

Počítačové sítě

Minimum "síťariny", která si nečiní nárok na úplnost a některé věci vědomě zamlčuje

Důležité pojmy a jejich význam

- Počítačová síť
- IP adresa
- NAT
- DNS
- DHCP
- Masky sítě, brána
- ping
- MAC
- Služba
- Port

Počítačová síť

Počítačová síť

Počítačová síť je **system propojených zařízení, která si vyměňují data.**

Tvoří ji soubor propojených počítačů a dalších zařízení umožňující **sdílení dat, zdrojů a komunikaci.** Hlavní složky:

- **Uzly (nodes)** – počítače, servery, tiskárny, routery, switche
- **Komunikační médium**
 - kabelové – metalické, optické
 - bezdrátové – Wi-Fi, Bluetooth
- **Síťový hardware** – směrovače (routery), přepínače (switche), síťové karty
- **Síťové protokoly** – pravidla pro komunikaci (např. TCP/IP)

Typy sítí

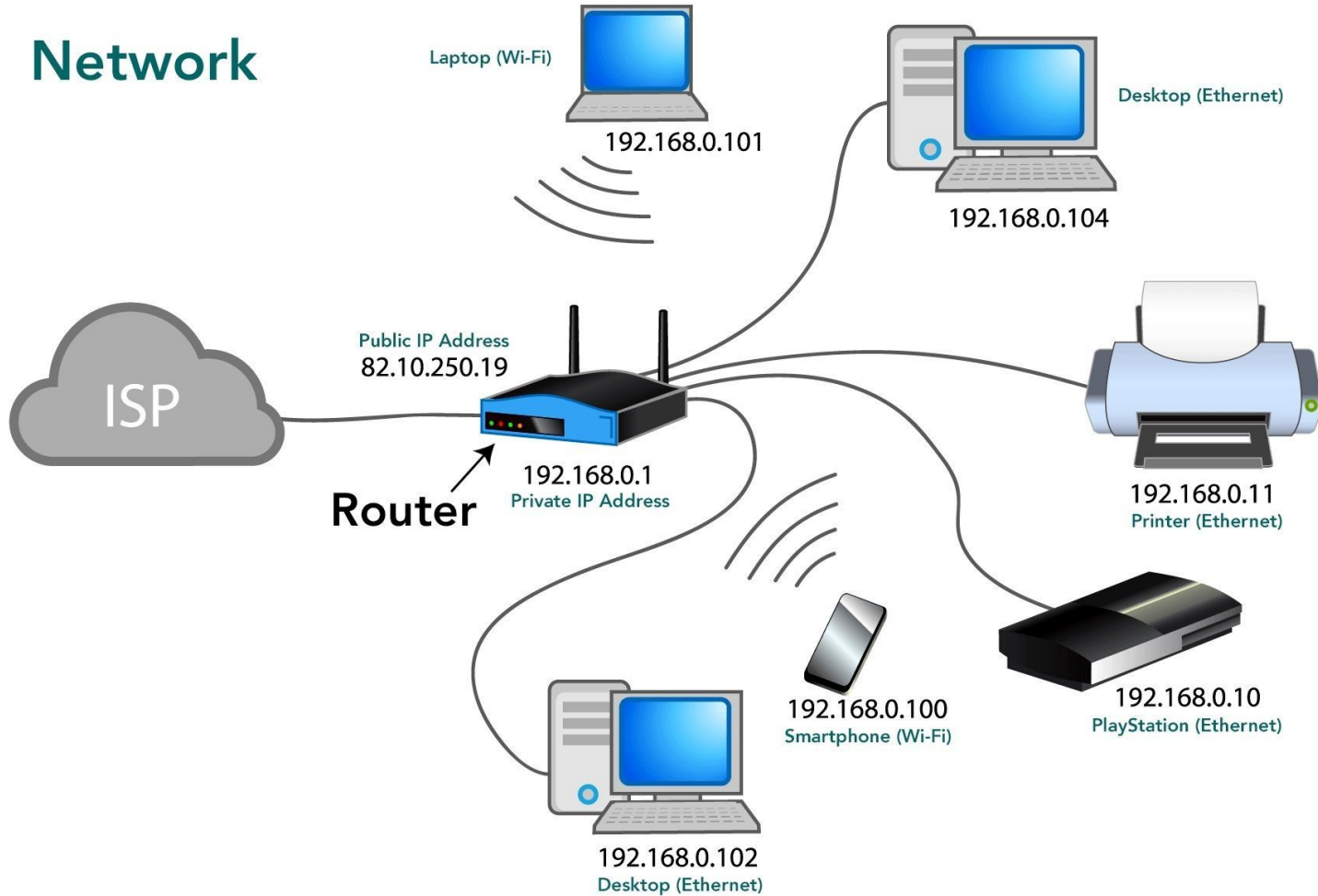
LAN (Local Area Network) – místní síť (např. doma, škole, firmě)

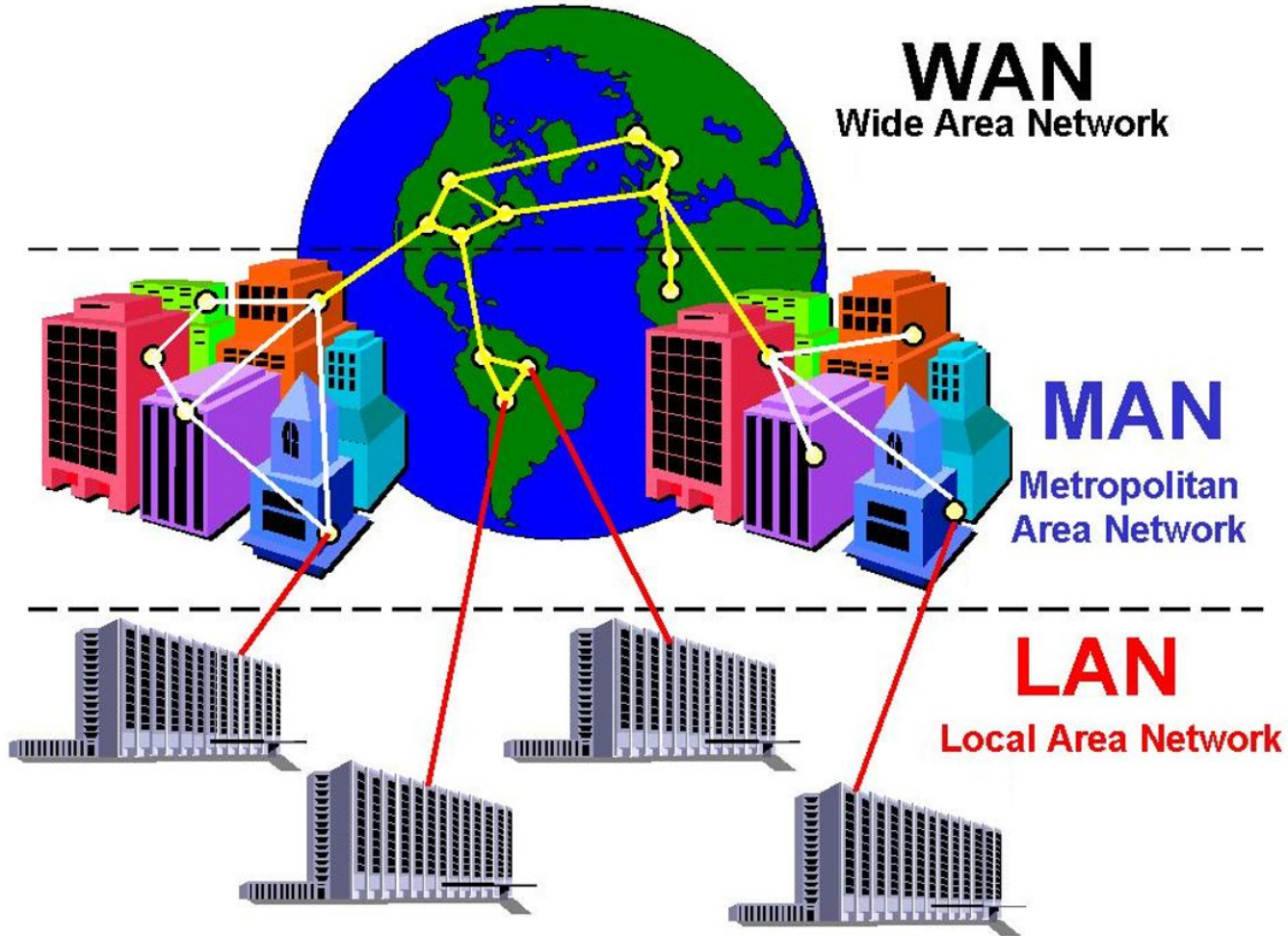
WLAN (Wireless LAN) – bezdrátová síť (Wi-Fi)

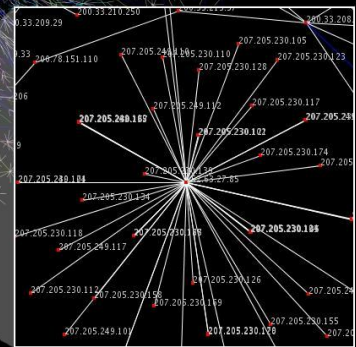
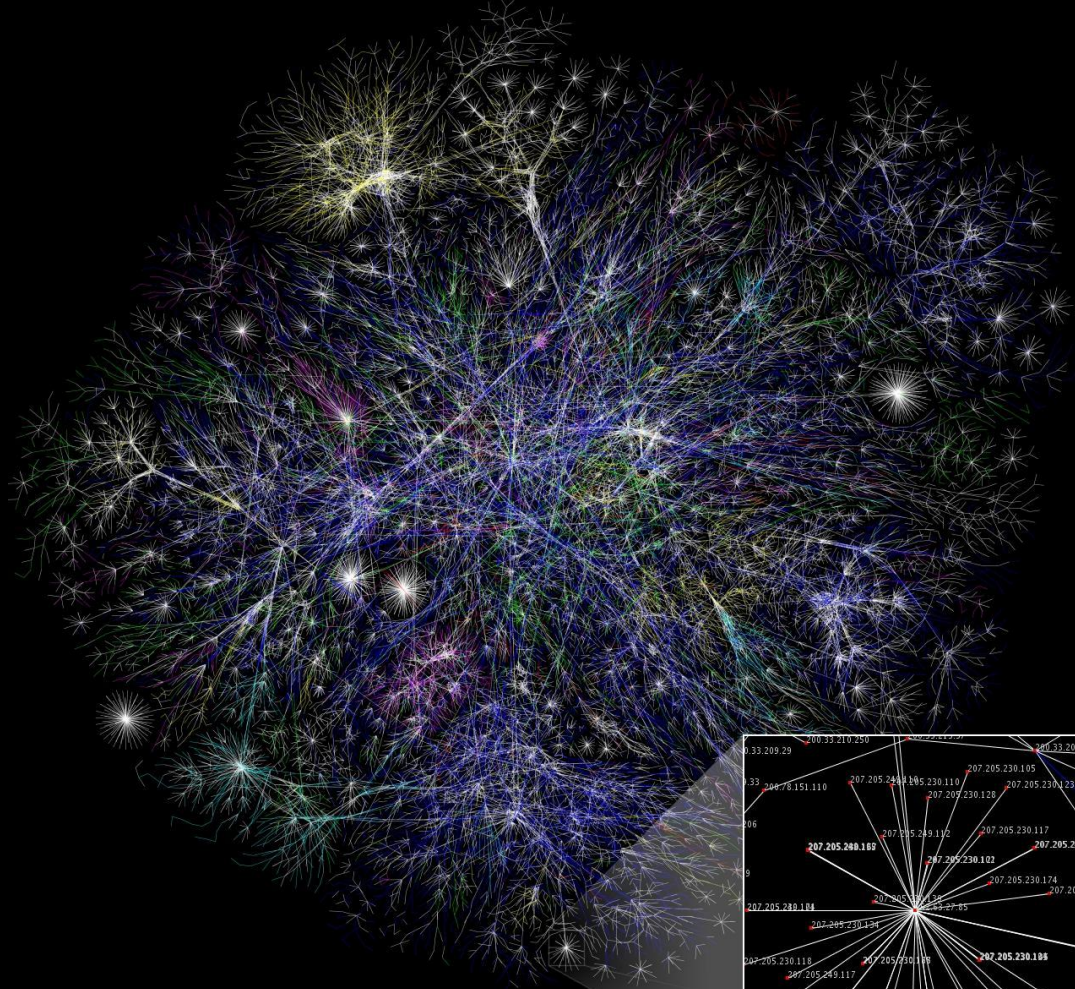
MAN (Metropolitan Area Network) – síť na úrovni jednoho města

WAN (Wide Area Network) – rozlehlá síť (např. internet)

Network







Funkce a využití

- Sdílení souborů a tiskáren
- Připojení k internetu
- Online komunikace (e-mail, VoIP, videokonference)
- Cloudové služby a vzdálená správa

Bezpečnost

- Šifrování
- Firewally
- VPN
- Autentizace uživatelů

IP adresa

IP adresa

Východisko: **Každý počítač v síti musí mít unikátní IP adresu.**

- Síť je několik vzájemně propojených počítačů (min. 2).
- Jednu síť jde propojit s jinou sítí.
- I zde platí stejné pravidlo unikátnosti IP adres.
- Internet není nic jiného, než **mnoho propojených sítí.**
- Žádná síť není nadřízená/podřízená jiné.
- A zde nastává problém: **Adresní rozsah IPv4 se před několika lety vyčerpal.**
- Toto se vědělo už dlouho dopředu.
- Proto se s předstihem vyvinul a zavedl systém **NAT.**

IP adresa

V současnosti existují **současně dvě verze**:

- IPv4

- Velikost: **32 b** (4 B)
- 4 dekadická čísla 0-255 oddělená tečkou
- Příklad: **217.195.162.12**
- Adresní rozsah (počet různých adres): $2^{32} = 4,3$ miliardy

- IPv6

- Velikost: **128 b** (16 B)
- 8 dvoubajtových čísel 0000-FFFF oddělených dvojtečkou
- Příklad: **2a02:0b20:0100:0217:0000:0000:0000:0012**
- Zkráceně (bez nul): **2a02:b20:100:217::12**
- Adresní rozsah (počet různých adres): $2^{128} =$ číslo s 38 nulami

NAT

- NAT je nouzová "berlička" zavedená pro IPv4.
- Nebýt jí, rozvoj internetu by se zastavil (a to nikdo nechce, že?).
- Princip je celkem prostý:
 - Několik IP adres se z veřejného internetu vyčlenilo.
 - Lze se používat **pouze v místních sítích** (počítače uvnitř organizace, domácnosti...).
 - Výhodou je, že **stejná IP adresa se může opakovat**.
 - Tím se ušetřilo nemalé množství adres.
 - Zvenku se pak všechny "tváří" jako jedna adresa.
- Vyčleněné rozsahy IP adres (nejčastější):
 - 192.168.0.0 – 192.168.255.255 (celkem 65536 adres)
 - 10.0.0.0 – 10.255.255.255 (celkem 16,7 milionu adres)

Veřejné a neveřejné IP adresy

- Z předchozího plyne, že v IPv4 jsou zavedeny tyto dvě kategorie.
- **Veřejné** musí mít servery (počítače) dostupné na Internetu.
 - Jsou celosvětově unikátní.
 - tux.panska.cz (217.195.162.12)
 - www.panska.cz (217.195.162.4)
 - www.google.com (142.251.36.142)
- **Neveřejné** jsou "schované" za NATem.
 - Stejně IP adresy se v různých sítích mohou opakovat (v rámci jedné pochopitelně ne).
 - Všechny počítače a mobily připojené k síti eduroam
 - Každý tvůj počítač, mobil, tiskárna u tebe doma.

ip -c a

Ve Windows příkaz: `ipconfig`

V macOS příkaz: `ifconfig`

- Příkaz vypíše informace o všech síťových rozhraních počítače.
- IP adresa tvého serveru je ta fialová za **inet** u rozhraní **enp0s3**.

```
debian [Beží] - Oracle VirtualBox
Soubor Počítač Náhled Vstup Zařízení Nápověda
root@debian:~# ip -c a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKN
  link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
  inet 127.0.0.1/8 scope host lo
    valid_lft forever preferred_lft forever
  inet6 ::1/128 scope host noprefixroute
    valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_co
  link/ether 08:00:27:60:36:18 brd ff:ff:ff:ff:ff:ff
  inet 192.168.1.241/24 brd 192.168.1.255 scope global dynamic
    valid_lft 863858sec preferred_lft 863858sec
  inet6 2a02:b20:100:1:a00:27ff:fe60:3618/64 scope global dynar
    valid_lft 2591996sec preferred_lft 604796sec
  inet6 fe80::a00:27ff:fe60:3618/64 scope link
    valid_lft forever preferred_lft forever
root@debian:~# _
```

Maska sítě

Co je to číslo za lomítkem (192 . 168 . 23 . 254 / **24**)

Maska sítě je nástroj, který v počítačových sítích pomáhá určit, **jak velká část IP adresy označuje síť a jak velká část označuje zařízení** (hosty) v této síti.

IP adresa je rozdělena na **dvě části**:

1. **Síťová část** – označuje konkrétní síť.
2. **Hostitelská část** – označuje zařízení uvnitř sítě.

Maska sítě říká, **kolik bitů z IP adresy patří síti a kolik hostům**.

- Pomáhá zařízením zjistit, kdo je v jejich síti, a kam poslat data.
- Pokud je IP adresa jiná, pošle data do brány (gateway).
- Bez masky sítě by zařízení nevěděla, kam data posílat.

ping

ping

- <https://cs.wikipedia.org/wiki/Ping>
- Příkaz otestuje, zda daný počítač v síti "žije" (a je dostupný).
- V unixových systémech "pingá" stále. Zastavení **Ctrl+C**.

```
ping [-4|-6] <IP adresa>
```

```
ping [-4|-6] <doména>
```

```
$ ping 217.195.162.12
```

```
$ ping tux.panska.cz
```

```
$ ping 192.168.23.xxx
```

-4 ... přes IPv4

-6 ... přes IPv6

Domény a DNS

Doména

- Doména je **unikátní název serveru**.
- Co se snáze pamatuje: www.panska.cz nebo `2a02:b20:100:217::4`?
- Je to jako jméno a telefonní číslo.

DNS

- To, která unikátní veřejná IP adresa bude navázaná na konkrétní doménu je uloženo ve speciálních **DNS serverech**.
- <https://www.jakfungujedns.cz/> (3:19 min)
- Náš server doménové jméno nemá – pro naše potřeby není potřeba.



Kde se vzala IP adresa mého serveru?

- Každý server má jinou IP adresu – kde se vzala?
- V každé síti je server, který přiděluje IP adresy klientským počítačům.
- Tento koncept se nazývá **DHCP**.
- Funguje to nějak takto:
 - Po zapnutí počítače vyšle OS do sítě požadavek, zda tam není nějaký, který by mu IP adresu přidělil. Pokud tam takový je, přidělí mu ji.
 - DHCP server si do svého seznamu "zapíše" **jakou IP přidělil, komu a do kdy rezervace platí**.
- Mám doma DHCP server? Určitě ano



MAC adresa

MAC adresa

- Jednoznačný identifikátor síťového zařízení (ne počítače, ale síťové karty)
- **Toto číslo si DHCP uloží jako identifikátor počítače**
- Velikost: **48 b** (6 B) $2^{48} = 281\,474\,976\,710\,656$ (vystačí nejméně do roku 2100)
 - Šestice dvojciferných hexadecimálních čísel oddělených
 - pomlčkami (např. **e4-b1-bf-07-14-c3**)
 - nebo dvojtečkami (např. **e4:b1:bf:07:14:c3**)
- Unikátní MAC adresu má i tvůj telefon (ověř si to).

Riziko spojené s přenosem MAC adresy po síti

Při připojení k Wi-Fi síti se z důvodu přidělení IP adresy pomocí protokolu DHCP přenáší MAC adresa zařízení. Tato adresa je jedinečným identifikátorem síťového adaptéru, a **pokud ji útočník odposlechne, může ji zneužít například ke klonování zařízení (MAC spoofing)** nebo k **cílenému sledování uživatele**. Tento přenos představuje bezpečnostní riziko, zejména v otevřených nebo špatně zabezpečených sítích. Toto riziko lze zmírnit několika způsoby.

1. Moderní zařízení umožňují zapnout funkci náhodného generování MAC adresy (**MAC randomization**), která při připojení k síti používá jednorázovou nebo dočasnou adresu místo skutečné.
2. Pro větší bezpečnost je také důležité připojovat se pouze k důvěryhodným sítím a používat šifrování na úrovni sítě (např. **WPA3**).
3. V případě podnikových sítí lze zavést další opatření, jako je filtrování MAC adres a použití VPN pro šifrování veškeré komunikace.

Služby a party

IP adresa serveru

Server TuX má **pevnou** a **veřejnou** IP adresu `217.195.162.12` a FQDN `tux.panska.cz`. Jeho název se stejný.

Server s webem Panské má IP `217.195.162.4`, FQDN `www.panska.cz`, jeho název je `valbom.panska.cz`.

Náš server má **dynamickou** a **neveřejnou** IP adresu. **Doménové jméno nemá**, neboť není registrovaný v systému DNS. Každý má (resp. musí mít) IP adresu jinou. Zjistíš ji příkazem

```
# ip -c a
```

To je to 4 bajtové fialové číslo za `inet` u rozhraní `enp0s3`.

Zapiš si ho!

Služby, protokoly, porty

Primárním úkolem serveru je poskytovat služby přes datovou síť (nejčastěji internet).

Protokol je „standardizovaný způsob komunikace mezi počítači“. Každý protokol náleží určité **internetové službě**. Aby se data různých protokolů mezi sebou nepletla, „cestují“ v datových sítích domluvenými **síťovými porty**. Port je číslo od 0 do 65535 (2 bajty).

Příklady běžných služeb a jejich portů (delší seznam je [zde](#)):

- HTTP (80) – (Hypertext Transfer Protocol) komunikace s WWW servery
- HTTPS (443) – Šifrovaný přenos HTTP protokolu přes [TLS](#)
- SMTP (25) – (Simple Mail Transfer protocol) odesílání pošty
- IMAP (993) – (Internet Message Access Protocol) vzdálený přístup k poště
- DNS (53) – (Domain Name System) hierarchický systém doménových jmen
- SSH (22) – (Secure Shell) zabezpečený komunikační protokol – ten důvěrně známe

! Platí zásada, že otevřené jsou jen ty používané, ostatní blokuje firewall!

Porty

Otevřené porty jde zjistit příkazem:

```
$ nmap <server>
```

Zkus z TuXe:

```
$ nmap 217.195.162.4
```

```
$ nmap www.panska.cz
```

Jak to dopadlo?