Nefunguje internet

jak najít příčinu výpadku připojení

Petr Krčmář

5. října 2025

O mně

- linuxák od roku 1998
- správce serverů
- lektor a konzultant
- šéfredaktor Root.cz
- člen vpsFree.cz
- organizátor LinuxDays
- můj web je petrkrcmar.cz

ROOT.CZ vpsFree.cz

Prezentace už teď na webu

www.petrkrcmar.cz

Začínáme

Chtěl jsem začít vtipem...

„Pán sedí na záchode“ – ZonerAI

Nejste připojeni k internetu

Zkuste:

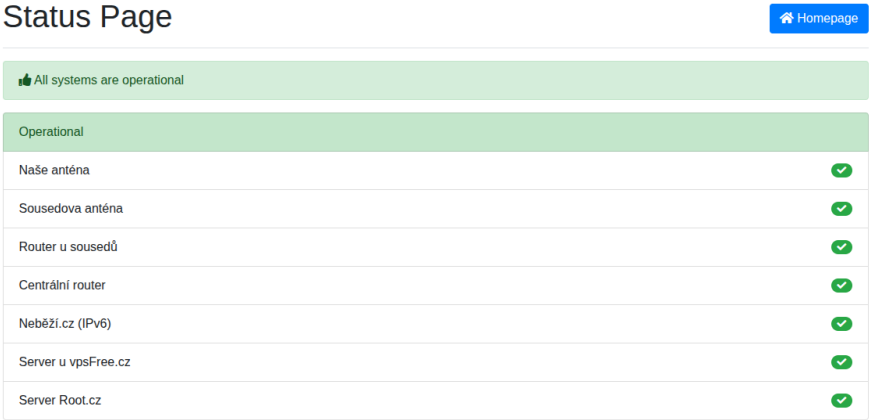
- Zkontrolovat síťové kabely, modem a směrovač
- Obnovit připojení k síti Wi-Fi

ERR_INTERNET_DISCONNECTED

Co je to připojení?

Jak zjistit, že funguje internet?

- internet je decentralizovaná síť různých sítí
- nelze snadno zjistit, že jako celek funguje
- různé nástroje zkoušejí různé cíle
  - Android `connectivitycheck.gstatic.com/generate_204`
  - NetworkManager to má konfigurovatelné v `[connectivity]`
  - GNOME používá `nmcheck.gnome.org`
  - Microsoft má doménu `www.msftconnecttest.com`
  - Apple má doménu `captive.apple.com`
- obecně ale nelze rozlišit mezi chybou připojení a cíle
  - při výpadku služby selžou detekce
  - lze částečně omezit kontrolou více cílů



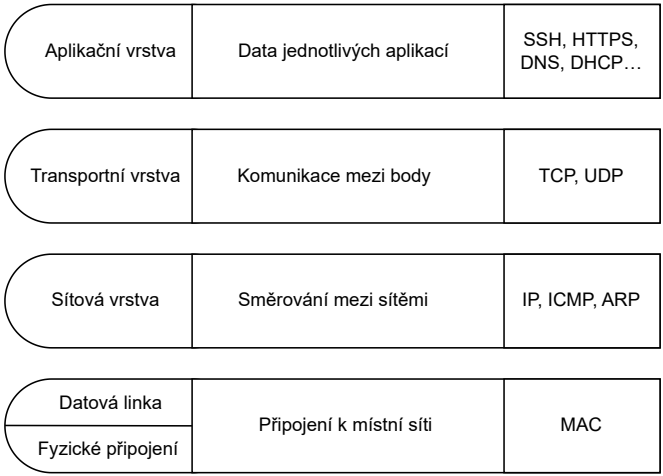
github.com/Cyclenerd/static_status

ROOT.CZ vpsFree.cz

Něco nefunguje, co teď?

- připojení k internetu je široký pojem
- zahrnuje velkou skupinu věcí a technologií
  - fyzické připojení (třeba Wi-Fi)
  - automatická konfigurace (DHCP, SLAAC)
  - adresace uvnitř sítě
  - směrování do ostatních sítí
  - překlad domén na adresy (DNS)
  - firewall a překlad adres (pro IPv4)
- všechno to musí fungovat, aby byl uživatel spokojen
- výpadek různých vrstev má různé dopady
  - i když to vypadá jen, že „to nejde“

Vrstvový model TCP/IP



Síťové vrstvy

Aplikační vrstva	Překlad uživatelských požadavků do síťových zpráv, formátování a zpracování dat. (DHCP, DNS, HTTPS)
Transportní vrstva	Komunikace mezi koncovými body, segmentace dat, řízení přenosu, spolehlivost. (TCP, UDP)
Síťová vrstva	Směrování paketů mezi sítěmi, adresování pomocí IP adres, diagnostika. (IP, ICMP, ARP)
Rozhraní	Fyzické služby pro přenos dat v rámci jedné sítě/přímého spojení. (MAC)

Nebojíme se příkazové řádky

- řádka je náš přítel, rychle dá správné odpovědi
- pro ovládání rozhraní musíme mít práva roota (`sudo`)
  - pro zkoumání situace to obvykle není potřeba
- **nepoužívejte** zastaralé nástroje z balíčku `net-tools`
  - utility jako `ifconfig`, `route`, `netstat`…
  - ve výchozím stavu už nejsou nainstalované (často v návodech)
  - jsou přes dvacet let neudržované a nevyvíjené
  - používají emulované rozhraní ioctl (moderní je netlink)
  - klidně vám bude lhát a tajit některé informace (neví o nich)
    - více IP adres, tunely, VLAN, policy routing…
  - nové síťové funkce jádra v něm nejsou
    - jmenné prostory, řízení provozu, zpracování paketů s XFRM, IPsec…

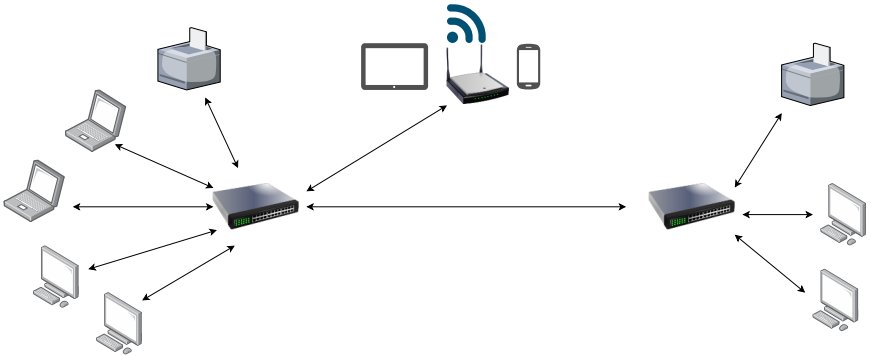
ROOT.CZ vpsFree.cz

Fyzická vrstva

Úkoly fyzické vrstvy

- definice přenosových médií, modulací a napěťových úrovní
- kódování a dekódování bitů do signálu (elektřina, rádio, světlo…)
- stanovení přenosových rychlostí a šířky pásma fyzického média
- určení fyzické topologie (sběrnice, hvězda, kruh…)
- synchronizace přenosu, omezení kolizí, řešení kolizních situací
- detekce chyb způsobených rušením
- fyzická adresace jednotlivých prvků v síti (MAC adresy)
- zabezpečení fyzického přístupu

Schéma sítě Ethernet



Síťové rozhraní

- cesta, přes kterou linuxové jádro posílá a přijímá provoz
  - fyzická – ethernet, Wi-Fi
  - virtuální – loopback, tun/tap (VPN), bridge
- rozhraní musí být ve stavu UP a musí být někam připojeno
- stav zjistíme utilitou `ip` a `nmcli` s NetworkManagerem

Zjištění stavu rozhraní

```
# ip link
# ip -s link
# nmcli device status
```

Když to nefunguje

- zkontrolujte fyzické připojení k síti
  - zda bliká LED na počítači
  - zda bliká LED na druhé straně
  - zda jste asociováni k Wi-Fi síti
- zkuste jiný kabel, ověřte jeho zapojení →
- vyzkoušejte připojit jiné zařízení
- znovu a správně nastavte připojení k Wi-Fi

Fyzické rozhraní

```
# ethtool enp0s3
# nmcli device status
# nmcli radio wifi
```

Síťová vrstva

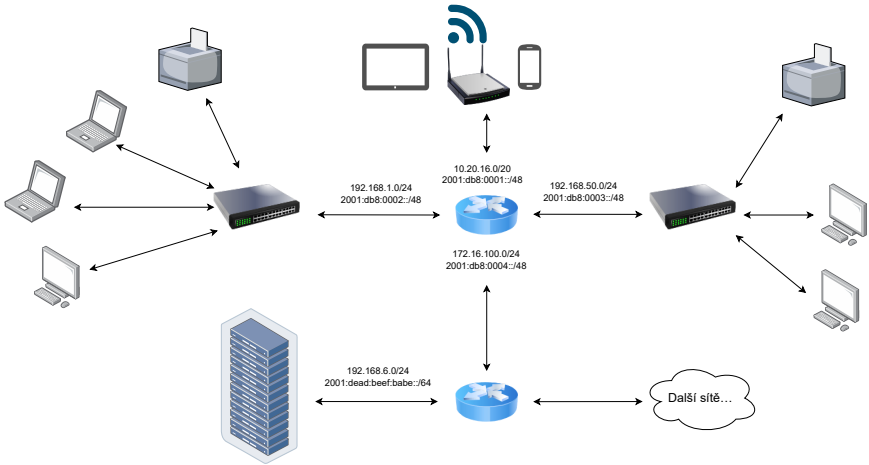
Úkoly síťové vrstvy

- adresace logickou adresou (IPv4, IPv6) pro komunikaci mezi sítěmi
- objevování sousedů v místní síti (ARP, ND)
- adresní plány, dělení na podsítě, překlad adres (NAT)
- udržování směrovacích tabulek pro výběr cesty
- směrování (routing) – výběr rozhraní pro cestu k cíli
- přeposílání paketů (forwarding) – předávání paketů mezi rozhraními
- tunelování provozu – pro přepravu mezilehlými sítěmi (VPN)
- mnoho dalšího: QoS, policy routing, metriky, řízení provozu, směrovací protokoly…

Síťová adresa a prefix

- síťová adresa: identifikátor uzlu a celé podsítě v IP síti
- jedna podsíť = adresy mají společný začátek (prefix) adresy
- prefix se určuje číslem udávající jeho délku v bitech
  - 192.0.2.1/24 označuje za prefix prvních 24 bitů
  - 2001:db8::/32 označuje za prefix prvních 32 bitů
- podle prefixu zjistíme, zda cíl leží ve stejné síti
  - pokud ano, můžeme s ním mluvit přímo na L2
  - pokud ne, musíme komunikaci poslat na prostředníka (směrovač)
- směrovač s námi musí ležet ve stejné síti
  - musí pro nás být přímo dostupný

Schéma IP sítě



IP adresy

- musíme se ujistit, že máme očekávané IP adresy a prefixy
- musejí být ve stejné podsíti jako náš směrovač
- dev – které rozhraní má adresu přidělenou
- inet/inet6 + prefix — určuje síťovou část a velikost podsítě
- scope — zda je adresa lokální, linková nebo globální

IP adresy

```
# ip addr show
# ip -brief addr show
# ip route get 192.0.2.5
```

Směrovací tabulka

- obsahuje seznam cílových prefixů pro směrování
- pro každý záznam je uvedeno rozhraní pro odeslání
- pokud cíl není přímo připojen – next hop
- při shodě se volí záznam s nejdelším prefixem (nejkonkrétnější)
- jeden směr je označen jako výchozí (default) – náš směrovač

Směrovací tabulka

```
# ip route
default via 192.168.1.1 dev enp0s3 proto static metric 100
192.168.1.0/24 dev enp0s3 proto kernel scope link src 192.168.1.10…
```

ROOT.CZ vpsFree.cz

Vyhledání sousedů v síti

- známe IP adresu směrovače – potřebujeme ho kontaktovat
- na místní síti (L2) nepoužíváme IP, ale MAC adresy
  - potřebujeme vytvořit vazbu IP ↔ MAC
- používáme protokoly ARP (IPv4) a ND (IPv6)
  - pošleme všem uzlům dotaz: Kdo má tuhle IP?
  - jeden uzel odpoví a řekne nám svou MAC
- výsledek se ukládá do tabulky sousedů – můžeme komunikovat

Hledání sousedů

```
# arping 192.0.2.1
# ndisc6 2001:db8::1 enp0s3
# tcpdump -i enp0s3 'arp or icmp6'
# ip neighbour show
```

MTU

MTU: Maximum Transmission Unit

- maximální velikost paketu, který lze odeslat přes rozhraní
- známe jen MTU svého rozhraní (u ethernetu obvykle 1500 bajtů)
- paket ale může jít delší cestou, tam MTU neznáme
- Path MTU Discovery (PMTUD) – objevování MTU celé cesty
  - zkouší se odeslat velké pakety a sledují se reakce
  - IPv4: ICMP Type 3 Code 4 (Fragmentation needed)
  - IPv6: ICMPv6 Type 2 (Packet Too Big)
  - v reakci na chybu snížíme hodnotu MTU a pošleme znovu
  - opakuje se, až paket prochází – známe bezpečnou hodnotu

Kdy se to může rozbít?

- PMTUD závisí na zpětných zprávách
  - fragmentation needed a packet too big
- problém nastane při blokaci ICMPv6/ICMP
  - blokace může být na kterékoliv straně
  - obvykle ale není přímo na koncových stranách
  - častěji na síťových prvcích mezi nimi
  - firewall u serveru, špatná konfigurace stacku na serveru
  - CPE u klienta, špatně nastavený operační systém
  - ale taky firewall, NAT, ISP, brány VPN, load balancery…
- dojde k **tiché ztrátě** paketů – vysíláme a nic nedostáváme
- druhá strana informuje o velkých paketech, ale zpráva nedorazí
- kolečko v prohlížeči se točí a my čekáme…

ROOT.CZ vpsFree.cz

Diagnostika problémů s PMTUD

- malé pakety (ping, SSH) nám projdou, velké ne (HTTPS, SFTP)
  - podle uživatele se „internet chová divně“
  - weby se nenačítají celé, něco funguje a něco ne
- obvykle se TCP spojení naváže, ale data netečou
- říká se tomu „spojení do černé díry“

Ověření PMTUD

```
# ping -M do server.example.com -s 1500
# tracepath server.example.com
# tcpdump -i enp0s3 'icmp6 or icmp'
```

Co s tím?

- povolit průchod souvisejících zpráv ICMP a ICMPv6
  - často je ale problém na druhé straně a ten neopravíme
  - musíme zavést opatření u sebe
- snížit MTU na odchozím rozhraní na funkční hodnotu
  - tím ale snížíme efektivitu všech přenosů
- na směrovači můžeme zapnout **TCP MSS clamping**
  - MSS je Maximum Segment Size v paketech TCP SYN
  - pole určující maximální velikost TCP datové části
  - MSS = MTU IP vrstvy − IP hlavička (20 B) − TCP hlavička (20 B)
  - při navazování spojení ho přepíšeme na MSS linky – 40

MSS TCP clamping

```
# iptables -t mangle -A FORWARD -p tcp --tcp-flags SYN,RST SYN \
           -j TCPMSS --clamp-mss-to-pmtu
# nft add rule ip filter forward tcp flags syn tcp option maxseg size set rt mtu
```

Aplikační vrstva

Poslouchá mi proces?

- na aplikační vrstvě komunikují procesy s procesy
- UDP a TCP přidávají pro identifikaci **porty**
  - číslo 0 až 65535 identifikující jednotlivé procesy
- server má fixní předvídatelné číslo portu (obvykle do 1024)
  - poslouchá trvale, obsluhuje mnoho klientů
- klient má náhodný dočasný port (vysoké číslo)
  - využívá dočasně, po zavření je port recyklován

Poslouchající porty a procesy

```
# ss -tulpn
```

DNS

- překlad doménových jmen na IP adresy (A/AAAA) a další záznamy
- různé prvky v hierarchii DNS
  - autoritativní server – drží data o doménách
  - rekurzivní server – shání data od autoritativních
  - pahýlový (stub) resolver – klientská strana, v operačním systému
- používá TCP a UDP porty 53, dotaz-odpověď protokolem DNS
- rekurzivní server je obvykle u našeho poskytovatele
  - v koncových zařízeních je nastavená jeho IP
  - může být i u nás ve směrovači (často přeposílač)
- existují i veřejné rekurzivní servery
  - Cloudflare 1.1.1.1, 2606:4700:4700::1111
  - Google 8.8.8.8, 2001:4860:4860::8888
  - Quad9 9.9.9.9, 2620:fe::9
  - ODVR 193.17.47.1, 2001:148f:ffff::1

Jaký používám DNS resolver?

- v systému (stub resolveru) je nastaven resolver
- na něj se posílají všechny dotazy k vyřízení
- liší se v distribucích se systemd-resolved
  - stub resolver je namířen na localhost
  - tam poslouchá místní resolver (kešuje, validuje, mDNS…)

Zjištění resolveru

```
# cat /etc/resolv.conf
# resolvectl
# ss -tulpn | grep 53
# nslookup www.example.com
```

ROOT.CZ vpsFree.cz

Jak ověřím funkčnost?

- v odpovědi je také stav – jak to dopadlo
  - NOERROR – úspěch!
  - NXDOMAIN – jméno neexistuje
  - SERVFAIL – chyba komunikace
  - REFUSED – odmítnuto serverem
  - FORMERR – chyba interpretace
  - NOTIMP – operace není interpretovaná
- pozor na DNSSEC – chyba v podpisech rozbije doménu
  - validaci lze vypnout pomocí příznaku CD (Checking Disabled)

Pohled do DNS

```
# dig www.example.com @1.1.1.1
# dig +cd www.rhybar.cz
```

Typické problémy

- ping na IP funguje, jméno nefunguje
  - problém je jednoznačně v překladu jmen
- dostávám odpovědi SERVFAIL
  - server je nedostupný
- překlad DNS trvá dlouho
  - resolver je přetížený
- dostávám odpovědi NXDOMAIN
  - chyba v konfiguraci, nebo máte špatné jméno
- vyzkoušejte nástroj `dig` proti různým serverům
  - pokud váš resolver nefunguje, vyberte si jiný

DHCP

- Dynamic Host Configuration Protocol
  - protokol pro automatické přidělování síťových parametrů
- umožňuje informovat klienty o zvycích v místní síti
  - IP adresa, maska, brána, MTU, DNS, NTP…
- běží na aplikační vrstvě v UDP (klient 67, server 68)
  - používá broadcast na oslovování serveru
  - zprávy DHCPDISCOVER, DHCPOFFER, DHCPREQUEST, DHCPACK
- ekvivalentem v IPv6 je bezestavový protokol SLAAC
  - součástí ICMPv6, DNS je v rozšíření RDNSS

Pohled do DHCP

```
# tcpdump -i enp0s3 -vvv 'port 67 or port 68'
```

Typické problémy v DHCP

- klient nedostává žádné odpovědi od serveru
  - chyba na fyzické vrstvě, špatná konfigurace DHCP serveru
  - zkontrolujte připojení a nastavení serveru
- klient nedostává IP adresu
  - vyčerpaná zásoba adres
  - rozšiřte pool, zkraťte prefix či dobu zápůjčky
- klient má konfliktní IP adresu
  - DHCP má statické příděly uvnitř poolu
  - přeadresujte tak, aby ke kolizím nedocházelo
- klient nedostává další informace
  - chyba v konfiguraci DHCP serveru
  - ověřte odpovědi pomocí `tcpdump` a `dhclient`

Komunikace s DHCP

```
# dhclient -v -1
```

Kde je problém?

Hledání žáby na prameni

- chceme zjistit místo způsobující problém
  - lokální zařízení, domácí síť, ISP, internet
- musíme postupovat od blízkého zařízení směrem ven
- spojení na směrovač, prvek poskytovatele, body v internetu
- sledujeme dostupnost, ztrátovost paketů, rychlost přenosu

Užitečné nástroje

```
# mtr server.example.com
# iperf3 -c ping.online.net -u -b 10M -t 20
# speedtest-cli
```

ROOT.CZ vpsFree.cz

Otázky?

Petr Krčmář
petr.krcmar@iinfo.cz