané fyzické spojení
- řádek `link/ether` uvádí adresu MAC
- řádky `inet` a `inet6` uvádějí adresy IPv4 a IPv6 s prefixem

Pojmenování síťových rozhraní

```
$ ip -brief link
lo       UNKNOWN  00:00:00:00:00:00 <LOOPBACK,UP,LOWER_UP>
enp1s0   UP       52:54:00:3a:1f:7c <BROADCAST,MULTICAST,UP,LOWER_UP>
```

- `systemd-udevd` odvozuje název z umístění karty v hardwaru
- název se nemění po restartu ani po přidání další karty
- první dva znaky určují typ: `en` Ethernet, `wl` Wi-Fi, `ww` WWAN
- starší schéma `eth0`, `eth1` číslovalo karty v pořadí detekce

Schémata názvů

Příklad	Schéma	Zdroj údaje
`eno1`	`o<index>`	karta na základní desce, index z firmwaru
`ens3`	`s<slot>`	číslo slotu podle firmwaru
`enp1s0`	`p<sbernice>s<slot>`	umístění na sběrnici PCI
`enx5254003a1f7c`	`x<mac>`	adresa MAC, používá se pro adaptéry USB
`eth0`	jádro	pořadí detekce, pokud ostatní schémata selžou

> **Poznámka** — Názvy virtuálních rozhraní určuje nástroj nebo správce, který je vytváří: `virbr0`, `bond0`, VLAN `enp1s0.100`, `wg0`.

Routovací tabulka

```
$ ip route show
default via 192.168.10.1 dev enp1s0 proto static metric 100
192.168.10.0/24 dev enp1s0 proto kernel scope link src …
$ ip route get 1.1.1.1
1.1.1.1 via 192.168.10.1 dev enp1s0 src 192.168.10.20 uid 0
```

- trasa `default` určuje gateway pro cíle mimo ostatní trasy
- síť `192.168.10.0/24` je dosažitelná přímo, bez gateway
- `ip route get <ip_adresa>` vyhodnotí tabulku pro konkrétní cíl

Změna stavu příkazem `ip`

Příkaz	Účel
`ip link set <rozhrani> down`	vypne rozhraní
`ip link set <rozhrani> up`	zapne rozhraní
`ip link set <rozhrani> mtu <hodnota>`	změní MTU rozhraní
`ip address add <ip_adresa>/<prefix> dev <rozhrani>`	přidá adresu
`ip address del <ip_adresa>/<prefix> dev <rozhrani>`	odebere adresu

> **Upozornění** — Změny provedené příkazem `ip` platí pouze do restartu systému nebo do příští aktivace profilu.

Aktivace a deaktivace spravovaného rozhraní

- NetworkManager sleduje rozhraní a reaguje na změny provedené příkazem `ip`
- `nmcli device disconnect` deaktivuje rozhraní a zablokuje automatickou aktivaci
- `nmcli device connect` rozhraní znovu aktivuje podle profilu
- spravovaná rozhraní aktivujte a deaktivujte nástrojem `nmcli`

```
nmcli device disconnect enp2s0
nmcli device status
nmcli device connect enp2s0
```

Upozornění — Deaktivace rozhraní, přes které vede vzdálené spojení, toto spojení ukončí. Obnovu umožní pouze přístup ke konzoli.

DEMONSTRACE

Správa virtuálního rozhraní

```
ip link add test0 type dummy
ip link set test0 up
ip address add 10.99.0.1/24 dev test0
ip route add 10.98.0.0/16 via 10.99.0.254
ip -brief address
ip route show
ip link set test0 down
ip route show
ip link del test0
```

Uložený profil a aktuální stav

- `nmcli connection show <profil>` zobrazí konfiguraci uloženou v profilu
- `ip` zobrazí aktuální stav rozhraní v jádře
- po změně profilu se výpisy liší až do jeho opětovné aktivace
- změny provedené příkazem `ip` aktivace profilu odstraní

```
nmcli device status
nmcli connection show
nmcli -g ipv4.addresses connection show <profil>
ip -brief address
```

Nastavení statické adresy

```
nmcli connection modify <profil> \
  ipv4.method manual \
  ipv4.addresses 192.168.10.20/24 \
  ipv4.gateway 192.168.10.1 \
  ipv4.dns "192.168.10.5 1.1.1.1"
nmcli connection up <profil>
```

- `ipv4.method manual` vypne přidělení adresy serverem DHCP
- `ipv4.method auto` obnoví přidělení adresy serverem DHCP

Ověření překladu názvů

- NetworkManager generuje `/etc/resolv.conf`; soubor se ručně neupravuje
- `resolvectl status` vypíše servery DNS, je-li aktivní `systemd-resolved`
- pořadí zdrojů pro překlad názvů určuje `/etc/nsswitch.conf`
- `getent hosts <nazev>` použije stejné pořadí zdrojů jako aplikace
- `dig` se dotazuje serveru DNS přímo, mimo `/etc/nsswitch.conf`

3.2 Diagnostika sítě

Postup po vrstvách, `ping`, `tracepath`

Sergey Kuroedov 2026

Postup diagnostiky po vrstvách

Krok	Příkaz
stav rozhraní	`ip link show`
adresa a prefix	`ip -brief address`
výchozí gateway	`ip route show default`
dosažitelnost gateway	`ping -c3 <gateway>`
překlad názvu	`getent hosts <nazev>`

Ověření dosažitelnosti příkazem `ping`

```
$ ping -c3 192.168.10.1
64 bytes from 192.168.10.1: icmp_seq=1 ttl=64 time=0.412 ms
…
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
```

- `ping` odešle žádost ICMP echo a změří dobu odpovědi
- `-c <pocet>` omezí počet žádostí, jinak `ping` běží do `Ctrl+C`
- `Destination Host Unreachable` znamená, že cíl v místní síti neodpovídá
- ztráta odpovědí bez hlášení ukazuje na filtrování nebo výpadek cesty

Upozornění — Chybějící odpověď neprokazuje nedostupnost stroje.
Firewall může zprávy ICMP echo zahazovat.

Sledování cesty k cíli

```
$ tracepath -n 1.1.1.1
 1?: [LOCALHOST]                      pmtu 1500
 1:  192.168.10.1                                          0.512ms
 2:  10.0.0.1                                              3.204ms
 3:  no reply
 4:  1.1.1.1                                               8.911ms reached
```

- každý řádek odpovídá jednomu routeru (hopu) na cestě
- `no reply` znamená, že router neodpověděl, nikoli výpadek
- `tracepath` je součástí základní instalace a nevyžaduje root
- `traceroute` a `mtr` nabízejí více metod a instalují se samostatně

Cvičení 3.1 — Stav a diagnostika sítě

Zadání

1. Zjistěte názvy rozhraní, jejich stav a adresu MAC.
2. Vypište adresu s prefixem, výchozí gateway a servery DNS.
3. Zjistěte, přes které rozhraní a gateway vede cesta k `1.1.1.1`.
4. Ověřte dosažitelnost gateway a druhého cvičného stroje.
5. Zobrazte cestu k `1.1.1.1` a určete počet hopů.
6. Doplňte do profilu další server DNS bez přerušení spojení.
7. Přidejte dočasně druhou adresu, ověřte ji z druhého stroje a odeberte ji.

Očekávaný výsledek — Uvedete rozhraní, adresu, gateway a počet hopů k cíli. Profil obsahuje doplněný server DNS a spojení nebylo přerušeno. Dočasná adresa odpovídala z druhého stroje a po odebrání zanikla.

Čas — 18 minut

3.3 Systémový firewall

Nástroj firewalld, zóny, služby a porty

Sergey Kuroedov 2026

Architektura firewalld

- firewalld je daemon, který spravuje pravidla subsystému `nftables`
- ve výchozí konfiguraci filtruje příchozí spojení, odchozí propouští
- firewalld uspořádává pravidla do zón
- `firewall-cmd` ovládá firewalld z příkazového řádku

Zóna jako seznam pravidel

- zóna je pojmenovaný seznam povolených služeb a portů
- položka `target` určuje naložení se spojeními mimo seznam
- zóna platí pro rozhraní a zdrojové sítě, které jí správce přiřadí
- jedné zóně lze přiřadit libovolný počet rozhraní i sítí
- každé příchozí spojení vyhodnotí firewalld podle jediné zóny

> **Poznámka** — Zóna odpovídá příchozímu ACL s implicitním zákazem na konci.

Výpis zóny

```
$ firewall-cmd --list-all --zone=FedoraServer
FedoraServer (default, active)
  target: default
  interfaces: enp1s0
  sources:
  services: cockpit dhcpv6-client ssh
  ports:
  …
```

- `interfaces` a `sources` určují, na která spojení se zóna uplatní
- `services` a `ports` tvoří seznam povolených spojení
- `target: default` ostatní spojení odmítne

Přiřazení spojení k zóně

```
příchozí spojení
  1. zdrojová adresa patří síti přiřazené zóně → pravidla této zóny
  2. rozhraní je přiřazeno zóně                → pravidla této zóny
  3. jinak                                     → výchozí zóna
```

- zdrojová síť má přednost před rozhraním
- rozhraní i zdrojová síť patří nejvýše do jedné zóny
- spojení bez shody vyhodnotí výchozí zóna

Předdefinované zóny

Zóna	Výchozí obsah
`drop`, `block`	zahazuje, resp. odmítá veškerá příchozí spojení
`public`	povoluje vybrané služby, výchozí zóna v RHEL
`FedoraServer`	výchozí zóna Fedora Server, povoluje SSH a Cockpit
`internal`	povoluje rozšířený seznam služeb pro vnitřní sítě
`trusted`	povoluje veškerá spojení

Vlastní zóna a přiřazení

```
# vlastní zóna pro síť správců
firewall-cmd --permanent --new-zone=spravci
firewall-cmd --permanent --zone=spravci --add-service=ssh
firewall-cmd --permanent --zone=spravci --add-source=10.0.5.0/24
firewall-cmd --reload
# přiřazení rozhraní zóně v profilu NetworkManageru
nmcli connection modify <profil> connection.zone internal
nmcli device reapply <rozhrani>
firewall-cmd --get-active-zones
```

Upozornění — Přesun rozhraní se vzdáleným spojením do zóny bez služby `ssh` toto spojení ukončí.

Správa pravidel

Příkaz	Účel
`firewall-cmd --get-active-zones`	vypíše zóny s přiřazenými rozhraními
`firewall-cmd --list-all`	vypíše obsah výchozí zóny
`firewall-cmd --add-service=http`	povolí službu v runtime konfiguraci
`firewall-cmd --permanent --add-service=http`	povolí službu v permanent konfiguraci
`firewall-cmd --reload`	nahradí runtime konfiguraci permanent konfigurací

Runtime a permanent konfigurace

- runtime konfigurace platí okamžitě a zaniká při `--reload` či restartu
- permanent konfiguraci mění příkazy s parametrem `--permanent`
- `--reload` nahradí runtime konfiguraci permanent konfigurací
- `--runtime-to-permanent` uloží ověřenou runtime konfiguraci natrvalo

Povolení služby a portu

```
firewall-cmd --permanent --add-service=https
firewall-cmd --permanent --add-port=8080/tcp
firewall-cmd --reload
firewall-cmd --list-all
```

- definice služeb dodává distribuce v `/usr/lib/firewalld/services/`
- vlastní definice služeb patří do `/etc/firewalld/services/`

DEMONSTRACE

Poslouchající služba a firewall

```
firewall-cmd --get-default-zone
firewall-cmd --list-all
systemctl start httpd
ss -tulpn | grep ':80'
firewall-cmd --permanent --add-service=http
firewall-cmd --reload
```

Cvičení 3.2 — Zóny a pravidla firewallu

Zadání

1. Zjistěte, ve které zóně firewallu je vaše rozhraní.
2. Povolte trvale port `8080/tcp` a ověřte jej ve výpisu zóny.
3. Z druhého stroje vyzkoušejte spojení na porty `8080` a `8081`.
4. Bez `--permanent` přiřaďte adresu druhého stroje zóně `trusted`.
5. Zopakujte bod 3, poté obnovte permanent konfiguraci.

Očekávaný výsledek — V bodě 3 skončí spojení na oba porty odlišným hlášením, v bodě 5 stejným. Rozdíl dokážete vysvětlit.

Čas — 15 minut

Shrnutí modulu

Shrňte vlastními slovy, jak ve své praxi:

- zjistíte a změníte síťovou konfiguraci serveru
- postupujete, když server není dostupný
- ověříte, které služby jsou dostupné z jiných strojů
- povolíte novou službu, aniž byste ztratili vzdálený přístup

Odkazy na dokumentaci

- Nastavení sítě ve Fedoře — https://docs.fedoraproject.org
- Dokumentace firewalld — https://firewalld.org/documentation/
- Příručka NetworkManageru — https://networkmanager.dev/docs/
- Parametry profilu připojení — `man 5 nm-settings-nmcli`
- Příkaz `ip` a jeho objekty — `man 8 ip`, `man 8 ip-route`
- Správa firewallu — `man 1 firewall-cmd`