

Úvod do informačních technologií

počítačové sítě

Martin Trnečka

Katedra informatiky
Univerzita Palackého v Olomouci

Motivace

- jak funguje Internet?
- Internet = největší systém vytvořený lidstvem
- Q: Lze jej jednoduše popsat? A: Ano.
 - popis hardware a software
 - popis komunikace
- spoustu technických detailů zamlčíme a některé aspekty výrazně zjednodušíme
→ základní přehled jak to funguje

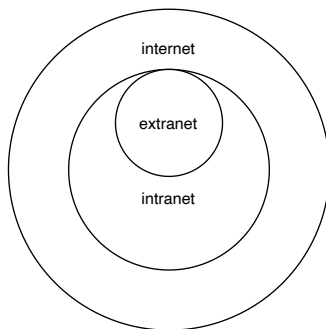
Počítačová síť

- počítačová síť obecně:
 - uzly
 - fyzické propojení uzlů (síťové rozhraní, přenosové médium, síťové prvky)
 - komunikace mezi uzly
 - realizace (síťových) služeb (sídelní hardware, software a dat, komunikace)
- příklad: počítačová síť Internet (WWW, DNS, e-mail)
- uzly
 - hostitelské uzly, hostitelé, koncové systémy
 - počítače, celá řada dalších zařízení
 - *Internet of things* (IoT)

Klasifikace počítačových sítí

- internet (psáno s malým „i“)
 - vnější síť
 - propojení více různých sítí
- intranet
 - vnitřní síť
 - požadavky na bezpečnost
- extranet
 - část vnitřní sítě přístupná z internetu

Klasifikace počítačových sítí



Klasifikace počítačových sítí

- dle rozsahu (velikosti)
 - Personal Area Network (PAN)
 - Local Area Network (LAN)
 - Campus Area Network (CAN)
 - Metropolitan Area Network (MAN)
 - Wide Area Network (WAN)
- dle topologie (propojení)
 - hvězdicová
 - kruhová
 - sběrníková
 - a další
- dle přenosového média
 - drátové (metalické, optické)
 - bezdrátové (radiový signál)
- dle rychlosti

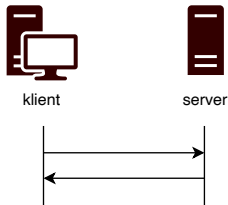
Komunikace v počítačové síti

- veškeré síťové služby jsou realizovány prostřednictvím komunikace mezi uzly
- komunikace = zasílání zpráv
- uzel sítě komunikuje s jedním či více uzly
 - *unicast* – uzel komunikuje s uzlem
 - *multicast* – uzel komunikuje se skupinou uzlů
 - *broadcast* – uzel komunikuje se všemi uzly v (lokální) síti
- realizace komunikace:
 - *přepínání okruhů*
 - *přepínání paketů* (Internet)
- poznámka: pojem paket budeme používat nepřesně
- obecně složitý proces → dělení na menší části

Přenos dat

- parametry
 - rychlost
 - spolehlivost
- zprávy jsou rozděleny na pakety
- pakety (fyzicky) přenášeny po bitech
- metoda uložit a odešli
 - dokud neobdržíme celý paket data ukládáme do bufferu → zpoždění
 - více zdrojů = fronta → zpoždění
 - zaplnění fronty = ztráta paketu
- odbočka: zpoždění šíření, zpoždění zpracování, ...

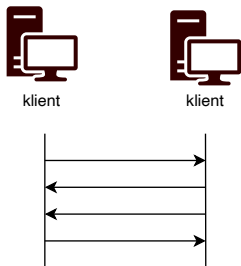
Architektury služeb v počítačové síti



■ *klient-server*

- klient žádá server o poskytnutí služby
- nerovnocenné role
- centralizace → slabé místo
- *proxy server* = prostředím mezi klientem a serverem
- např. prohlížení webové stránky

Architektury služeb v počítačové síti



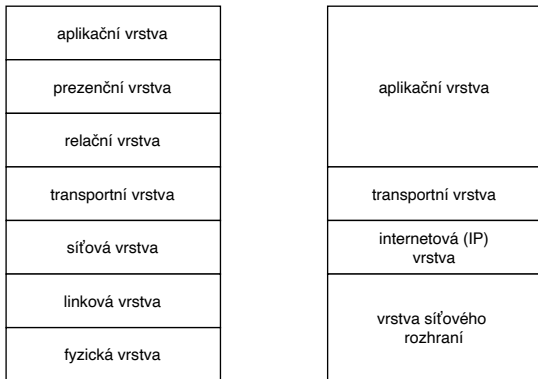
■ *peer-to-peer (P2P)*

- se serverem (hybridní) i bez
- rovnocenné role uzlů
- decentralizace
- např. sdílení souborů přes tzv. *torrent síť*

Síťový model

- abstrakce nad procesem komunikace
- rozdělení na menší části tzv. *vrstvy* (obecný designový princip)
- vrstva:
 - poskytuje služby vyšší vrstvě
 - používá služeb nižší vrstvy
- vrstvy popisují různé části komunikace
- nejběžnější modely:
 - OSI (abstraktní, referenční)
 - TCP/IP (Internet)
- abstrakce → klíčová
- vrstvy jsou nezávislé → robustnost (implementace vrstvy je nezávislá na ostatních vrstvách)

Síťový model



Obrázek: Porovnání modelů OSI a TCP/IP

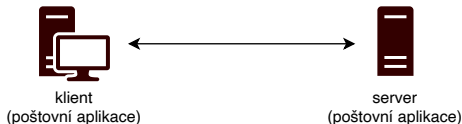
Protokol

- vrstvy jsou tvořeny *protokoly*
- protokol = množina jasně daných pravidel
- analogie protokolu v lidské komunikaci (např. „dobré chování“)
- komunikace pouze mezi sousedními vrstvami
- standardy a standardizace
- Internetové síťové standardy – RFC (Request For Comments), dostupné na <https://www.rfc-editor.org/>

TCP/IP

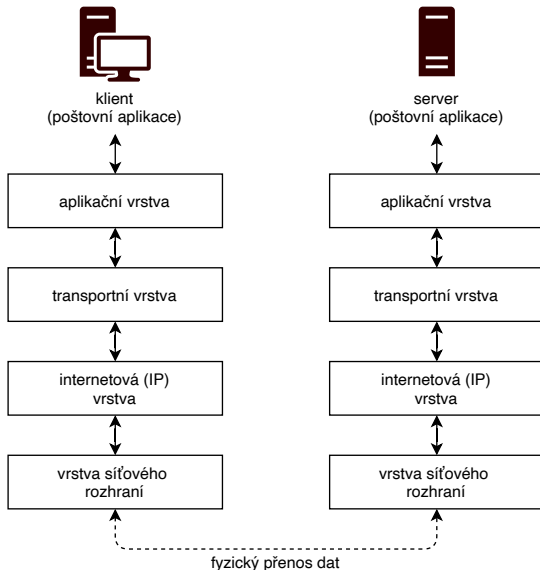
- Transmission Control Protocol/Internet Protocol
- počítačová síť → TCP/IP architektura
- TCP/IP dělení na 4 vrstvy
 - aplikační
 - transportní
 - internetová
 - síťového rozhraní

TCP/IP: Komunikace

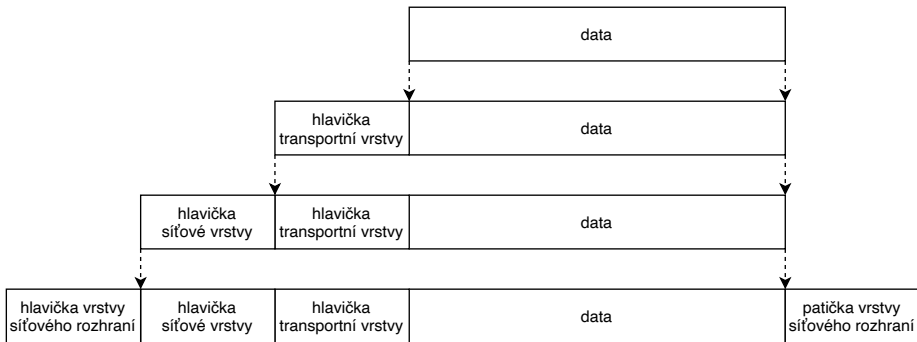


- analogie: posláání zprávy mezi aplikacemi na dvou počítačích = posláání dopisu (zpráva) obyvatelem (aplikace) jednoho domu (počítač) obyvatelem (jiná aplikace) jiného domu (jiný počítač)
- potřebujeme zajistit (zjednodušeno):
 - formát vyměňovaných dat
 - identifikaci (adresaci) komunikujících aplikací
 - adresaci uzlů v síti
 - identifikaci konkrétních síťových rozhraní
 - přenos dat skrze síť

TCP/IP: Komunikace



TCP/IP: Komunikace mezi vrstvami



- hlavička a patička = data potřebná pro funkci dané vrstvy
- „balení“ a „vybalování“
- na koncových uzlech i síťových zařízeních

Aplikační vrstva

- aplikační protokoly
- popisují formát (podobu) vyměňovaných dat a další
- řeší zabezpečení (ostatní vrstvy řeší pouze okrajově)
 - TCP/IP původně neřešila bezpečnost vůbec
 - dodatečně „záplatováno“
 - → Internet je nebezpečný
- aplikační protokol = *služba*
- např. HTTP(S), DNS, (S)FTP, SSH, IMAP(S), SMTP(S), ...
- napojení na aplikace: implementace protokolu + *síťový soket* (poskytovaný OS)
- příklad: e-mailový klient
- k aplikačním protokolům se vrátíme později

Transportní vrstva

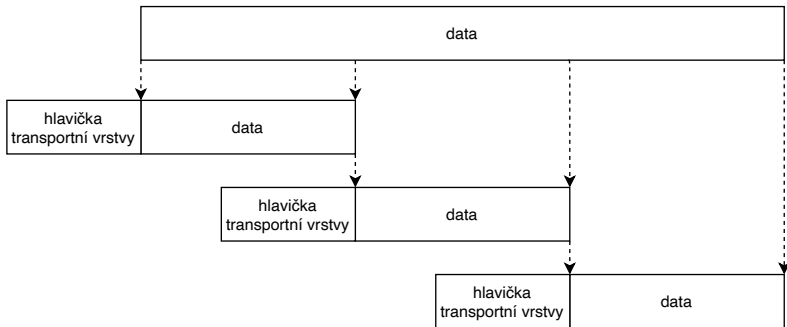
- předávání dat mezi aplikacemi (identifikace aplikací v rámci uzlu)
- *port*
 - číslo 0–65535
 - ≤ 1023 vyhrazené (privilegované), dáno standardy
 - například: 80 pro webovou službu
- dva typy služeb:
 - *Transmission Control Protocol* (TCP)
 - *User Datagram Protocol* (UDP)
- TCP i UDP identifikace pomocí portu
- značení: číslo/tcp
- zabezpečení SSL/TLS (mezivrstva mezi transportní a aplikační vrstvou)

Protokol TCP

- data ve formě *segmentů* → *segmentace dat*
- *spolehlivá spojová služba*
 - navazuje a udržuje spojení mezi uzly (režie, potvrzování) → spojení musí být ukončeno
 - zajišťuje doručení dat (řeší ztráty segmentů, potvrzení přijetí segmentu a další)
- klient-server architektura
- zajišťuje řízení toku sítě
- zajišťuje integritu dat → kontrolní součet
- hlavička protokolu: zdrojový a cílový port, číslo segmentu, číslo potvrzeného segmentu, příznaky (a další)

Protokol TCP: Segmentace

- převádí data z aplikační vrstvy na *segmenty*
- proud dat, *segmentace*



Protokol UDP

- data ve formě datagramů (nutnost manuálního dělení na aplikační vrstvě)
- *nespolehlivá nespojová služba*
 - nevytváří spojení
 - nezajišťuje doručení dat
 - nelze řídit tok dat
- nízká režie
- hlavička protokolu: zdrojový a cílový port (a další)

Internetová (IP) vrstva

- identifikace uzlů v síti → *IP adresa*
- směrování mezi nesousedními uzly (skrže internet)
- data se přenáší ve formě (IP) paketu
- služební protokoly pro hlášení chyb a diagnostiku (ICMP)

IP adresa

- uložena v hlavičce IP protokolu
- IPv4 (32 bitů), IPv6 (128 bitů)
- příklad (`phoenix.inf.upol.cz`):
 - 158.194.80.13
 - 2001:718:1401:50:0:0:0:0d, zkrácený formát 2001:718:1401:50::0d
- Internet je síť sítí → hierarchie
- lokální adresy (používané v lokálních sítích) a veřejné adresy (ostatní)
- *IP adresa sítě* a *IP adresa uzlu*
 - logické a praktické rozdělení
 - hierarchické směrování

IP adresa

- *maska sítě* = rozdělení na adresu sítě a adresu v síti (adresa síťového rozhraní)
- příklad:
 - adresa sítě 192.168.1.0
 - maska sítě: 255.255.255.0
 - adresy v síti: 192.168.1.1–192.168.1.254
 - 192.168.1.255 vyhrazena pro broadcast
- používanější CIDR (Classless Inter-Domain Routing) formát 192.168.1.0/24

adresa sítě 192.168.1.0/24

192								168								1								0							
1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0

maska sítě

255								255								255								0							
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0

IP adresa

adresa sítě 192.168.0.0/16

192								168								0								0							
1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

první adresa v síti 192.168.0.0/16

192								168								0								1							
1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1

...

poslední adresa v síti 192.168.0.0/16

192								168								255								254							
1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0

broadcast v síti 192.168.0.0/16

192								168								255								255							
1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

IP adresa

adresa sítě 192.168.192.0/18

192								168								192								0							
1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0

první adresa v síti 192.168.192.1/18

192								168								192								1							
1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	1

poslední adresa v síti 192.168.255.254/18

192								168								255								254							
1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0

broadcast v síti 192.168.255.255/18

192								168								255								255							
1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

maska sítě

255								255								192								0							
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Odbočka: Princip tvorby podsítí

- síť lze dále dělit na podsítě
- síť lze spojovat do větších sítí (agregace)
- manipulace s maskou sítě

adresa sítě 192.168.0.0

192								168								0								0							
1	1	0	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

původní maska sítě /16

255								255								0								0							
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

nová (prodloužená) maska sítě /18

255								255								192								0							
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Speciální IP Adresy

IP adresa	popis
127.0.0.1	zpětná smyčka (loopback)
10.0.0.0/8	adresa lokální sítě
172.16.0.0/12	adresa lokální sítě
192.168.0.0/16	adresa lokální sítě
192.168.0.0/24	adresa lokální sítě

Odbočka: Omezení IPv4

- omezený (teoretický) maximální rozsah ($2^{32} = 4\,294\,967\,296$)
- pro lokální síť dostatečný
- správa veřejných adres:
 - Internet Assigned Numbers Authority (IANA)
 - Regional Internet registry (RIR)
 - provideři
- IPv4 adresy již došli (na několika úrovních)
- IPv6: obtížně zapamatovatelné, IP adresy vnitřní a vnější síť lze oddělit (NAT), poskytovatelé neinvestují do infrastruktury
- poznámka: IPv6 nepoužívá masku, ale délku prefixu (zkráceně prefix), jinak stejné

Odbočka: Přidělení IP adresy uzlu

- statické
 - manuální konfigurace
- dynamické
 - DHCP protokol
 - klient-server služba
 - server zašle uzlu údaje pro konfiguraci síťového rozhraní

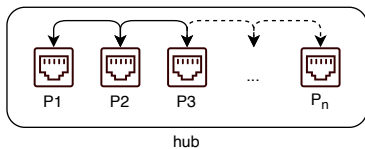
Vrstva síťového rozhraní

- řeší fyzický přenos dat a přenosová média
- linková část (přenos v rámci LAN pomocí *rámců*) a fyzická část (přenos signálu po jednotlivých bitech)
- různé typy přenosu (analogový, digitální)
- identifikace fyzického rozhraní: *MAC adresa*
- například 01:23:45:67:89:ab
- lze změnit
- přenosové medium:
 - kroucená dvojlinka (Cat 5e, Cat 6, Cat 6a, Cat 7 a další, konektor RJ45)
 - optické vlákno
 - prostor

Struktura počítačové sítě

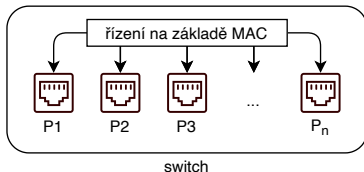
- uzly sítě
- přenosové médium
- repeatery (opakovače)
- huby (rozbočovače)
- switche (přepínače)
- routery (směrovače)
- modemy
- a další

Hub



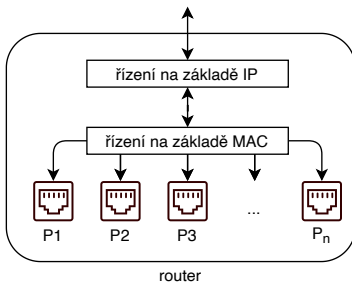
- „rozbočení“ komunikace
- každý komunikuje s každým (nelze jinak)
- nebezpečí odposlechu
- funguje na fyzické části vrstvy síťového rozhraní (přenáší data po bitech)
- repeater = „jednoportový hub“

Switch



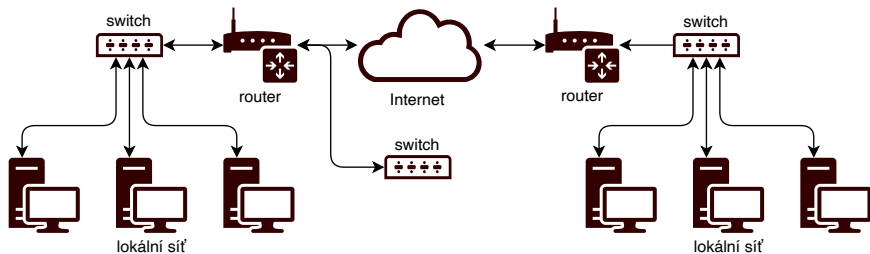
- řízené „rozbočení“ komunikace (switch se sám naučí)
- funguje na linkové části vrstvy síťového rozhraní (data se přenáší po rámcích)
- každý komunikuje s každým (lze nastavit)
- promiskuitní režim síťového rozhraní
- poznámka: bridge

Router



- obsahuje obvykle switch (přesněji, zařízení pracující na Internetové vrstvě)
- umožňuje směřovat komunikaci mimo lokální síť

Komunikace v síti



■ směrování v lokální síti

- na úrovni linkové vrstvy = stačí MAC adresa
- známe IP adresu → musíme získat MAC adresu (protokol ARP)

■ směrování mimo lokální síť

- na úrovni internetové vrstvy = IP adresa
- *směrovací tabulka* určuje kam poslat IP paket dál tzv. *next hop*
- statická a dynamická změna tabulky

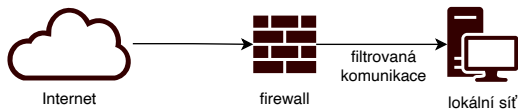
Odbočka: Připojení počítačů do lokální sítě

- fyzické propojení
- stejná adresa sítě (statická či dynamická konfigurace)
- různé adresy v síti (statická či dynamická konfigurace)
- různé MAC adresy
- přístup k internetu (Internetu) výchozí brána (gateway)
- překlad doménových jmen (vysvětlíme později)

Ochrana lokální sítě

■ firewall

- filtrace síťové komunikace
- na základě IP
- na základě čísla portu
- obvykle součást OS, případně speciální zařízení

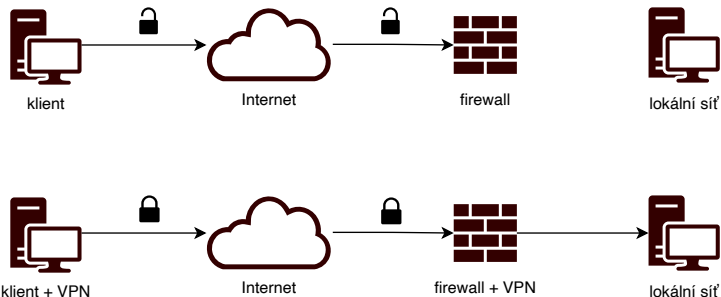


■ Network Address Translation (NAT)

- adresy v síti jsou maskovány za adresu přístupového bodu do nadřazené sítě

Virtual Private Network (VPN)

- šifrované propojení sítí či klienta a sítě skrze nebezpečnou síť
- klient je součástí lokální sítě → výhody
- komunikace je šifrována (nikoliv anonymní)
- vlastní, případně řada poskytovatelů (pozor na bezpečnost)



Wi-Fi

- WLAN
- z pohledu TCP/IP → vrstva síťového rozhraní
- jiný typ rámce
- sdílené medium
 - problém s kolizemi
 - různé metody řešení
- protokol: 802.11, různé verze (např. b, g, n, ac, ax): rychlost, parametry sítě, podpora zařízení → složité, zavedení Wi-Fi X, $X \in \{5, 6, 6E, 7\}$

Wi-Fi router

- router, běžněji access point (AP)
- navíc bezdrátové síťové rozhraní
- běžné zařízení
- různá kvalita, různá cena
- počet klientů
- základní Wi-Fi routery → rozsáhlé nastavení
 - jméno sítě
 - parametry sítě (přenos, šifrování)
 - dynamická konfigurace
 - firewall

Název sítě

- SSID
- například: eduroam
- název sítě lze skrýt, uživatel musí znát, aby se připojil (možnost hide SSID)
- skryté SSID \neq zabezpečení

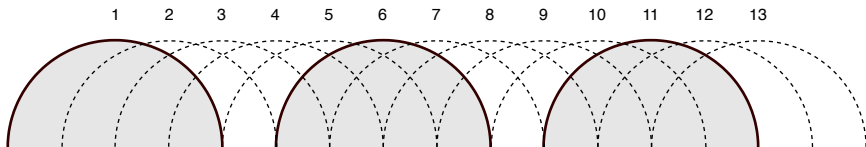
Parametry sítě (fyzický přenos)

■ pásmo:

- 2,4 GHz, 5 GHz, 6 GHz
- vyšší frekvence = rychlejší přenos, menší dosah, náchylnější na rušení

■ kanál:

- počet kanálů závisí na zemi
- 2,4 GHz, 13 překrývajících se kanálů
- 5 GHz, (ČR) 25 nepřekrývajících se kanálů
- výběr → chceme volný kanál, nepřekrývající se kanál, kanál s co nejméně AP



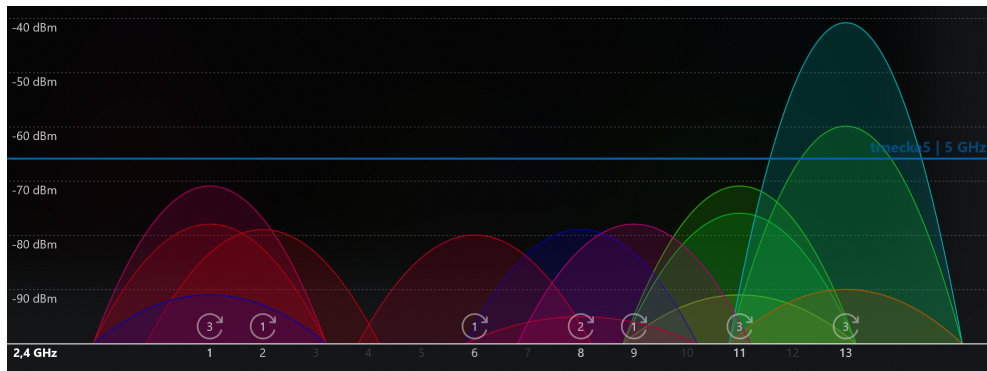
Obrázek: Rozložení kanálů v 2.4 GHz.

Parametry sítě (fyzický přenos)

- šířka kanálu: 20 MHz, 40 MHz, 80 MHz (5 GHz), 160 MHz (6 GHz), větší šířka → větší propustnost, některé zařízení nemusí podporovat)
- výkon vysílače (ne vždy lze ovlivnit)
- signál/šum (jednotka -dBm, 0–100), typicky: -60dBm/-90dBm, čím blíže 0 tím lépe (u šumu naopak)
- kvalita signálu (SNR) rozdíl mezi signálem a šumem (jednotka dB): 40dB a více kvalitní signál (čárky na ikoně)

Ukázka

- Wi-Fi Analyzer (Windows)
- řada nástrojů pro různé OS (Windows, Linux, macOS, Android, ...)
- specializovaný hardware



Obrázek: Wi-Fi síť v pásmu 2,4 GHz.

Parametry sítě (bezpečnost)

■ šifrování:

- žádné (veřejné Wi-Fi) → velmi nebezpečné
- WEP → prolomitelné = nedostatečné
- WPA → bezpečnostní problémy, lze prolomit slovníkovým útokem
- WPA2 → bezpečnostní problémy, lze prolomit slovníkovým útokem
- WPA3 → malá podpora, bezpečnostní problémy

■ heslo:

- TKIP (WPA)
- AES (WPA2)

■ autentifikace:

- PSK (heslo)
- EAP (autentifikační server, obvykle firemní infrastruktura, některé Wi-Fi routery nepodporují)

WPS

- tlačítko na Wi-Fi routeru
- automatické připojení do Wi-Fi sítě pomocí PIN
- velice nebezpečné (zejména u starších routerů) → lze odposlechnout a prolomit

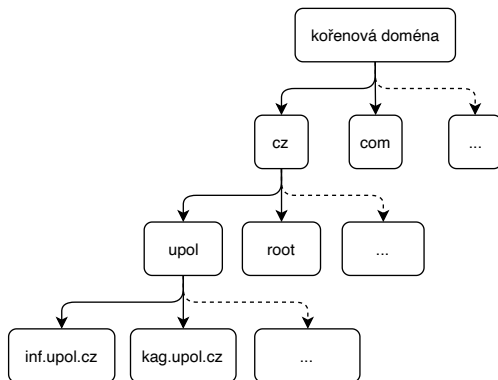
Odbočka: Jak vylepšit signál?

- opakovače
- mesh
- kabel

Doménové jméno

- IP adresy
 - obtížně zapamatovatelné
 - zachycují fyzickou strukturu
- logická struktura → doménové jméno
- příklad: `phoenix.inf.upol.cz`
- služba DNS
 - překlad doménového jména na IP adresu (a obráceně, bezpečnost)
 - `phoenix.inf.upol.cz` → `158.194.80.13`
 - decentralizovaná služba (systém DNS)
 - řeší resolver (součást OS), který předává řízení DNS resolver serveru
- struktura: standardně ASCII znaky, omezená délka, oddělovač: . (tečka), běžně: 1. řádu, 2. řádu, ...
- nákup doménových jmen

Hierarchie doménových jmen



Obrázek: Hierarchie doménových jmen

- doména (zóna) spravována jmenným serverem
- top-level domény (generické a národní): edu, com, gov, org, info, ...

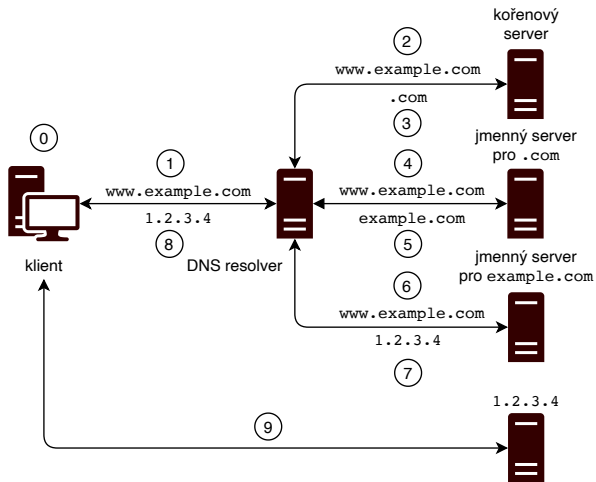
DNS servery

- primární:
 - každá doména má právě 1 primární server
 - autoritativní odpověď o dané doméně
- sekundární:
 - záloha primárního
 - každá doména má alespoň 1 sekundární server
 - autoritativní odpověď o dané doméně
- cache:
 - často součástí primárních a sekundárních, ale mohou být i samostatné
 - neautoritativní odpověď

Překlad doménového jména na IP

- formou dotazu
- dotazování:
 - klient (řeší resolver)
 - klient žádá DNS resolver server
- dva typy dotazů:
 - rekurzivní (vyřešení dotazu)
 - nerekurzivní (předání na jiný server)

Překlad doménového jména



Překlad jména (řešení dotazu)

- ① klient chce zjistit IP adresu ke jménu `www.example.com`, klient prohledá svoji cache zda nezná odpověď
- ① klient pošle *rekurzivní dotaz* na DNS resolver (musí být nastaven), pokud DNS resolver zná odpověď (má ji v chache) pošle jí klientovi
- ② pokud lokální jmenný server nezná odpověď pošle *nerekurzivní dotaz* na kořenový jmenný server
- ③ kořenový jmenný server nezná odpověď, ale ví kdo je zodpovědný za doménu `com` v dotazu, pošle DNS resolveru jeho adresu
- ④ DNS resolver pošle *nerekurzivní dotaz* na jmenný server spravující doménu `example.com`

Překlad jména (řešení dotazu)

- ⑤ jmenný server zodpovědný za doménu `example.com` nezná odpověď, ale ví kdo je zodpovědný za doménu `example.com`, pošle DNS resolveru jeho adresu
- ⑥ DNS resolver pošle *nerekurzivní dotaz* na jmenný server spravující doménu `example.com`
- ⑦ jmenný server spravující doménu `example.com` zná odpověď (`1.2.3.4`) a pošle ji DNS resolveru
- ⑧ DNS resolver předá `1.2.3.4` klientovi a uloží si údaje do cache
- ⑨ klient uloží `1.2.3.4` do cache a kontaktuje `1.2.3.4`

Reálně

- situace je mnohem komplikovanější
- řada typů jmenných serverů
- časové omezení na vyřešení dotazu
- update informací na serverech
- problém s cache
- veřejné DNS resolvers
 - 8.8.8.8 (Google)
 - 1.1.1.1 (Cloudflare)
 - 193.17.47.1 a 185.43.135.1 (cz.nic)

Elektronická pošta

- odesílání a příjem e-mailu
- mailbox
- odeslání: SMTP(S) (Simple Mail Transfer Protocol)
- příjem: IMAP4(S) (Internet Message Access Protocol), zastaralý POP3 (Post Office Protocol)
- hlavička e-mailu
- bezpečnost, spam

Vzdálené přihlašování

■ SSH (Secure Shell)

- použití: `ssh [user@]hostname[:port]`
- PuTTY (pro Windows)

```
ssh phoenix.inf.upol.cz  
ssh trnecka@phoenix.inf.upol.cz
```

■ SCP (Secure Copy)

- použití: `scp zdroj cil`
- adresace `[user@]hostname:cesta`
- WinSCP (grafická varianta pro Windows)

```
scp trnecka@phoenix.inf.upol.cz:~/ ./soubor.txt  
scp ./soubor.txt trnecka@phoenix.inf.upol.cz:~/
```

- RDP (Remote Desktop Protocol, Windows), vzdálená plocha, grafický
- VNC, vzdálená plocha, grafický

Základní nástroje

- program ping
 - odezva uzlu v síti
 - může být blokován
 - `ping www.inf.upol.cz`
- program traceroute (Linux) a tracert (Windows)
 - analýza cesty v síti

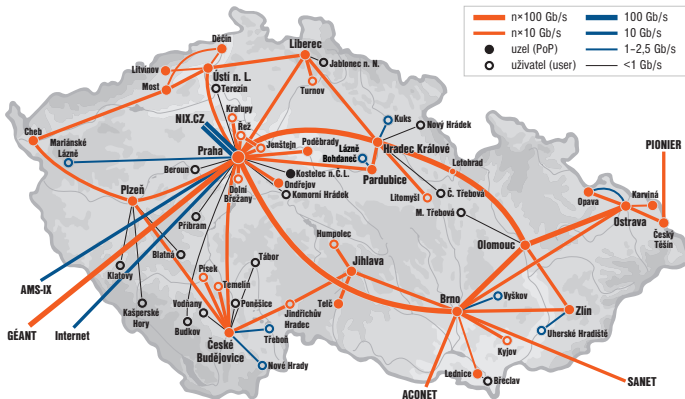
Základní nástroje

```
trneckam — -zsh — 80x24

Last login: Thu Mar 18 07:52:04 on console
[trneckam@Martin-MacBook-Air ~ % ping 158.194.80.13
PING 158.194.80.13 (158.194.80.13): 56 data bytes
64 bytes from 158.194.80.13: icmp_seq=0 ttl=59 time=4.159 ms
64 bytes from 158.194.80.13: icmp_seq=1 ttl=59 time=3.566 ms
64 bytes from 158.194.80.13: icmp_seq=2 ttl=59 time=3.528 ms
64 bytes from 158.194.80.13: icmp_seq=3 ttl=59 time=3.497 ms
^C
--- 158.194.80.13 ping statistics ---
4 packets transmitted, 4 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 3.497/3.688/4.159/0.273 ms
[trneckam@Martin-MacBook-Air ~ % traceroute 158.194.80.13
traceroute to 158.194.80.13 (158.194.80.13), 64 hops max, 52 byte packets
 1  10.144.32.1 (10.144.32.1)  16.435 ms  20.397 ms  14.479 ms
 2  158.194.2.65 (158.194.2.65)  3.199 ms  3.451 ms  3.104 ms
 3  158.194.110.1 (158.194.110.1)  18.926 ms  19.984 ms  24.312 ms
 4  ugw-idp1-m510.upol.cz (158.194.254.65)  14.877 ms  22.472 ms  27.248 ms
 5  prf-gw.upol.cz (158.194.203.126)  4.856 ms  5.181 ms  8.065 ms
 6  phoenix.inf.upol.cz (158.194.80.13)  4.219 ms  3.957 ms  3.548 ms
trneckam@Martin-MacBook-Air ~ %
```

CESNET2

- národní vysokorychlostní počítačová síť pro vědu a vzdělávání
- www.cesnet.cz



Obrázek: Mapa síť CESNET2, 2018.

- správce CZ domény
- `nic.cz`

Síť Internet

- Internet = síť sítí
- lokální síť (uživatelé)
- uživatelé propojeni přes ISP (Internet Service Provider)
- více úrovní ISP (přístupové, regionální, globální)
- propojení skrze PoP (Points of Presence)
- propojení více ISP na stejné úrovni = peering
- IXP (internet Exchange Point), peeringové centrum, např. nix.cz
- poskytovatelé obsahu