

Detailní dokumentace síťového projektu (GNS3 v2.2.54)

Cisco IOS + FRRouting + Linux

Obsah

1	Zadání projektu	2
2	Stručné shrnutí a důležité poznámky	2
3	Topologie a propojení (fyzické / logické)	2
4	Pořadí kroků (doporučené)	3
5	Krok 0 — přidání slotu na R1 (GNS3)	4
6	Krok 1 — konfigurace rozhraní mezi směrovači	4
6.1	R1 (Cisco) — rozhraní směrem k R2	4
6.2	R2 (FRRouting) — rozhraní směrem k R1	4
6.3	R2 — rozhraní směrem k R3	4
6.4	R3 (Cisco) — rozhraní směrem k R2	4
7	Krok 2 — konfigurace LAN rozhraní na R1	4
8	Krok 3 — DHCP (R1) — kompletní kontext a vysvětlení	5
9	Krok 4 — Nastavení linuxových klientů (DHCP nebo statická konfigurace)	5
10	Krok 5 — Statické směrování	6
11	Krok 6 — OSPF (doporučeno pro větší flexibilitu a škálovatelnost)	7
11.1	Povolení OSPF ve FRRouting (R2)	7
11.2	Volba směrovací cesty a administrativní vzdálenost	7
11.3	Odstranění statických rout	7
11.3.1	Router R1 (Cisco)	7
11.3.2	Router R2 (FRRouting)	7
11.3.3	Router R3 (Cisco)	8
11.4	Konfigurace OSPF na R1 (Cisco)	8
11.5	Konfigurace OSPF na R2 (FRRouting)	8
11.6	Konfigurace OSPF na R3 (Cisco)	8
11.7	Ověření funkčnosti OSPF	8
12	Krok 7 — NAT na R3 (Edge router) — kompletní	9
13	Krok 8 — ověření konektivity a testování	10

1 Zadání projektu

Cílem projektu je implementovat menší počítačovou síť s topologií odpovídající přiloženému schématu (minimálně). Síť bude připojena k Internetu přes NAT gateway, která bude realizována konfigurací Cisco routeru.

Síť musí obsahovat:

- alespoň dvě koncové větve (LANy) s připojenými stanicemi, přičemž každá větev má svůj DHCP server pro automatické přidělování IP adres,
- alespoň jeden směrovač běžící na systému Free Range Routing (FRR),
- dynamické směrování pomocí protokolu OSPF, přičemž bude použita *area 0* pro všechny routery.

Funkčnost sítě bude ověřena tím, že z každé stanice v koncových větvích bude možné přistupovat na Internet (např. pomocí příkazu `ping www.seznam.cz`).

2 Stručné shrnutí a důležité poznámky

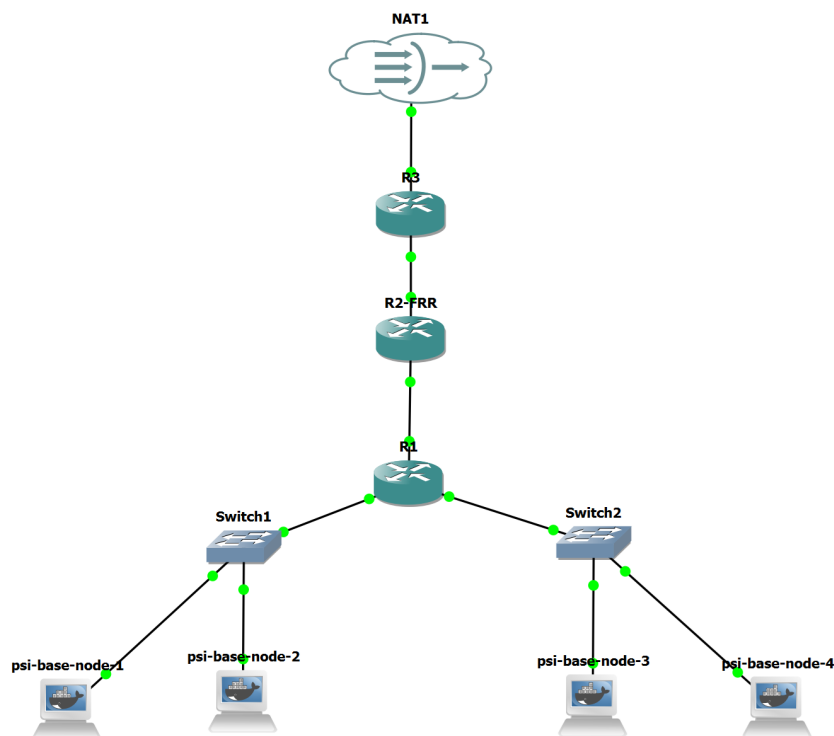
Projekt je realizován v prostředí GNS3 verze **2.2.54**. GNS3 server běží ve virtuálním stroji, ke kterému se uživatel připojuje pomocí GNS3 klienta ve stejné verzi (2.2.54). Pořadí jednotlivých kroků je zásadní. Doporučená sekvence je následující je uvedena níže. Všechny ukázky konfigurace v CLI jsou jednoznačně označeny podle zařízení, na kterém mají být provedeny (R1/R2/R3/Linux/klient). Při změnách konfigurace za běhu v prostředí GNS3 (např. úprava proměnných prostředí u FRRouting) může dojít k automatickému restartu příslušné instance. Proto je doporučeno mít konfiguraci předem uloženou.

Použité verze zařízení a software

- **Cisco routery:** IOS verze 15.0
- **FRRouting (R2):** FRRouting 10.0.4_git (balíček FRRouting10.0.4-1) na Linuxu s jádrem 5.15.0-136-generic
- **Linux klienti:** jádro 5.15.0-136-generic

3 Topologie a propojení (fyzické / logické)

```
cisco R3 Gi1/0 - frrouter R2 eth0
frrouter R2 eth1 - cisco R1 Gi0/0
cisco R1 Gi1/0 - switch1 eth0
cisco R1 Gi2/0 - switch2 eth0
switch1 eth1 - psi-base-node1 eth0
switch1 eth2 - psi-base-node2 eth0
switch2 eth1 - psi-base-node3 eth0
switch2 eth2 - psi-base-node4 eth0
```



Obrázek 1: Struktura projektu

Adresace použité v projektu:

- R1–R2: 192.168.1.0/30 (R1 .1, R2 .2) — v poznámkách je R1 192.168.1.1 a R2 192.168.1.2
- R2–R3: 192.168.2.0/30 (R2 .1, R3 .2) — v poznámkách je R2 192.168.2.1 a R3 192.168.2.2
- LAN1 (připojena na R1 Gi1/0): 10.0.1.0/24, R1 = 10.0.1.254
- LAN2 (připojena na R1 Gi2/0): 10.0.2.0/24, R1 = 10.0.2.254

4 Pořadí kroků (doporučené)

1. Nastavit sloty/moduly na R1 v GNS3 (PA-GE).
2. Nakonfigurovat rozhraní mezi R1, R2, R3 (linky 192.168.1.0/30 a 192.168.2.0/30).
3. Nakonfigurovat lokální rozhraní R1 a přepínače (LANy).
4. Na R1 nastavit DHCP pooly pro obě LAN s vyřazenými adresami.
5. Nakonfigurovat statické směry tam, kde je potřeba (záložní).
6. Povolit OSPF (FRR i Cisco) — nejprve povolit OSPF v FRR containeru (ENV var).
7. Na R3 nakonfigurovat NAT (inside/outside), access-list a NAT overload.
8. Ověřit konektivitu z Linux klientů (pingy, DNS).

5 Krok 0 — přidání slotu na R1 (GNS3)

(GNS3 klient / GNS3 VM)

Right-click na R1 → Configure → Slots → nastavit slot2: PA-GE

6 Krok 1 — konfigurace rozhraní mezi směrovači

6.1 R1 (Cisco) — rozhraní směrem k R2

Spust v R1:

```
conf t
interface GigabitEthernet 0/0
ip address 192.168.1.1 255.255.255.252
no shutdown
CTRL + Z
write
```

6.2 R2 (FRRouting) — rozhraní směrem k R1

```
conf t
interface eth1
ip address 192.168.1.2/30
CTRL + Z
write
```

6.3 R2 — rozhraní směrem k R3

```
conf t
interface eth0
ip address 192.168.2.1/30
CTRL + Z
write
```

6.4 R3 (Cisco) — rozhraní směrem k R2

```
conf t
interface GigabitEthernet 1/0
ip address 192.168.2.2 255.255.255.252
no shutdown
CTRL + Z
write
```

7 Krok 2 — konfigurace LAN rozhraní na R1

```
conf t
interface GigabitEthernet 1/0
ip address 10.0.1.254 255.255.255.0
no shutdown
exit

interface GigabitEthernet 2/0
ip address 10.0.2.254 255.255.255.0
no shutdown
CTRL + Z

write
```

8 Krok 3 — DHCP (R1) — kompletní kontext a vysvětlení

Důležité: DHCP server na R1 obsluhuje oba LANy. To znamená, že:

- musí být správně nakonfigurována IP rozhraní R1 (provedeno výše),
- musí být vytvořeny DHCP pooly pro každou síť,
- musí se vyřadit adresa použitá pro default gateway (R1) ze DHCP (jinak by ji mohl server přidělit klientovi).

Konfigurace (spustit na R1):

```
conf t

! LAN1
ip dhcp excluded-address 10.0.1.254
ip dhcp pool LAN1
network 10.0.1.0 255.255.255.0
default-router 10.0.1.254
dns-server 8.8.8.8 8.8.4.4
exit

! LAN2
ip dhcp excluded-address 10.0.2.254
ip dhcp pool LAN2
network 10.0.2.0 255.255.255.0
default-router 10.0.2.254
dns-server 8.8.8.8 8.8.4.4
CTRL + Z

write
```

Poznámky: Příkaz `ip dhcp excluded-address` musí být definován před vytvořením DHCP poolu. Název poolu je libovolný; v tomto dokumentu jsou pro lepší přehlednost použity názvy LAN1 a LAN2.

Kontrola (R1):

```
show ip dhcp pool
show ip int brief
```

Co očekávat: Příkaz `show ip dhcp binding` zobrazí IP adresy přidělené klientům (vazba MAC → IP → doba zapůjčení). Pokud se žádné záznamy nezobrazí, je nutné ověřit, že klienti mají rozhraní `eth0` nastavené na získávání adresy pomocí DHCP a že jsou připojeni ke správnému switchi a portu.

9 Krok 4 — Nastavení linuxových klientů (DHCP nebo statická konfigurace)

Na všech linuxových klientech (`psi-base-node1` až `psi-base-node4`) je nutné nakonfigurovat síťové rozhraní `eth0` buď pomocí DHCP, nebo staticky pro účely testování konektivity.

Konfigurace pomocí DHCP (permanentní)

Pro trvalé nastavení DHCP je nutné upravit soubor `/etc/network/interfaces`. Konkrétně v něm následující řádky:

```
/etc/network/interfaces

auto eth0
iface eth0 inet dhcp
```

Statická konfigurace (dočasná)

Pro krátkodobé testování lze IP adresu a výchozí bránu nastavit přímo z příkazové řádky. Toto nastavení se po restartu klienta ztratí.

```
ip addr add 10.0.1.1/24 dev eth0      # klient v LAN1
ip link set eth0 up
ip route add default via 10.0.1.254

# pro LAN2:
# ip addr add 10.0.2.1/24 dev eth0
# ip route add default via 10.0.2.254
```

Poznámka k úpravě výchozí trasy

Pokud má klient chybně nastavenou výchozí trasu a je potřeba ji rychle nahradit, lze použít následující příkaz:

```
ip route replace default via <IP>
```

Ověření konektivity

Funkčnost konfigurace lze ověřit testem konektivity k výchozí bráně:

```
ping 10.0.1.254
```

10 Krok 5 — Statické směrování

Tento krok je volitelný a slouží pouze jako demonstrace manuální konfigurace statických směrovacích záznamů. Umožňuje názorně ukázat princip ručního směrování a ověřit základní konektivitu sítě bez použití dynamických směrovacích protokolů.

V **kroku 6** jsou však statické trasy z důvodu kolize priorit (*administrative distance*) s protokolem OSPF odstraněny. Z tohoto důvodu je možné tento krok zcela vynechat a pokračovat přímo konfigurací dynamického směrování pomocí OSPF.

Na R1:

```
conf t
ip route 0.0.0.0 0.0.0.0 192.168.1.2
exit
write
```

Na R2 (FRR):

```
conf t
ip route 0.0.0.0/0 192.168.2.2 eth0
ip route 10.0.0.0/16 192.168.1.1
exit
write
```

Na R3:

```
conf t
ip route 10.0.0.0 255.255.0.0 192.168.2.1
exit
write
```

Testy na klientovi:

```
ping 192.168.2.1
ping 192.168.2.2
```

11 Krok 6 — OSPF (doporučeno pro větší flexibilitu a škálovatelnost)

V tomto kroku je statické směrování nahrazeno dynamickým směrovacím protokolem OSPF. OSPF umožňuje automatickou výměnu směrovacích informací, rychlou konvergenci a lepší rozšiřitelnost topologie oproti statickým trasám.

11.1 Povolení OSPF ve FRRouting (R2)

Než lze OSPF na routeru R2 (FRRouting) konfigurovat, je nutné jej explicitně povolit pomocí proměnné prostředí. **Doporučení:** před touto změnou uložte veškerou konfiguraci, protože úprava proměnných prostředí způsobí restart instance.

Postup v prostředí GNS3:

Pravé tlačítko na R2 → Configure → General Settings → Environment variables → přidat: `ENABLE_OSPF=yes`

Po nastavení proměnné restartujte instanci R2 (pokud k němu nedojde automaticky).

Podrobná dokumentace k FRRouting Docker image je dostupná na:

<https://github.com/maxotta/kiv-psi-frr-docker>

11.2 Volba směrovací cesty a administrativní vzdálenost

Router vybírá výslednou trasu na základě tzv. *administrative distance*. Nižší hodnota má vždy přednost.

Typ routy	Administrative Distance
Connected	0
Static	1
OSPF	110
RIP	120

Z tohoto důvodu je nutné před nasazením OSPF odstranit veškeré dříve nakonfigurované statické routy, jinak by měly přednost před dynamickým směrováním.

11.3 Odstranění statických rout

11.3.1 Router R1 (Cisco)

```
conf t
no ip route 0.0.0.0 0.0.0.0 192.168.1.2
exit
write
```

11.3.2 Router R2 (FRRouting)

```
conf t
no ip route 0.0.0.0/0 192.168.2.2 eth0
no ip route 10.0.0.0/16 192.168.1.1
exit
write
```

11.3.3 Router R3 (Cisco)

```
conf t
no ip route 10.0.0.0 255.255.0.0 192.168.2.1
exit
write
```

11.4 Konfigurace OSPF na R1 (Cisco)

Router R1 inzeruje v OSPF interní síť a spoj mezi R1 a R2.

```
conf t
router ospf 1
network 10.0.0.0 0.0.255.255 area 0
network 192.168.1.0 0.0.0.3 area 0
CTRL + Z
write
```

11.5 Konfigurace OSPF na R2 (FRRouting)

Router R2 funguje jako tranzitní uzel mezi R1 a R3 a inzeruje oba point-to-point spoje.

```
conf t
router ospf
network 192.168.1.0/30 area 0
network 192.168.2.0/30 area 0
CTRL + Z
write
```

11.6 Konfigurace OSPF na R3 (Cisco)

Router R3 distribuuje výchozí trasu do OSPF pomocí příkazu `default-information originate`.

```
conf t
router ospf 1
network 192.168.1.0 0.0.0.3 area 0
network 192.168.2.0 0.0.0.3 area 0
default-information originate
CTRL + Z
write
```

11.7 Ověření funkčnosti OSPF

Správnou funkčnost OSPF lze ověřit následujícími příkazy:

```
show ip ospf neighbor      % stav sousedství
show ip ospf database      % link-state databaze
show ip route ospf         % OSPF routy v tabulce
```

Poznámky:

- `default-information originate` na R3 rozšiřuje default do OSPF, takže R1/R2 získají default přes R3.
- pokud OSPF sousedství nefunguje, zkontroluj masky, MTU, a zda jsou rozhraní UP.

12 Krok 7 — NAT na R3 (Edge router) — kompletní

Na R3 je potřeba označit rozhraní, která jsou **inside** (směrem do vnitřní sítě) a **outside** (směrem k poskytovateli/internetu). V našem příkladu:

- Gi1/0 — vnitřní (směrem k R2) → `ip nat inside`
- Gi0/0 — vnější (DHCP od ISP) → `ip nat outside`

Konfigurace R3

```
conf t
interface GigabitEthernet 1/0
ip address 192.168.2.2 255.255.255.252
ip nat inside
no shutdown
exit

interface GigabitEthernet 0/0
ip address dhcp
ip nat outside
no shutdown
exit

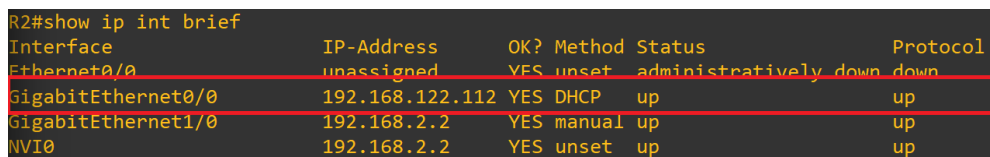
access-list 100 permit ip 192.168.1.0 0.0.0.3 any
access-list 100 permit ip 192.168.2.0 0.0.0.3 any
access-list 100 permit ip 10.0.0.0 0.0.255.255 any

ip nat inside source list 100 interface GigabitEthernet 0/0 overload
exit
write
```

Kontrola přiřazené IP adresy

Po konfiguraci je vhodné ověřit přiřazenou adresu:

```
show ip int brief
```



Interface	IP-Address	OK?	Method	Status	Protocol
Ethernet0/0	unassigned	YES	unset	administratively down	down
GigabitEthernet0/0	192.168.122.112	YES	DHCP	up	up
GigabitEthernet1/0	192.168.2.2	YES	manual	up	up
NVI0	192.168.2.2	YES	unset	up	up

Obrázek 2: Výpis IP rozhraní na R3

Nastavení defaultní trasy

Pro přístup do internetu je potřeba nastavit defaultní trasu směrem k bráně poskytovatele (ISP). Pozor: nejedná se o dosazení přímo IP adresy rozhraní, které R3 získalo přes DHCP, ale o adresu brány v dané podsíti (obvykle poslední nebo první IP v rozsahu).

Příklad:

```
conf t
ip route 0.0.0.0 0.0.0.0 <IP_brany>
exit
write
```

Kde <IP_brany> je adresa gateway poskytovatele (např. pokud R3 získá DHCP adresu 192.168.122.122, pak typická default gateway je 192.168.122.1).

Kontrolní příkazy R3

```
show ip nat translations
show ip nat statistics
show ip int brief
show ip route
```

Co očekávat

- Příkaz `show ip nat translations` by měl zobrazit překlady odchozích spojení klientů.
- Pokud žádné překlady nejsou, ověřte, že klient skutečně posílá odchozí request (např. `ping 8.8.8.8`).

13 Krok 8 — ověření konektivity a testování

Na linuxových klientech proved':

```
# overeni lokalni brany
ping -c 3 10.0.1.254

# overeni souseda R2
ping -c 3 192.168.1.2

# overeni internetu (pres NAT)
ping -c 3 8.8.8.8
ping -c 3 google.com
```

Na Cisco/FRR routerech ověř:

```
show ip interface brief
show ip route
show ip nat translations
show ip dhcp binding
show ip ospf neighbor
show ip ospf database
```