## Hotspot

Místo, které nabízí přístup k internetu prostřednictvím wifi. Přístupové body Hotspot jsou většinou umístěny na veřejných místech (restaurace, letiště, nádraží apod.).

## Wi-Fi

Wireless Fidelity - technologie bezdrátových sítí, která pracuje v bezlicenčním pásmu podle standardu 802.11. Umožňuje připojit se k internetu bezdrátově pomocí zařízení, jež wifi podporuje.

## IEEE 802.11

IEEE 802.11 je Wi-Fi standard s dalšími doplňky pro lokální bezdrátové sítě. Výraz 802.11x je používán pro množinu doplňků k tomuto standardu. Standard 802.11 zahrnuje několik druhů modulací pro posílání radiového signálu, přičemž všechny používají stejný protokol. Nejpoužívanější modulace jsou definované v dodatcích k původnímu standardu s písmeny a, b, g. 802.11n přináší další techniku modulace. Původní zabezpečení bylo vylepšeno dodatkem i. Další dodatky (c–f, h, j) pouze opravují nebo rozšiřují předchozí specifikaci. Standardy 802.11b a 802.11g používají 2,4 gigahertz (GHz) pásmo. Proto mohou zařízení interferovat s mikrovlnnými troubami, bezdrátovými telefony, s Bluetooth nebo s dalšími zařízeními používajícími stejné pásmo. Oproti tomu standard 802.11a používá 5 GHz pásmo a není tedy ovlivněn zařízeními pracujícími v pásmu 2,4 GHz. V únoru roku 2011 byl příchod nového standardu 802.11ac, který využívá zároveň obě pásma, tedy 2,4 gigahertz (GHz) a zároveň 5 gigahertz (GHz).

Přehled standardů IEEE 802.11

Standard Rok Pásmo [GHz] Max. rychlost [Mbit/s]

původní IEEE 802.11 1997 2,4 2

IEEE 802.11a 1999 5 54 IEEE 802.11b 1999 2,4 11 IEEE 802.11g 2003 2,4 54 IEEE 802.11n 2009 2,4 nebo 5 600 IEEE 802.11y 2008 3,7 54

IEEE 802.11ac 2013 2,4 a 5 1000 IEEE 802.11ad 2014 2,4, 5 a 60 7000

IEEE 802.11ax 2019 2,4 a 5 10000

Wi-Fi Alliance **mění značení** všudypřítomné bezdrátové technologie. Namísto nepřehledného **IEEE 802.11a/b/g/n/ac/ax** se teď budeme setkávat se srozumitelným označením **Wi-Fi 6**. Čím vyšší číslo, tím novější, lepší a rychlejší verze. Přeznačení se dotkne i starších verzí podle jednoduchého klíče:

* 802.11a --> Wi-Fi 1
* 802.11b --> Wi-Fi 2
* 802.11g --> Wi-Fi 3
* 802.11n --> Wi-Fi 4
* 802.11ac --> Wi-Fi 5
* 802.11ax --> Wi-Fi 6

...přičemž platí zpětná kompatibilita (většinou), tedy Wi-Fi 5 pracuje i se zařízeními Wi-Fi 1 až 4.

## SSID

Service Set Identifier je jedinečný identifikátor každé bezdrátové (Wi-Fi) počítačové sítě. Přístupový bod (AP) vysílá pravidelně každých několik sekund svůj identifikátor a klienti si tak mohou snadno vybrat, ke které bezdrátové síti se připojí. Jedná se tedy o název vysílané bezdrátové sítě.

## WEP

Wired Equivalent Privacy, tj. soukromí ekvivalentní drátovým sítím je zastaralé zabezpečení bezdrátových sítí podle původního standardu IEEE 802.11 z roku 1997. Cílem WEP bylo poskytnout zabezpečení obdobné drátovým počítačovým sítím (např. kroucená dvojlinka), protože rádiový signál je možné snadno odposlouchávat i na delší vzdálenost bez nutnosti fyzického kontaktu s počítačovou sítí. WEP byl prolomen v srpnu 2001, a proto je nahrazeno zabezpečením pomocí WPA2 podle standardu IEEE 802.11i.

## WPA, WPA2, WPA3

Wi-Fi Protected Access, tj. chráněný přístup k Wi-Fi je obchodní označení pro zabezpečení bezdrátových sítí definované Wi-Fi Alliancí v roce 2002. WPA2, je dodatek k IEEE 802.11 standardu vylepšující autentizační a šifrovací algoritmus pro bezdrátové sítě Wi-Fi. Byl schválen v roce 2004 a zneplatňuje tak původní zabezpečení WEP. WPA2 používá blokovou šifru Advanced Encryption Standard (AES) a poskytuje utajení, integritu a autentizaci. V lednu 2018, Wi-Fi Alliance oznámila vydání WPA3 s několika vylepšeními zabezpečení oproti WPA2.

## IP adresa

Jedinečné označení zařízení v počítačové síti. Na bázi protokolu IP spolu komunikují všechna zařízení v síti. IP adresa je v informatice číslo, které jednoznačně identifikuje síťové rozhraní v počítačové síti, která používá IP (internetový protokol). V současné době je nejrozšířenější verze IPv4, která používá 32bitové adresy zapsané dekadicky po jednotlivých oktetech (osmicích bitů), například 192.168.0.2. Z důvodu nedostatku IP adres je postupně nahrazován protokolem IPv6, který používá 128bitové IP adresy. IPv6 adresy se obvykle zapisují jako osm skupin čtyř hexadecimálních číslic. Například 2001:0db8:85a3:08d3:1319:8a2e:0370:7334 je platná adresa IPv6.

IPv4 má celkem 232 = 4 294 967 296 adres /kombinací/, IPv6 má 3.4×1038 unikátních adres. Na nejvyšší úrovni byl adresní prostor IPv4 vyčerpán 3.2.2011. Na počátku roku 2014 používalo protokol IPv6 přibližně 3% uživatelů Google.

Nedostatek IP adres se řeší různými způsoby: dynamickým přidělováním (tzn. např. každý uživatel dostane dočasnou IP adresu ve chvíli, kdy se připojí, ale jakmile se odpojí, je jeho IP adresa přidělena někomu jinému; při příštím připojení pak může tentýž uživatel dostat úplně jinou adresu), překladem adres (Network address translation) a podobně. Ke správě tohoto přidělování slouží specializované síťové protokoly, jako např. DHCP.

## MAC adresa

Media Access Control adresa je jedinečný identifikátor síťového zařízení. Je přiřazována síťové kartě bezprostředně při její výrobě a proto se jí také někdy říká fyzická adresa, nicméně ji lze dnes u moderních karet dodatečně změnit. MAC adresa se skládá ze 48 bitů a častěji se píše jako šestice dvojciferných hexadecimálních čísel oddělených pomlčkami nebo dvojtečkami (např. 01-23-45-67-89-ab nebo 01:23:45:67:89:ab). MAC adresa přidělená výrobcem je vždy celosvětově jedinečná.

## Maska sítě

Maska sítě je číslo, které popisuje rozdělení počítačové sítě do podsítí (subnets). Maska sítě zapsaná v binárním tvaru má zleva samé jedničky až do místa, kde končí číslo sítě a na místě části pro číslo síťového rozhraní jsou samé nuly. Pomocí masky sítě router rozhoduje o směrování (routing) IP datagramů.

Maska sítě je v IPv4 zapisována stejně jako IP adresa – čtyřmi desítkovými čísly oddělenými tečkami, z nichž každé odpovídá jednomu oktetu v 32bitové adrese. Maska 255.255.255.0 může být tedy binárně zapsána jako 11111111.11111111.11111111.00000000BIN. Nepřerušená řada jedniček jdoucích zleva označuje umístění čísla sítě a zbylé nuly v pravé části udávají umístění čísla síťového rozhraní (v dané podsíti). V tomto případě tedy zadaná maska rozděluje IP adresu na prvních 24 bitů s číslem sítě a zbylých 8 bitů pro číslo síťového rozhraní.

Pokud známe číslo sítě a masku, můžeme spočítat rozsah IP adres, které se v této podsíti nacházejí a tím i počet IP adres, které je možné použít pro síťová rozhraní v této podsíti. Administrátor tak může číslem sítě a maskou jednoduše vyjádřit rozsah adres, které má k dispozici.

Příklad

Zjistěte, jaké IP adresy lze využít pro počítače (resp. čísla síťových rozhraní) v podsíti 192.168.64.0/20.

Maska binárně: 11111111.11111111.11110000.00000000 (20 bitů)

Číslo sítě binárně: 11000000.10101000.01000000.00000000 (192.168.64.0)

1. IP adresa: 11000000.10101000.01000000.00000001 (192.168.64.1 - o 1 vyšší, než číslo sítě)

2. IP adresa: 11000000.10101000.01000000.00000010 (192.168.64.2 - o 1 vyšší, než předchozí)

...

Předposlední IP: 11000000.10101000.01001111.11111101 (192.168.79.253 - o 2 menší, než broadcast)

Poslední IP: 11000000.10101000.01001111.11111110 (192.168.79.254 - o 1 menší, než broadcast)

Broadcast: 11000000.10101000.01001111.11111111 (192.168.79.255)

Z tabulky je vidět, že:

192.168.64.0 – číslo sítě

192.168.64.1 – první použitelná IP adresa

192.168.79.254 – poslední použitelná IP adresa

192.168.79.255 – broadcast (na místě čísla síťového rozhraní má samé jedničky, další v pořadí by již byla mimo zadané číslo sítě)

počet IP adres použitelných pro síťová rozhraní je 4094 (212 - 2), tj. 2 na mocninu počtu bitů, které jsou k dispozici pro čísla síťových rozhraní, mínus jedna pro číslo sítě a mínus druhá pro broadcast)

## TCP/IP

Transmission Control Protocol/Internet Protocol – je sada primárních protokolů pro komunikaci v počítačové síti a je hlavním protokolem celosvětové sítě Internet. Komunikační protokol je množina pravidel, která určují syntaxi a význam jednotlivých zpráv při komunikaci.

TCP vytváří virtuální okruh mezi koncovými aplikacemi, tedy spolehlivý přenos dat. Spolehlivá transportní služba, doručí adresátovi všechna data bez ztráty a ve správném pořadí. Transparentní přenos libovolných dat. Rozkládá data na datagramy /pakety, balíčky/ a na druhé straně je zase skládá dohromady.

IP provádí vysílání datagramů na základě síťových IP adres obsažených v jejich záhlaví. Každý datagram je samostatná datová jednotka, která obsahuje všechny potřebné údaje o adresátovi i odesilateli a pořadovém čísle datagramu ve zprávě. Datagramy putují sítí nezávisle na sobě a pořadí jejich doručení nemusí odpovídat pořadí ve zprávě. Doručení datagramu není zaručeno, spolehlivost musí zajistit vyšší vrstvy (TCP, aplikace). Má na starost cestu datagramů.

## DHCP

Dynamic Host Configuration Protocol je název protokolu z rodiny TCP/IP nebo označení odpovídajícího DHCP serveru či klienta. Používá se pro automatickou konfiguraci počítačů připojených do počítačové sítě. DHCP server přiděluje počítačům, mobilním telefonům, tabletům… pomocí DHCP protokolu zejména IP adresu, masku sítě, implicitní bránu a adresu DNS serveru. Bez nastaveného DHCP by se síťová zařízení nemohla připojit k nejčastěji bezdrátové síti a sdílet tak nejčastěji připojení na internet.

## Telnet

Zkratka z Telecommunication Network je označení protokolu používaného v počítačových sítích, který pomocí stejnojmenné aplikace umožňuje uživateli připojení ke vzdálenému počítači. Jedná se o emulaci terminálu, která poskytovala možnost práce uživatele na vzdáleném počítači v příkazovém řádku. Bez šifrování přenášených dat. Dnes nahrazen SSH.

## SSH

Secure Shell je program a zároveň zabezpečený komunikační protokol v počítačových sítích, které používají TCP/IP. Je to náhrada za telnet, který posílá heslo v nezabezpečené formě a umožňují tak jeho odposlechnutí při přenosu pomocí počítačové sítě. Šifrování přenášených dat, které SSH poskytuje, slouží k zabezpečení dat při přenosu přes nedůvěryhodnou síť, jako je například Internet.

## DNS

Domain Name System je hierarchický systém doménových jmen, který je realizován servery DNS a protokolem stejného jména, kterým si vyměňují informace. Jeho hlavním úkolem a příčinou vzniku jsou vzájemné převody doménových jmen a IP adres uzlů sítě. Tedy doménový název [www.seznam.cz](http://www.seznam.cz) převede na IP adresu 77.75.77.39.

## VPN

Virtual Private Network neboli privátní virtuální síť. Slouží k propojení několika počítačů, které se nacházejí na různých místech počítačové sítě/internetu, do jedné virtuální počítačové sítě.

## Proxy server

Proxy server funguje jako prostředník mezi klientem a cílovým počítačem (serverem), překládá klientské požadavky a přijatou odpověď od serveru následně odesílá zpět na klienta. Proxy server odděluje lokální počítačovou síť (intranet) od Internetu. Tedy zajišťuje a filtruje komunikaci mezi vnější a vnitřní sítí. Může se jednat jak o specializovaný hardware, tak o software provozovaný na běžném počítači.

## Gateway (brána)

Gateway (brána) je název aktivního síťového zařízení, které má v počítačové síti nejvyšší postavení. Brána propojuje dvě sítě pracující s odlišnými komunikačními protokoly. Vykonává i funkci routeru (směrovače). Příkladem brány je počítač, který pomocí webové stránky přijme z Internetu zprávu, kterou odešle do mobilní GSM sítě v podobě SMS zprávy. Označení default gateway (implicitní brána) označuje router (směrovač), přes který se stanice dostanou do vnější sítě (tj. obvykle do Internetu).

## Firewall

Systém ochrany sítě před neoprávněným vstupem ze sítě jiné. Ochranu mohou tvořit prvky softwarové /součást OS či Internet Security/ a hardwarové /součást routeru/ nebo jejich kombinace.

## NAT

Network Address Translation (překlad síťových adres) je způsob úpravy síťového provozu přes router přepisem výchozí nebo cílové IP adresy u průchozích IP paketů. NAT se většinou používá pro přístup více počítačů z lokální sítě na Internet pod jedinou veřejnou adresou.

Překlad síťových adres je funkce, která umožňuje překládání adres. Což znamená, že adresy z lokální sítě přeloží na jedinečnou adresu, která slouží pro vstup do jiné sítě (např. Internetu), adresu překládanou si uloží do tabulky pod náhodným portem, při odpovědi si v tabulce vyhledá port a pošle pakety na IP adresu přiřazenou k danému portu. NAT je vlastně jednoduchým proxy serverem. NAT může být software (Nat32, Kerio Winroute firewall), nebo hardware (nejčastěji router s implementací nat).

Vznikl jako důsledek omezeného počtu veřejných IP adres (IPv4 má 32 bitů a část z nich je navíc rezervována pro speciální účely). Každý uživatel dnešního internetu nemůže mít adresu z vnějšího rozsahu, NAT umožňuje celou vnitřní síť ukrýt za adresu jedinou.

Router má přidělenu soukromou adresu lokální sítě (intranetu), ale také je spojen s Internetem, nejčastěji jedinou veřejnou adresou (overloaded NAT), přidělenou poskytovatelem připojení k Internetu (Internet Service Provider). Jakmile jde paket z lokální sítě do Internetu, je jeho zdrojová adresa (soukromá) přeložena na veřejnou. Router si uchovává základní data o každém aktivním spojení (adresu cíle, port). Když se vrátí odpověď na router, využije data získaná při odchozí fázi a určí kam na vnitřní síť je třeba odpověď zaslat. Pro systém na Internetu se jeví router jako zdroj i cíl komunikace. NAT zvyšuje bezpečnost počítačů za ním připojených (útočník nezná strukturu sítě a nemůže se spojit přímo s konkrétním počítačem). NAT ovšem firewall nenahrazuje a existují způsoby, jak počítače za NATem napadnout.

## Aktivní (napájené) síťové prvky

* **HUB** (Rozbočovač) – slouží k fyzickému propojení jednotlivých síťových zařízení do sítě. Uzly jsou propojovány ve hvězdicové síťové topologii.
* **SWITCH** (Přepínač) – inteligentně spojuje jednotlivá síťová zařízení do sítě. Data rozesílá jen tam, kam je skutečně potřeba, čímž zatížení sítě snižuje a řeší kolize.
* **WI-FI ROUTER** (Směrovač) – provádí rozšíření sítě, vytváří novou podsíť drátovou/bezdrátovou, např. v domácnosti na sdílení internetu pro více zařízení. Pro příchozí datové pakety dokáže díky znalosti topologie celé sítě najít nejvhodnější další cestu.
* **REPEATER –** opakovač signálu, na připojení vzdálenějších zařízení v síti
* **MODEM** – provádí **mo**dulaci a **dem**odulaci signálu, zpracovává digitální signál na signál přenositelný po daném médiu providera

## Sítě podle velikosti

* **LAN** – lokální počítačová síť, domácnost, učebna, do 2km
* **MAN** – městská počítačová síť, do 20km
* **WAN** – rozlehlá počítačová síť – internet, nad 20km