Počítačové Sítě – vyřešené otázky k maturitě

- **Autor:** Karel Čermák, info@k-cermak.com.
- **Ročník:** 2023.
- **Repozitář:** https://github.com/K-cermak/SPSE-Maturita.
- **Práva:** Materiály autor zveřejňuje bez záruk a pouze pro osobní nekomerční použití. Šíření těchto materiálů je povoleno pouze s původním (nezměněným) ponecháním této stránky či sdílením na oficiální repozitář uvedený výše.
- **Tip:** Pro rychlou orientaci v kapitolách lze použít klávesovou zkratku CTRL + F a přejít do funkce Nadpisy.

- **Donate:** Pokud ti mé materiály pomůžou a jsi ochoten ocenit moji snahu nějakou kačkou, můžeš tak učinit přes QR kódy níže: ❤️❤️❤️
  - **Účet:** 2262692018/3030

  - **Crypto:**
    - **BTC:** bc1qasgxc552wjqlpcm9vt7ucmw6p4zuz007dxh8n4
    - **ETH:** 0x29Ca9054B2241aB39010a1434fb50e504EE10871
    - **LTC:** ltc1qxpgp3jc5jyem6096n48w48qqrwsrnj5eq9j890
    - **ADA:** addr1q8c89cet02nyql4ygj96s0cz5ntusgzxfzuykfngmaf0zt2ftj7wrayqm7dx52et7k7tkjjl2edan0wykww6q4twn79shzx8vn
    - **DOGE:** DCYFq9hPcVJkYKAgttkRXNSAkfbjEmLGdo

  - A pokud jsi chudý student a všechny prachy prochlastáš, můžeš mi alespoň dát hvězdičku na GitHub repozitář...

1. Základní pojmy počítačových sítí

- *topologie*
- *taxonomie sítí*
- *Internet (vývoj a autority)*
- *modely ISO/OSI a TCP/IP, princip zapouzdření, pojem užitečný náklad*
- *příklady zařízení pracujících na jednotlivých vrstvách*
- *standardy používané v počítačových sítích*

KZ – koncové zařízení.

KU – koncový uzel.

NIC – network interface card, síťová karta, ethernetová karta.

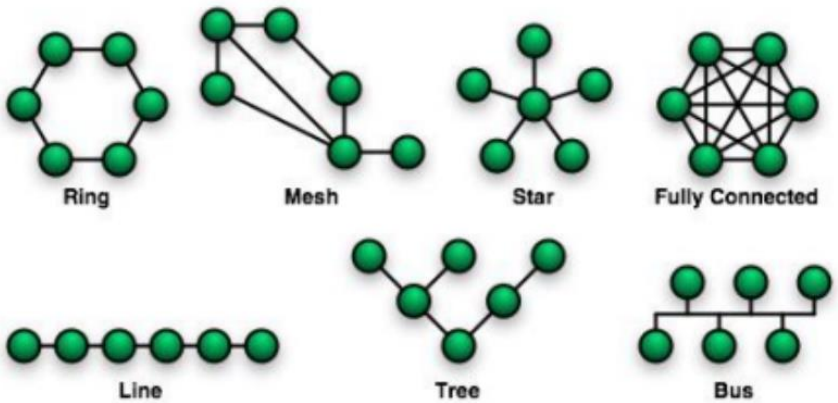
Pasivní prvky sítě – prvky "pasivní" realizace přenosové cesty, konektory, kabely, rozvaděče apod.

Aktivní prvky sítě – prvky, které "aktivně" zpracovávají data přenášená sítí, opakovače, přepínače, konvertory apod.

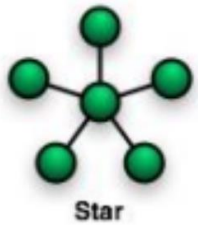
Infrastruktura sítě – soubor prvků sítě odpovídající použité technologii.

1.1. Topologie

- Určuje způsob zapojení zařízení.



- **Hvězdicová (Star)**

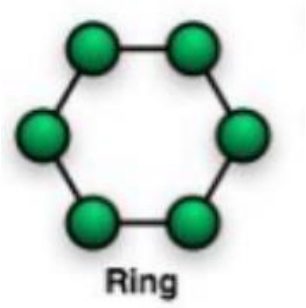


  - Nejčastější způsob zapojení zařízení v sítích.
  - Ve tvaru hvězdy.
  - Každé zařízení je připojeno kabelem (UTP - nestíněný, STP - stíněný) k centrálnímu prvku – hubu nebo switchi.
  - **Výhody:**
    - Pokud selže zařízení či kabel, vypadne jen daná stanice.
    - Snadno se zavádí a rozšiřuje.
    - Snadno se nachází a řeší závady.
  - **Nevýhody:**
    - Potřeba mnoha kabelů – 1 pro každé zařízení.
    - Potřeba centrálního prvku – např. switch.
    - Když selže centrální prvek, vypadne celá síť.

- **Stromová (Tree)**

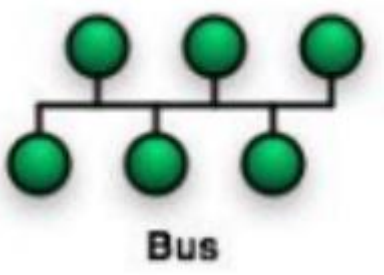
  - Vychází z hvězdicové topologie, pro velké firmy.
  - **Výhody:**
    - Při selhání nižší části sítě zbytek sítě funguje.
    - Potřeba méně kabelů.
    - Vyšší bezpečnost – zvyšuje se obtížnost odposlouchávání komunikace.
  - **Nevýhody:**
    - Selháním prvku vypadnou i prvky pod ním.

- **Kruhová (Ring)**



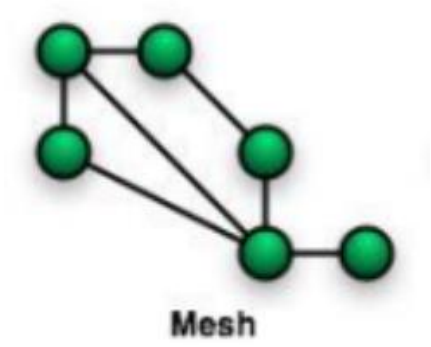
  - Ve tvaru kruhu, data tečou v jednom směru.
  - Stanice si posílají ve směru toku dat **paket token** – kdo ho má, může vysílat, po určitém čase vysílání ho pošle dál.
  - **Výhody:**
    - Levné zapojení.
    - Není potřeba řešit kolizi dat.
  - **Nevýhody:**
    - Data musí projít celou cestu v kruhu.
    - Při selhání jednoho uzlu selže celá síť.
    - Není snadné najít závadu.
    - Pro zapojení nového zařízení se odstavuje celá síť.

- **Sběrnicová (Bus)**



  - Jeden souvislý kabel.
  - Funguje takto vlastně USB.
  - Stanice zapojeny za sebou do kabelu.
  - Ukončeno terminátory.
  - Používání CSMA (Carrier Sense Multiple Access).
  - **Výhody:**
    - Jednoduchá levná realizace.
    - Vhodná pro malé a dočasné sítě.
  - **Nevýhody:**
    - Při problému s kabelem výpadek celé sítě.
    - Malá přenosová rychlost.
    - Vyslanou informaci dostávají všechny zařízení.
    - Dvě zařízení nemohou vysílat najednou.

- **Mesh**



  - Není přesně specifikováno.
  - Používáno u sítí, které mají mít vyšší odolnost proti výpadkům, které se skládají z tolika uzlů, že nelze realizovat Fully Connected.
  - Jedná se vlastně o Internet, telekomunikační sítě, elektrická přenosová soustava.
  - **Výhody:**
    - Pokud má uzel více připojení, po výpadku jednoho připojení lze stále komunikovat.
    - Neexistuje centrální prvek.
    - Není potřeba tolik kabelů jako u plně propojené sítě.
    - Síť lze snadno rozšiřovat.
  - **Nevýhody:**
    - Nutné směrování provozu.
    - Nutná ochrana proti zacyklení.

1.2. Taxonomie sítí

- Určuje klasifikaci sítě (její parametry).
- Může se jednat o:
    - **Topologie sítě**
        - Viz předchozí bod.
    - **Rozsáhlost sítě**
        - **PAN** (Personal Area Network) – třeba Bluetooth spojení.
        - **LAN** (Local Area Network) – místní síť, například domácnost.
        - **MAN** (Metropolitan Area Network) – propojení LAN sítí, oblast města.
        - **WAN** (Wide Area Network) - propojení států, kontinentů.
    - **Určení funkce sítě**
        - **SAN** (Storage Area Network) – propojení počítačů s diskovými poli.
        - **NAN** (Neigbour Area Network) – sousedské sítě – Wi-Fi hotspot, WLAN pro rodinu, sousedy.
    - **Vlastnictví sítě**
        - **Veřejná** – pro přenos dat přes internet, ke komunikaci s ostatními.
        - **Privátní** – slouží ke komunikaci doma, v kanceláři, v podniku.
        - **VPN** (Virtual Private Network) – soukromé zabezpečení propojení vzdálených počítačů přes veřejnou síť.
    - **Mobilita sítě**
        - **WLAN** (Wireless Local Area Network) – Bezdrátový přenos.
        - **Wi-Fi** (Wireless Fidelity) – Druh WLAN.
        - **WiMax** – pro internetové a mobilní poskytovatele – dosah na několik km.
    - **Použité přenosové technologie**
        - Drátové sítě (metalické).
        - Optické sítě.
        - Bezdrátové sítě.
        - Satelitní (Starlink).

1.3. Internet (vývoj a autority)

Vývoj

- Nejprve různé custom sítě – terminálové sítě, RAS (Remote Access) apod.
- **ARPANET**
  - **Slučování více různorodých sítí.**
  - 1969 v USA kvůli studené válce.
  - Komunikace na základě **přepojování paketů**.
  - První uzly na univerzitách – propojení superpočítačů.
  - Po úspěchu se začala dále šířit.
  - Síťový protokol NPC (Network Control Protocol).
- **Komercializace internetu**
  - Byl navržen pro výzkum a univerzity, **komerčním účelům bráněno**.
  - Vznik různých (regionálních) sítí vedle internetu – např. e-mailové.
  - V roce **1991** zlom – **umožněno propojování sítí v rámci světa**, začátek internetu známého tak, jako dnes.
  - V ČR poprvé 1992 (ČVUT) – 19200 b/s.
  - První sítí CESNET.
  - Po roce 1995 různé soukromé subjekty a ISP.

Autority

- **ICANN**
  - Internet Corporation for Assigned Names and Numbers.
  - Provoz a rozvoj, nejvyšší autorita.
- **IANA**
  - Internet Assigned Numbers Authority.
  - Provoz internetu, podléha ICANN.
  - Adresa, jména (DNS) a zařízení protokolů.
- **RIR**
  - Regional Internet Registry.
  - Přidělování IP adres po blocích.

- **RIP RIPE NCC**
  - Réseaux IP Européens Network Coordination Centre.
  - Evropský RIR.
- **IETF**
  - The Internet Engineering Task Force.
  - Dokumentace vývoje, podklady a standardizace.

1.4. Modely ISO/OSI a TCP/IP, princip zapouzdření, pojem užitečný náklad

Orientace	Model ISO/OSI	TCP/IP
Přenos dat	L1 Fyzická vrstva	Vrstva síťového rozhraní
	L2 Linková vrstva	
	L3 Síťová vrstva	Sítová IP vrstva
Přizpůsobovací vrstva	L4 Transportní vrstva	Transportní vrstva
Podpora aplikací	L5 Relační vrstva	Aplikační vrstva
	L6 Prezentační vrstva	
	L7 Aplikační vrstva	

- Bylo nutné **standardizovat pravidla pro komunikaci** v počítačových sítích.
- Modely byly zavedeny, aby zařízení s různými OS mohly komunikovat přes jiné síťové technologie.
- ISO/OSI je zbytečně moc složitý, v **praxi se používá spíše TCP/IP**.

ISO/OSI

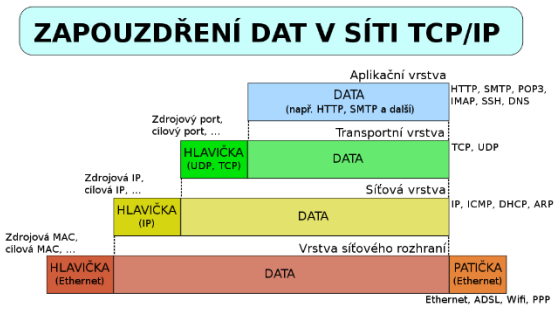
- **L1 Fyzická vrstva** – přenos bitů.
- **L2 Linková vrstva** – přenos rámců, CRC (detekce chyb), sdružování bitů do rámců.
- **L3 Síťová vrstva** – přenos dat v síti, přenáší pakety.
- **L4 Transportní vrstva** – v koncových zař., řídí spojení, kontroluje, zda data dorazila.
- **L5 Relační vrstva** – koordinuje a udržuje komunikaci, stará se o přihlašování a správu.
- **L6 Prezentační vrstva** – formát dat, kompresi, dekompresi, šifrování.
- **L7 Aplikační vrstva** – protokoly, přenášejí určitá data pomocí protokolů ostatních vrstev, třeba DHCP.

TCP/IP

- **Vrstva síťového rozhraní** – slouží k řízení fyzického přenosového média – linky.
- **Síťová vrstva** – zajišťuje především síťovou adresaci, směrování a předávání datagramů.
- **Transportní vrstva** – stará se o celistvost dat, řídí spojení, kontroluje, zda data dorazila, protokoly TPC a UDP, je implementována pouze v koncových zařízení.
- **Aplikační vrstva** – protokoly a aplikace, přenášejí určitá data pomocí protokolů transportní vrstvy a ostatních vrstev, třeba DHCP.

Princip zapouzdření

- Data nejsou přenášena kontinuálně, ale jsou předávána v blocích.
- Datové bloky linkové vrstvy na LAN se nazývají datové rámce (Frame).
- V rámcích jsou zabaleny datové bloky dalších vyšších protokolů, jedná se o princip zapouzdření (encapsulace).



Užitečný náklad

- Jedná se o data, která dokážeme skutečně využít – takže jsou bez hlavičky apod.
- Může být označeno taktéž jako přenosový výkon.

Paket

- Bloky dat na síťové vrstvě.

Datagram

- Obecný název bloku dat přenášený od síťové vrstvy níže (k L1 Fyzické).

1.5. Příklady zařízení pracujících na jednotlivých vrstvách

- **Fyzická vrstva**
  - Neupravuje samotná data.
  - Kabel (pasivní), anténa, media konvertor (optika <-> metalika), hub.
- **Linková vrstva**
  - Musí rozumět MAC adresám a podle toho reaguje.
  - Switch, bridge.
- **Síťová vrstva**
  - Musí rozpoznávat IP adresy (překládání IP na MAC).
  - Router (směrovač), firewall.
- **Aplikační vrstva**
  - Prohlížeč (HTTP), email (SMTP), průzkumník (FTP).

1.6. Standardy používané v počítačových sítích

- **RFC**
    - Dokumenty napsané experty, je to spíše **doporučení pro řešení** nějakých **problémů**, popisuje internetové protokoly.
    - RFC 2046 – definuje text/plain MIME.

- **IEEE**
    - Organizace, formuluje různé **standardy pro komunikaci** v počítačových sítích a podobu počítačových sítí.
    - IEEE 802.11 – Wi-Fi.

2. Fyzická vrstva a metalická přenosová média

- *veličiny (přenosová rychlost, zpoždění, rychlost šíření signálu, zisk/útlum)*
- *metalická přenosová média a jejich vlastnosti (koaxiální kabel, UTP, konektory)*
- *kategorie kroucené dvoulinky a jejich použití*
- *kódování, modulace*
- *přístupové metody ke sdílenému médiu*
- *media konvertory*
- *PoE (využití, aktivní/pasivní, dodávaný výkon, vyjednávání napájení)*

Význam fyzické vrstvy - Binary Transmision.
Bezpečný přenos jednotky informace.

2.1. Veličiny (přenosová rychlost, zpoždění, rychlost šíření signálu, zisk/útlum)

- **Útlum**
  - Zeslabení signálu – jednotka dB.
- **Přeslech**
  - Deformace působením okolních signálů – jednotka dB.
- **Zkreslení**
  - Deformace signálu (přeslechem nebo rušením) – jednotka %.
- **Šum**
  - Deformace signálu (parametry součástek zařízení) – jednotka dB.
- **Přenosová rychlost**
  - Vyjadřuje objem dat, přenesených za jednotku času [b/s].
  - Neříká nic o frekvenci změn přeneseného signálu.
- **Modulační rychlost**
  - S jakou frekvencí se mění signál.
  - Měří se v Baudech (Bd).
  - Rychlost přenosu nezávisí pouze na frekvenci změny, ale i kolik informací nese signál.

- **Zpoždění**
  - Doba, za kterou datagram urazí cestu mezi dvěma zařízeními a zpět.
  - τ (tau) v sec (běžně µs - mikrosekundy).
  - Při vysokých rychlostech má vliv na maximální diametr sítě.
- **Rychlost šíření signálu**
  - **NESOUVISÍ S PŘENOSOVOU RYCHLOSTÍ!**
  - Rychlost šíření elektromagnetických vln v přenosovém médiu.
  - Udává se m/s.
  - Ve vakuu rovna rychlosti světla **c = 300 000 km/s**.
  - V běžném prostředí 0.6 – 0.9c. Pro metalické kabely 0.82c.
- **Zisk / útlum**
  - Rozdíl síly signálu na jednom konci vedení oproti druhému konci.
  - Jednotka dB/délka (km).
  - **Útlum** – **ztráta** (např.: -3 dB).
  - **Zisk** – **posiluje** (např.: 3 dB).

Výpočet dB

- Používání logaritmické měřítka.
- Decibel – logaritmická bezrozměrná poměrová jednotka.
- Protože **deci**bel – nutné násobit 10.
- Poměr výkonů (x1 – vstup; x2 – výstup) - Ap = 10 log $(\frac{P_2}{P_1})$.
- Napěťové (Au) či proudové zesílení (Ai) - Au = 20 log $(\frac{U_2}{U_1})$.

Příklady dB

- Zesilovač má na vstupu 20mW a jeho výstupní výkon je 3,5 W. Jaký má zisk v dB?
- $G = 10.log\frac{3{,}5}{20.10^{-3}} = 10.log\,175 = 10.2{,}24 = \underline{22{,}4dB}$ **(zisk)**

- Na vstup koaxiálního kabelu je přiveden od vysílače výkon 150 W a na výstupu byl naměřený výkon pouze 112 W. Jaké ztráty v dB má koaxiální kabel?
- $G = 10.log\frac{112}{150} = 10.log\,0,747 = 10.(-0{,}127) = \underline{-1{,}27dB}$ **(útlum)**

- **Logaritmus čísla menšího jak 1 je záporné číslo! Pro nulovou a zápornou hodnotu není logaritmus definován!**

- **Frekvence** – elektromagnetické vlny přenášejí data, a právě tyto elektromagnetické vlny musí mít nějakou frekvenci.
- **Impedance** – odpor vnitřních materiálů.

2.2. Metalická přenosová média a jejich vlastnosti (koaxiální kabel, UTP, konektory)

Koaxiální kabel

- Asymetrické vedení – jeden signál a GND – tedy half duplex.
- Sběrnicová topologie (BUS).
- Impedance Z_o je 50 Ω.

- Dobrá odolnost vůči rušení a použití i v exteriéru.
- Nepoužívá se, přenosová rychlost 10 Mbps (ale stále pro televizní antény apod.).

- **Thick (Tlustý)**
  - 5 segmentů po 500 m – max. 2.5 km.
  - Konektor DIX, následně AUI.
- **Thin (Tenký)**
  - 5 segmentů po 185 m – max. 925 m.
  - Konektor BNC.

- Na konci použit terminátor – má charakteristickou impedanci.

Pravidlo 5:4:3 – 5 kabelových segmentů, propojených pomocí 4 opakovačů a ke 3 z 5 mohou být připojeny nějaké uzly / KZ.

Kroucená dvoulinka (Twisted pair)

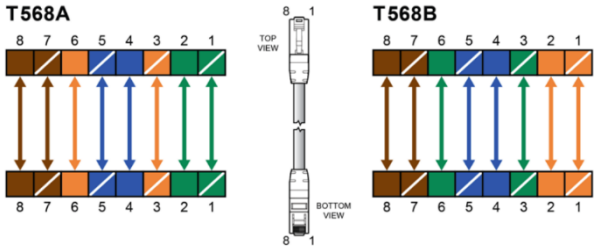
- Hvězdicová topologie (Star).
- Impedance Z_o je 100 Ω.
- Symetrické vedení – **diferenciální signál** (jeden je kladný a druhý záporný – Rx+, Rx-, Tx+, Tx-).
- Kroucením dochází k lepší odolnosti vůči rušení a vyřazování méně elektromagnetického vlnění.
- Kroucení musí být přesné a stálé.
- 4 páry vodičů (stačí 2 páry) – full duplex.

- **UTP (Unshielded Twisted Pair) - nestíněný**
  - Levný, nejpoužívanější, snadněji ohýbatelný.
- **STP (Shield Twisted Pair) – stíněné kabely**
  - **FTP (Foiled Twisted Pair)** – stíněné fólií.
  - **ISTP (Individual Shield Twisted Pair)** – individuálně stíněné páry.
  - Složitější montáž, kvalitnější, menší problémy s rušením.

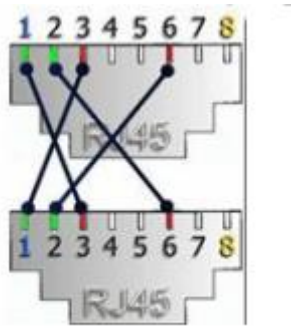
- **Kategorie CATx**

CAT3	CAT4	CAT5	CAT5e	CAT6	CAT6a	CAT7	CAT8
10 Mbps	16 Mbps	100 Mbps	1 Gbps	1 Gbps	10 Gbps	10 Gbps	25 / 40 Gbps
16 MHz	20 MHz	100 MHz	100 MHz	250 / 500 (STP) MHz	500 MHz	600 MHz	2000 MHz

- **Konektor RJ45 (Rear Jack)**
  - 8 pinů.
  - Keystone moduly – modulární, přesnější, kvalitnější, dražší.
  - 2 standardy – A / B (používanější).



- **Přímé** (Patch cable) – propojovací.
- **Křížené kabely** (CrossOver) – 2 KZ propojujeme mezi sebou (Rx na Tx a naopak).



2.3. Kódování, modulace

Baseband

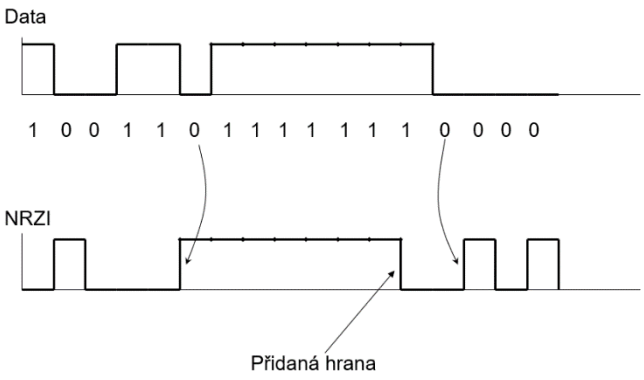
- Jde o takový druh přenosu, při kterém je **vstupní signál okamžitě převáděn na přenosové médium** – bez činnosti modulačního prvku.

Boardband

- **Data** k přenosu se **naloží na nosný signál**.
- Naloží se na něj pomocí modulace – ta mění pomocí signálu s daty parametry nosného signálu.

Kódování

- **NRZI**
  - Například i v USB.
  - 1 – změna, 0 – beze změny signálu (**u PS**), v **HW** to je přesně obráceně.



- **4b5b, 8b10b**
    - Odstraňuje dlouhé série nul a jedniček.
- **PSK, DPSK**
    - Spíše modulace signálu pomocí synchronizace.

Modulace

- Proces úpravy původního signálu, kdy neměníme přenášenou informaci, ale vlastnosti tohoto signálu – jeho amplitudu, frekvenci, fázi – **zlepšení přenosu na delší vzdálenost**.

- **Amplitudová modulace**
    - Amplitude Modulation (AM).
    - Málo odolná proti vnějšímu rušení.
- **Frekvenční modulace**
    - Frequency Modulation (FM).
    - Vhodná pro nižší rychlosti.
- **Fázová modulace**
    - Phase Modulation (PM).
    - Nejodolnější, vhodná i pro vyšší rychlosti.

2.4. Přístupové metody ke sdílenému médiu

- Základní rozdělení metod je na **kolizní** (**nedeterministické**) a **bezkolizní** (**deterministické**).

Kolizní:

- CSMA/CD (Ethernet), CSMA/CA (Wi-Fi).
- Aloha (na random začne vysílat).

Bezkolizní:

- **Frekvenční multiplex (FDMA)**
    - Frekvenční pásmo, které je k dispozici, se rozdělí na kanály s požadovanou šířkou pásma.
    - Wi-Fi, TV, rozhlas.
- **Časový multiplex (TDMA)**
    - ISDN (komunikace po telefonní lince – digitál na analogu), FrameRelay.
    - Jednotlivým kanálům se přidělí pravidelné časové úseky, ve kterých disponují celou šířkou pásma.
- **Kódový multiplex (Spread Spectrum)**
    - GSM, Wi-Fi.
    - Jednotlivé kanály používají pseudonáhodné kódování, ostatním se jeví jako šum.

Pokud vysílá více jak jedno KZ, dojde ke kolizi.

2.5. Media konvertory

- Převodník mezi různými druhy sítí – optická <-> metalická.
- Používají se, když potřebujeme změnit optický signál na elektrický.

2.6. PoE (využití, aktivní/pasivní, dodávaný výkon, vyjednávání napájení)

- PoE (Power over Ethernet) je napájení po datovém síťovém kabelu, bez nutnosti přivést napájecí napětí k přístroji dalším samostatným kabelem.
- Používá se u Wi-Fi AP, kamery, Raspberry Pi Clustery, ISP Wi-Fi přijímače.
- **Pasivní**
    - Napájení na nevyužitých vodičích v síťovém kabelu.
    - Kabel B – na vodičích 4-5 a 7-8.

- **Aktivní**
    - Fantomové napětí injektují na datové linky, lze tedy použít gigabitovou rychlost.
- **Vlastnosti**
    - 44 – 57 V.
    - Proud maximálně 550 mA, typicky 10-350 mA.
    - Běžně 370 W na 24 portovém switchi.
    - Switch většinou detekuje automaticky typ zařízení a dodává patřičný výkon bez konfigurace.

3. Optická vlákna

- *typy optických vláken a jejich vlastnosti (průměr, útlum, dosah)*
- *používané vlnové délky*
- *stavba optického vlákna*
- *způsoby spojování opt. vláken, typy konektorů*
- *optické transcievery (používané rychlosti, rozhraní, konektory)*
- *CWDM, DWDM (použití, princip)*

3.1. Typy optických vláken a jejich vlastnosti (průměr, útlum, dosah)

- **Optické vlákno** – tenké vlákno ze skla či průhledného plastu, které je schopné přenášet světelné záření.
- Tvoří naprostou většinu dálkových telekomunikačních sítí. Většinou o rychlosti **10, 40 či 100 Gbit**.
- Využívá princip **totálního odrazu paprsku** (**vidu**) **na rozhraní dvou prostředí s rozdílným indexem lomu**.
- Malý útlum oproti metalickým kabelům, imunní vůči elektrickému rušení.
- **Numerická apertura** (NA) – bezrozměrná veličina, která vyjadřuje schopnost optického vlákna navázat z okolí do svého jádra optický výkon. $A = n_0 * \sin\alpha$ (n_0 – index lomu prostředí vstupu světla, pro vzduch 1).
- **Vidová disperze (rozptyl)** – disperze způsobená lomem světla, kdy při každém lomu paprsků vyslaných pod různými vstupními úhly dojde k nepatrné odchylce dráhy jednotlivých vlnových délek. Projeví se různou délkou dráhy jednotlivých vidů v mnohavidových vláknech a tímto i různým zpožděním přenášené informace v cíli a ke zkreslení průběhu přijímaných dat.

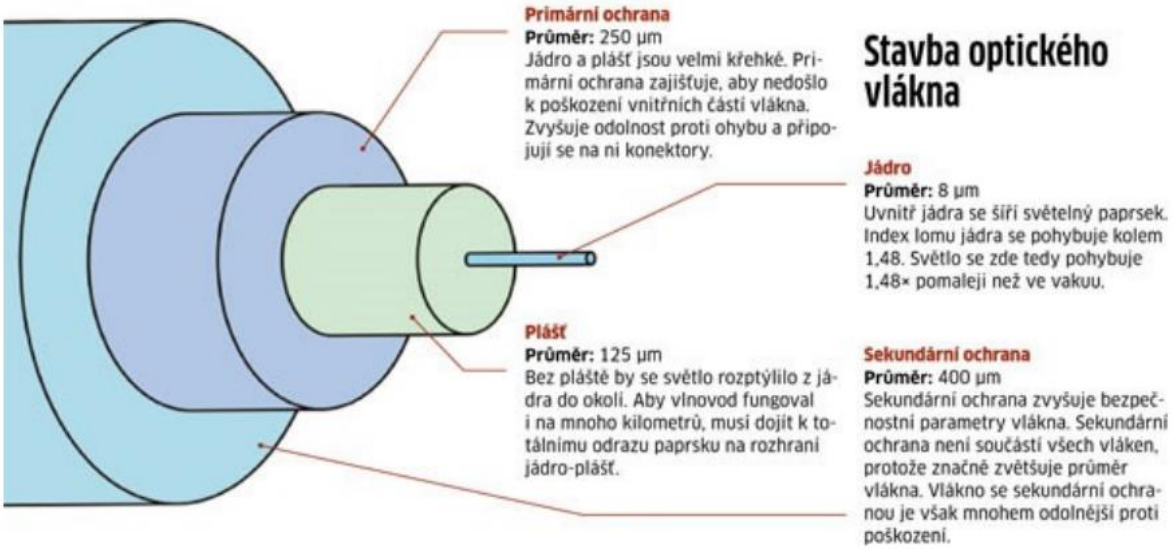
µm = mikro metr (0.01 m = 1 cm [$^{-2}$] = 10 mm [$^{-3}$] = 10000 µm [$^{-6}$]).

Typy

- **Mnohavidové optické vlákno (Multimode, MMF SI)**
  - Kratší vzdálenosti (uvnitř budov) – dosah 600 metrů.
  - Rychlost až 10 Gbps, vyšší ztráty.
  - Větší průměr jádra, více se odráží, tedy není tak kvalitní, ale je levnější.
  - Existují také s gradientním průběhem indexu lomu (MMF GI) – snížení vidové disperze (zkreslení impulsu), popisuje sinusovou křivku. Má tisíce tenkých vrstev, které se liší indexem lomu.
  - **Geometrie a průměrné vlastnosti:**
    - **Průměr jádra** – 50 / 62.5 µm.
    - **Průměr pláště** – 125 µm.
    - **Primární ochrana** – 250 µm.
    - **Měrný útlum** - 3 dB/km @ 850 nm.
    - **Vlnové délky** – 850, 1300 nm (infračervené, není viditelné).
  - **Typy (Optical Multi-mode):**
    - **OM1** – 200 MHz/km, oranžový.
    - **OM2** – 500 MHz/km, oranžový.
    - **OM3** - 2000 MHz/km, modro-zelený.
    - **OM4** - 3500 MHz/km, modro-zelený / fialový, až 40 / 100 Gbps.
- **Jednovidové optické vlákno (Singlemod, SMF)**
  - Přenosy na větší vzdálenosti – města, státy, kontinenty.
  - Rychlost větší než mnohavidové.
  - **Geometrie a průměrné vlastnosti:**
    - **Průměr jádra** – 9 µm.
    - **Průměr pláště** – 125 µm.
    - **Primární ochrana** – 250 µm.
    - **Měrný útlum** – 0.3 dB/km @ 1310 nm.
    - **Vlnové délky** – 1310, 1550 nm (infračervené, není viditelné).
  - **Typy (Optical Single-mode), žlutá barva:**
    - **OS1** – útlum 1 dB/km.
    - **OS2** – útlum 0.4 dB/km.

3.2. Stavba optického vlákna

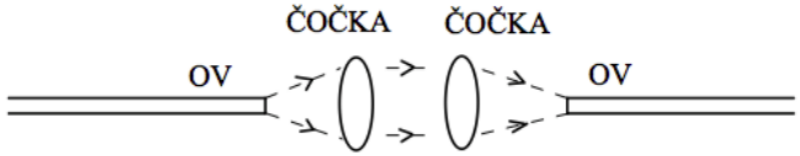
- Optická vlákna jsou obalena **primární ochranou zajišťující pružnost vlákna**, bez ní je velmi křehké.
- Sekundární ochrana značně zvyšuje tloušťku vlákna a proto zajišťuje dobrou ochranu. Její odstranění je běžné u propojovacích kabelů.

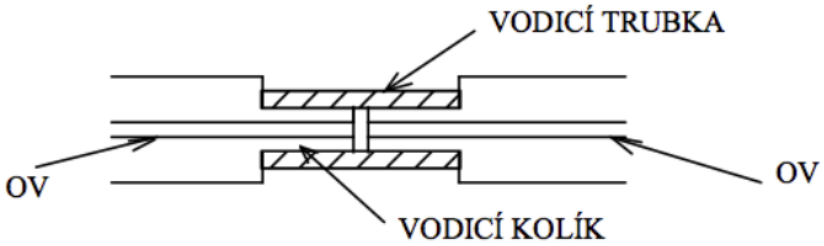


3.3. Způsoby spojování opt. vláken, typy konektorů

- **Permanentní spojení**
  - **Tavné svařování**
    - Nejnižší útlum (kolem 0.2 dB), dlouhá životnost, obtížné zejména kvůli malé velikosti jádra.
  - **Mechanické spojování**
    - Čelní spoje s přímým stykem spojovaných ploch.

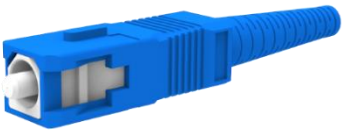
- **Semipermanentní**
    - Rozebíratelné spoje (konektory) požadují, aby se mechanické spoje nedotýkaly kvůli opotřebení ploch. Zároveň je nutné, aby mezi nimi byla minimální vzdálenost (maximálně 10 % průměru jádra).
    - Používají se pro spojování vláken, u kterých se předpokládá opakované rozpojování a spojování.
    - Vzácně se využívá spojování pomocí čoček. Tyto čočky jsou neúměrně drahé a složité na výrobu, zároveň ale dosahují minimálních útlumů – až 0,2 dB, podobné jako u svarů. (první obrázek).
    - Druhá skupina využívá mechanické vedení vlákna – pomocí v-drážky nebo pomocí vodícího kolíku a trubky. Typický útlum jsou menší než 1 dB.





Konektory

- **SC**
    - Malé ztráty, snadná montáž – lze pouze zamáčknout.
    - Vyšší cena.



- **LC**
    - Nízký, malé ztráty.
    - Vyšší cena.

- **ST**
    - Levný
    - Větší profil, nutné povolit před vytáhnutím, větší ztráty.

- **Pigtail**
  - Optické vlákno s připojeným konektorem.

- **Patch Cord**
  - Stejné jako UTP kabely, propojení na krátkou vzdálenost.

3.4. Optické transcievery (používané rychlosti, rozhraní, konektory)

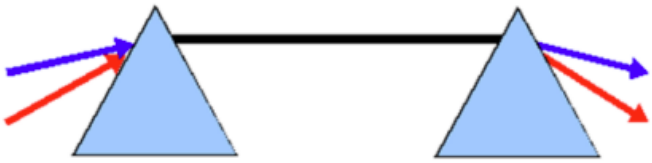
- Síťový prvek, který umožňuje překlad toku informací z jednoho typu sítě na typ jiný.
- **TRANSmitter** a **reCEIVER** - vysílač a přijímač.
- Využívají se nejčastěji při převodu metalické sítě na optickou, z bezdrátové na metalickou apod.
- Dnes už funkce transceiveru nebývá řešena jako samostatný hardwarový prvek, ale integruje se dnes do inteligentnějších zařízení (směrovač, access point).
- **TRANSMITTER + RECEIVER = Media konvertor**

- Přijímačem obvykle **fotodioda**.
- Vysílačem **LED** nebo **laserové diody**.
- **GBIC** (obr. 1)
  - Největší.
- **XFP** (obr. 2)
  - Hotswap.
  - 10 Gbps.

- **SFP (Small Form factor Pluggable)** (obr. 3)
  - 1 Gbps.
  - Označován jako mini-GBIC.
- **SFP+** (obr. 3)
  - 10 Gbps.
- **QSFP28** (obr. 3)
  - 100 (4x25) Gbps.

3.5. CWDM, DWDM (použití, princip)

- WDM (Wave Division Multiplexing) – vlnový multiplex.
- Do jednoho vlákna je pomocí více vlnových délek (barev) posláno více signálů, a tak dokáže vlákno přenášet **více informací** nebo být fullduplex.
- Používá se **optický hranol**, který smíchává / rozloží barvy.
- Spíše se používá u singlemode než u multimode.



  - **WDM** – 2 kanály.
  - **CWDM** - 16 kanálů.
  - **DWDM** – 40 kanálů.

4. Linková vrstva Ethernetu

- *typická struktura rámce*
- *chybovost, efektivita přenosu*
- *adresování (MAC)*
- *typy vysílání (unicast, broadcast, multicast)*
- *přístupové metody - principy kolizních a bezkolizních metod (TDMA, CSMA/CA, CSMA/CD)*
- *Ethernet (standardy, rychlosti)*

Oktet = byte.

Zajištění komunikace mezi dvěma nebo více uzly propojenými datovým spojem.

4.1. Typická struktura rámce

- **Nejpoužívanější Ethernet II rámec:**

Preambule	Hlavička	Paket	Patička
Synchronizace přijímacích stanic, počítá se spíše ale do L1	Adresa příjemce a odesílatele + specifikace vloženého protokolu	Vlastní přenášená data	Kontrolní součet (Frame Check Summary – FCS)
8 B	(MAC – 2x6 B + typ 2 B) = **14 B**	**46 B – 1500 B**	**4 B**

- **Maximální velikost (bez preambule)** – 1500 B + 18 B = **1518 B**
- **Minimální velikost (bez preambule)** – 46 B + 18 B = **64 B**
- **Minimální velikost** je **stanovena proto**, že dříve muselo být dostatek času na to, aby vysílač detekoval kolizi.
- **Maximální velikost** je **stanovena proto**, aby v případě chyby při přenosu nebylo nutné vysílat tolik informací.

4.2. Chybovost, efektivita přenosu

Chybovost:

- **q**
  - Pravděpodobnost chyby.
  - q = 0.0000001 (jeden bit z deseti milionů nebude přenesen správně).
- **p = 1 - q**
  - Pravděpodobnost správného (bezchybného) přenosu bloku.
  - **Nemělo by klesnout pod 0.99.**
  - Pravděpodobnost správného přenosu 1 kB dlouhého bloku dat:
    - 1 kB = 8192 b = p^{8192} = $(0.9999999)^{8192}$ = 0.9991
    - Pamatovat si **7 devítek** (1 špatný na 10 milionů bitů).

Efektivita:

- $\boldsymbol{efektivita} = \frac{\text{užitečná data}}{\text{celková data rámce}} * pravděpodobnost\ bezchybného\ přenosu^{délka\ bloku} * 100\ [\%]$
- Neměla by klesnout pod 70 %.

4.3. Adresování (MAC)

- **48 bitů (6B)**, zápis **hexadecimálně**, oddělena většinou **pomlčkou** či dvojtečkou
- **00-00-64-65-73-74**
- **První tři oktety** – výrobce nebo skupinová multicast adresa.
  - 0. bit z 1 bajtu.
    - **0** – výrobce.
    - **1** – multicast adresa.
- **Poslední tři oktety** – lokální jedinečnost.
- **Broadcast fyzická adresa.**
  - Oběžník pro všechny v LAN na L2.
  - **FF-FF-FF-FF-FF-FF**

4.4. Typy vysílání (unicast, broadcast, multicast)

- **Unicast**
  - Adresace jednoho zařízení, které je unikátní.
- **Multicast**
  - Adresace skupiny.
  - Nejčastěji na úrovni LAN – lokální multicast.
  - Video streaming.
- **Broadcast**
  - Adresace všech zařízení.
  - Volné šíření jen v určité časti sítě, jinak by vznikl pěkný zmatek.
  - ARP (získání MAC z IP adresy), DHCP (automatická konfigurace sítě).

4.5. Přístupové metody - principy kolizních a bezkolizních metod (TDMA, CSMA/CA, CSMA/CD)

Časový multiplex (TDMA - Time Division Multiple Access)

- ISDN (komunikace po telefonní lince – digitál na analogu), FrameRelay.
- Jednotlivým kanálům se přidělí pravidelné časové úseky, ve kterých disponují celou šířkou pásma, ve které mohou vysílat.

CSMA – metody s vícenásobným kolizním přístupem a nasloucháním nosné.

CSMA/CA

- Carrier Sense Multiple Access with Collision Avoidance
- Před začátkem vysílání paketu stanice určitý čas poslouchá, zda je přenosové médium volné. Pokud ano, může zahájit vysílání. Pokud ne, čeká náhodnou dobu a následně znovu ověřuje, zda může vysílat.
- Neumí detekovat kolize.
- Některé dokážou ověřit, zda zařízení data přijalo.
- Uplatnění u Wi-Fi.

CSMA/CD

- Stanice i při vysílání rámce neustále sledují stav média a jsou schopny detekovat vznik kolize. Metody CD využívají tuto schopnost detekce kolize k (téměř) okamžitému ukončení vysílání.
- Významně zvyšuje efektivitu využití média, protože stanice dále nepokračují ve vysílání rámce, který je již stejně poškozený, a tak zkrátí kolizní slot.
- **Jam** – signál, který vysílá stanice, která první rozeznala kolizi a cílem je ukončit co nejrychleji kolizní provoz.
- V případě kolize počká náhodně dlouhou dobu a začne znova vysílat. Pokud ani na 15. pokus neodvysílá, pak vysílání přeruší.
- Uplatnění u Ethernetu.

4.6. Ethernet (standardy, rychlosti)

Ethernet I je IEEE 802.3.

10 Mbps	1982	**Ethernet II**		
	1985	**IEEE 802.3a**	10Base2	Tenký koaxiál
100 Mbps	1995	**IEEE 802.3u**	100BaseTX/T4/FX	TP / TP FD / optika
1 Gbps	1998	**IEEE 802.3z**	1000Base-X	Optika
	1999	**IEEE 802.3 ab**	1000BaseT	TP
10 Gbps	2003	**IEEE 802.3 af**	PoE 19.95W	PoE
	2006	**IEEE 802.3 an**	10GBase T	UTP

5. Aktivní prvky

- *popis aktivních prvků fyzické vrstvy a jejich funkce (mediakonvertor, opakovač)*
- *popis aktivních prvků linkové vrstvy a jejich funkce (most, switch)*
- *popis aktivních prvků síťové vrstvy a jejich funkce (router, L3 switch)*
- *kolizní doména, broadcast doména, mikrosegmentace, plně duplexní provoz*
- *management přepínačů a HW routerů*
- *VLAN (access, trunk)*
- *paměti CAM/TCAM*
- *ACL*

5.1. Popis aktivních prvků fyzické vrstvy a jejich funkce (mediakonvertor, opakovač)

- **Mediakonvertor**
  - Převodník mezi různými druhy sítí – optická <-> metalická.
  - Používají se, když potřebujeme změnit optický signál na elektrický.
  - **TRANSMITTER + RECEIVER = Media konvertor.**
- **Opakovač**
  - Aktivní síťový prvek, který přijímá zkreslený, zašuměný nebo jinak poškozený signál a opravený, zesílený a správně časovaný ho vysílá dále.
- **Hub**
  - Pracuje na nejnižší připojené přenosové rychlosti.
  - Zvládá pouze half duplex.
  - Kolizní doména – rozbočuje všechny rámce všude a vzniká neefektivní provoz.
  - Vlastně úplně useless.

5.2. Popis aktivních prvků linkové vrstvy a jejich funkce (most, switch)

- **Most**
  - Vytváří "most" mezi dvěma segmenty sítě (má pouze dva porty, víceportový bridge je switch – ne teda podle Šedy). Přenosovým médiem je většinou tenký koaxiální kabel (topologie BUS) nebo nověji se používá bridge pro přepínání mezi různými typy přenosových médií.
  - Lze například použít mezi TP a Wi-Fi.

- **Switch (přepínač)**
  - Základní aktivní prvek LAN.
  - Jedná se víceportový bridge.
  - Optimalizován na výkon, je full duplex.
  - Každé připojené zařízení má vlastní kolizní doménu.
  - Nemohou vzniknout kolize, switch vždy propojí dvě KZ mezi sebou (může ale být zkombinováno tak, že Rx je připojeno jinam než Tx, takže jedno KZ může být připojeno na 2 zařízení, ale nedělá s nimi stejnou operaci).
  - **Mikrosegmentace** – na porty switche je připojeno pouze jedno zařízení. Neobsahuje víceportové opakovače ani sběrnice.
  - Má zmapované, na jakém portu je jaké zařízení pomocí MAC adres.
  - **MAC Adress Table**
    - Přiřazení fyzických adres k portům.
    - Paměť typu CAM/TCAM – asociativní paměť (používá klíče) nebo adresovatelná obsahem.
    - Velmi rychlá paměť – tedy nízká latence. Velká cena a velký příkon.
    - TCAM – lze hledat současně a lze nastavit parametr X (oproti 0 a 1 vyjadřuje to, že na něm nezáleží) – ternální rozhodování.
    - Pokud není MAC v tabulce, posílá se na všechny porty (tedy vlastně stejně jako HUB, proto na začátku pracuje i pomaleji).
    - Velikost MAC Address Table – jednotka kMAC – běžná hodnota 8 kMAC.

        - **Rozdělení tabulek:**
            - **Statické** – definované správcem sítě, každým přemístěním počítače nebo změnou konfigurace je nutné změnit nastavení.
            - **Dynamické** – během své práce switch automaticky vytváří – **učící se switch**. Při neaktivitě vyprší v řádů desítek sekund.
    - **Další parametry:**
        - **Rychlost vnitřní sběrnice** (v řádek Gbps) – jak se dokáže rychle přepínat.
        - **Propustnost switche** (přenosová kapacita. V Mpps (paket per sec). Běžné hodnoty 60-80 Mpps pro 64 B rámce.
        - **Buffery** – musí být, aby každé KZ mohlo mít jinou přenosovou rychlost. Řízení toku dat - v případě zaplnění stanovené hranice – simulovaná kolize – backpressure a následné zastavení nových rámců.
        - **Autonegace** – nastavení parametrů portu dle možnosti KZ – nastavení přenosové rychlost, režimu přenosu full duplex / half duplex a zda je port aktivní.
        - **Management switche** vs **switche bez správy** (**transparentní**).
            - Management pomocí RS232 či ethernetu.
            - Většinou console administrace (SSH či telnet).
            - Cisco – iOS – módy **User Exec**, **Privilaged Exec** a **Global Configuration**.

5.3. Popis aktivních prvků síťové vrstvy a jejich funkce (router, L3 switch)

L3 – směrování paketů pomocí IP.

- **Router (směrovač)**
    - Směrování síťového provozu mezi různými sítěmi.
    - Posílá data na základě IP adresy.
    - Umožňuje filtrování provozu a zajištění bezpečnosti sítě.
- **L3 Switch**
    - Router s L2 switchem, umožňuje přeposílání i pomocí MAC adres.
    - Má i tabulku IP adres (tedy dokáže přeposílat i pomocí IP adres).

Druhy směrování (algoritmy pro směrování):

- **Statické**
  - Statické směry.
  - Defaultní směr.
- **Dynamické**
  - Izolované.
  - Distribuované.
    - Vector Distance.
    - Link State.
  - Hierarchické.

5.4. Kolizní doména, broadcast doména, mikrosegmentace, plně duplexní provoz

- **Kolizní doména** – zařízení (část sítě), která mohou vysílat ve stejnou chvíli a způsobit tak kolizi.
- **Broadcast doména** – všechny zařízení se stejnou síťovou adresou. Šíření blokuje router, proto odděluje broadcast domény.
- **Mikrosegmentace** – viz switch.
- **Plně duplexní provoz** – data může zařízení zároveň vysílat i přijímat.

5.5. VLAN (access, trunk)

- **VLAN (Virtual Local Area Network)**
- Uzavřená skupina uživatelů, která je tvořena skupinou fyzických portů, které patří do **logické skupiny**.
- Většinou IP subnet (podsíť LAN).
- Každá VLAN má vlastní **broadcast doménu**, používá se tedy ke zmenšení velikosti defaultní.
- Každá VLAN má také vlastní AS a BA.

- **Cíle:**
  - Usnadnění správy sítě.
  - Zvýšení bezpečnosti a výkonu.
  - Cíl učinit logickou organizaci sítě nezávislou na fyzické vrstvě.
- **Vlan ID**
  - 12bitové číslo, které se vyskytuje součástí rámce v IEEE 802.1q.
- **Access Port**
  - Pouze jedna VLAN (většinou vlan1), ostatní provoz blokován.
- **Trunk Port**
  - Podporuje více VLAN.
  - Konfigurace pouze na switchi.

5.6. ACL

- **ACL** (Access control list).
- **Přístupové seznamy** – dokáže omezit například podle MAC adresy.
- Vlastně takový firewall.
- Dokáže určovat, jak kdo může přistupovat na daný port či IP adresu.

6. Síťová vrstva a směrování

- *služby a základní pojmy*
- *nehomogenní prostředí, internetworking*
- *logická adresa*
- *síťové protokoly*
- *přímé/nepřímé směrování, metrika*
- *dynamické směrování (RIPv2, RIPng, OSPFv2, OSPFv3)*
- *protokol ARP a NDP*

Službou síťové vrstvy L3 – Address and best path – nejefektivnější přenos dat mezi sítěmi.

Paket (packet) v překladu znamená balíček a jedná se o formátovaný blok dat, který se přenáší v počítačové síti. O paketech se mluví v souvislosti se síťovou vrstvou. Paket obsahuje IP adresu, další atributy a data. Zabalí se do rámce a následně putuje sítí.

Rámec (frame) je to, co skutečně putuje v síti. Rámce vznikají až na fyzické vrstvě síťového rozhraní. Název naznačuje, že se spíše než o objekt jedná o časový úsek. Rámců existuje více typů, nejpoužívanější je Ethernet II, který umí přepravovat TCP/IP i IPX/SPX.

6.1. Služby a základní pojmy

Všechny tyto pojmy jsou detailně rozebrány přímo ve svých kapitolách.

- **Transportní vrstva**
  - L4 zajišťuje end-to-end connection.
  - Multiplexing / demultiplexing dat – pomocí jedné cesty předává / dostává data od více aplikací.
  - Umožňuje adresovat přímo aplikace (například v protokolech TCP/IP pomocí čísel portů).
  - Poskytuje transparentní, spolehlivý přenos dat s požadovanou kvalitou.
  - Vyrovnává různé vlastnosti a kvalitu přenosových sítí.
  - Provádí převod transportních adres na síťové, ale nestará se o směrování.

- **IP adresa**
  - Unikátní adresa, která jednoznačně identifikuje síťové rozhraní v počítačové síti, která používá IP protokol.
  - IP adresa slouží k rozlišení síťových rozhraní připojených k počítačové síti.
- **Maska podsítě**
  - Maska podsítě nám pomáhá určit rozdělení sítě na podsítě.
  - Určuje, která část IP adresy je síťová, a která pro hosty.
  - Zápis je stejný jako u IP adresy, ale platné hodnoty jsou pouze ty, které mají v binárním tvaru zleva jedničky a zprava nuly.
  - Pomocí masky sítě router rozhoduje o směrování (anglicky routing) IP datagramů.
- **Adresa sítě**
  - IP adresa se skládá ze dvou částí net - ID (adresa sítě) a host - ID (adresa počítače).
  - Podle toho, jak jsou jednotlivé sítě rozlehlé (kolik mají hostů) rozlišujeme tři hlavní třídy IP adres - A, B a C.

6.2. Nehomogenní prostředí, internetworking

- **Nehomogenní (heterogenní) síť**
  - Propojení více různých sítí s různými principy přenosu.
  - Nehomogenní = nestejnorodý, heterogenní = různorodý.
  - Propojení více různých sítí s různými principy přenosu (nemusí být přeci vše Ethernet...).
- **Ethernet**
  - Je název souhrnu technologií pro počítačové sítě (LAN, MAN) z větší části standardizovaných jako IEEE 802.3, které používají kabely s kroucenou dvoulinkou či optické kabely.
- **Token Ring**
  - Je technologie lokální sítě (LAN), vyvinutá počátkem 80. let 20. století firmou IBM.
  - Byla standardizována jako IEEE 802.5. Zpočátku byla tato technologie poměrně úspěšná, ale počátkem 90. let byla postupně vytlačována technologií Ethernetu.

- **Internetworking**
    - Vzájemné propojování celých sítí i jednotlivých segmentů.
    - Propojením vzniká tzv. internet (tj. jakékoliv propojení alespoň dvou sítí nebo jejich částí).
    - Internet (s velkým I) je pak celosvětová síť propojující jednotlivé sítě, tak jak ji známe dnes.

6.3. Logická adresa

- **Logická adresa** – IPv4 nebo IPv6 adresa.
- **Fyzická adresa** – MAC.
- Hlavním rozdílem mezi logickou a fyzickou adresou je tedy ten, že **logická adresa** se používá **pro směrování dat v síti** a identifikaci konkrétní podsítě, zatímco **fyzická adresa** slouží pro **identifikaci konkrétního síťového rozhraní** (a tedy i zařízení) v rámci této podsítě.

6.4. Síťové protokoly

IPv4

- 32 bitů (4 B), odděleno tečkou mezi byty (.), psáno dekadicky.
- Například: 192.168.0.1.

Třída A	Třída B	Třída C	Třída D	Třída E
0.-127.	128.-191.	192.-223.	224.-239. (Lokální multicast)	240.-255. (Rezerva)
10.0.0.0 – 10.255.255.255	172.16.0.0 – 172.31.0.0	192.168.0.0 – 192.168.255.255	-	-

Vyhrazené adresy

- Nespecifikovaná adresa – 0.0.0.0.
- Lokální smyčka – 127.0.0.1.

- **Adresa sítě**
    - Část logické IP adresy, která identifikuje konkrétní síť v rámci celé sítě.

- **Maska**
  - Určuje, které bity v logické IP adrese identifikují adresu sítě a které identifikují konkrétní zařízení v této síti.
  - Maska sítě se zapisuje ve formátu číselného rozsahu nebo pomocí prefixu.
  - Například maska sítě 255.255.255.0 se může zapsat také jako /24.
- **Broadcast adresa**
  - Speciální adresa, která se používá pro odeslání dat všem zařízením v dané síti. Tato adresa má hodnotu všech bitů sítě nastavenou na 1.
  - Například pokud máme IP adresu 192.168.1.25 a masku sítě 255.255.255.0, broadcast adresa bude 192.168.1.255.
- **Gateway**
  - Adresa sítě, která slouží jako východ pro data směřovaná mimo tuto síť. Tento prvek propojuje jednu síť s jinou a umožňuje zařízením v této síti komunikovat s jinými sítěmi, včetně internetu. Obvykle se jedná o IP adresu routeru nebo brány.

IPv6

- 128 bitů (16 B), odděleno dvojtečkou (:) po 2 B (8 skupin), psáno hexadecimálně.
- Například: fedc:ba98:7654:3210:fedc:ba98:7654:3210
- Standardně 64 bitů část sítě, 64 bitů zařízení, ale není to podmínka.
- Není zpětně kompatibilní s IPv4.
- **Vyhrazené adresy:**
  - ::/128 – nedefinovaná adresa.
  - ::1/128 – lokální smyčka (loopback).

6.5. Přímé/nepřímé směrování, metrika

Přímé směrování

- Cíl je v LAN.
- Stačí vytvořit rámec, který obsahuje fyzické adresy cíle a zdroje v místní síti a IP paket je takto přenesen přímo k cíli.

Nepřímé směrování

- Není v LAN, směřuje se na gateway.
- Ve směrovací tabulce se použije záznam s nespecifikovanou adresou (0.0.0.0) s významem “pro všechny ostatní sítě“.
- Rámec je vždy označen fyzickou adresou skutečného odesilatele na dané trase a fyzickou adresu nejbližšího příjemce.
- Paket je vždy označen IP adresou originálního odesilatele a koncového příjemce **– funguje tedy mezi více sítěmi.** Obsahuje rámec. Dá se většinou zaměnit s IP datagramem.

Směrovací tabulka

- Obsahuje informace, které jsou nutné při rozhodování o směrování, jako adresu cílové sítě, masku, metriku (to, jak je daleko), stáří.
- Má ji každý směrovač.
- V Cisco iOS příkaz sh ip route.
- Výchozí směrování - pokud router neví, kam data poslat, posílá na **gateway**.

Metrika

- Jednotlivé routy mají metriku (1 až 9999), která určuje jejich prioritu.
- Čím nižší hodnota, tím větší priorita.
- Například u RIP označuje počet skoků k cíli.

6.6. Dynamické směrování (RIPv2, RIPng, OSPFv2, OSPFv3),

Druhy směrování (algoritmy pro směrování):

- **Statické**
  - Statické směry.
  - Defaultní směr.
- **Dynamické**
  - Izolované.
  - Distribuované.
    - Vector Distance.
    - Link State.
  - Hierarchické.

RIPv2

- Protokol typu Vector Distance (zná pouze své sousedy).
- Snaží se určit nejkratší cestu v síti.
- Metrikou směrování je počet skoků k cílové síti(max 15 skoků).
- Počet skoků nesmí přesáhnout 15, jinak je neplatný.

RIPng

- Přidání podpory IPv6.

OSPFv2

- Protokol typu Link State.
- Zná strukturu celé sítě, informuje ostatní směrovače.
- Určí nejefektivněji cestu.
- Metrika je součtem cen jednotlivých úseků (výpočet z rychlosti).
- Jen pro IPv4.

OSPFv3

- Podpora IPv6.

6.7. Protokol ARP a NDP

ARP

- Address Resolution Protocol.
- Přiřazení IP adresy k MAC adrese.
- Šířen jako broadcast linkové vrstvy (L2) určený všem KZ v síti.
- ARP odešle dotaz (ARP request) obsahující hledanou IP adresu a údaje o sobě (vlastní IP adresu a MAC adresu).
- Dotaz se posílá linkovým broadcastem – na MAC adresu identifikující všechny účastníky dané lokální sítě.
- ARP dotaz nepřekročí hranice dané podsítě, ale všechna k ní připojená zařízení dotaz obdrží a jako optimalizační krok si zapíší údaje o jeho odesilateli.
- Vlastník hledané IP adresy pak odešle tazateli ARP odpověď (ARP reply) obsahující vlastní IP adresu a MAC adresu.

NDP (Neighbor Discovery Protocol)

- Nahrazuje ARP v IPv6. Ověřuje, zda máme jedinečnou adresu v síti.
- Odpovědný za automatickou konfiguraci adres uzlů, objev zjišťování uzlů na lince, určování adresy linkové vrstvy jiných uzlů, hledání duplicit adres, hledání dostupných směrovačů a DNS serverů.
- Pro objevování sousedů. U IPv6 se využívá pro automatickou konfiguraci.

DHCP

- DHCP protokol umožňuje prostřednictvím DHCP serveru nastavovat stanicím v počítačové síti sadu parametrů nutných pro komunikaci pomocí IP protokolu.
- Obsahuje IP adresu, masku sítě, výchozí bránu, DNS.
- Pokud zařízení nezná DHCP server, vyšle broadcast paket na adresu 255.255.255.255. DHCP server odpoví s přidělenou IP a dalším nastavením.

DHCPv6

- Síťový protokol, který umožňuje počítačům získat IPv6 adresu, případně jiné parametry sítě.
- Umí spravovat více IP adres pro jedno rozhraní.
- Je jednodušší, protože klient využívá automatické konfigurace lokální linkové IPv6 adresy.
- Klient posílá zprávy na skupinové adresy, nikoliv všesměrovým vysíláním.
- Nedokáže poskytnout informaci o výchozí bráně.

RA

- Hosti se vysláním Router solicitation zprávy snaží na připojené lince najít směrovače (routery).
- Směrovače odpoví Router advertisement paketem ihned po obdržení této zprávy.

7. IP adresy a způsoby řešení nedostatku IPv4 adres

- *složení, syntaxe zápisu (IPv4, IPv6), rozdělení IPv4 do tříd*
- *rozdíly mezi IPv4 a IPv6*
- *způsoby získání adresy (DHCP, DHCPv6, SLAAC)*
- *základní údaje nutné pro směrování, maska a její použití*
- *řešení nedostatku IPv4 adres (CIDR, subnetting, privátní adresy, NAT, proxy)*
- *IP datagram (hlavička, TTL/hop limit, …), fragmentace*

7.1. Složení, syntaxe zápisu (IPv4, IPv6), rozdělení IPv4 do tříd

IPv4

- 32 bitů (4 B), odděleno tečkou mezi byty (.), psáno dekadicky.
- Maximální hodnota 255, protože se jedná o 1 bajt.
- Například: 192.168.0.1.

Třída A	Třída B	Třída C	Třída D	Třída E
0.-127.	128.-191.	192.-223.	224.-239. (Lokální multicast)	240.-255. (Rezerva)
10.0.0.0 – 10.255.255.255	172.16.0.0 – 172.31.0.0	192.168.0.0 – 192.168.255.255	-	-

Vyhrazené adresy

- Nespecifikovaná adresa – 0.0.0.0.
- Lokální smyčka – 127.0.0.1.

- **Adresa sítě**
  - Část logické IP adresy, která identifikuje konkrétní síť v rámci celé sítě.

- **Maska**
  - Určuje, které bity v logické IP adrese identifikují adresu sítě a které identifikují konkrétní zařízení v této síti.
  - Maska sítě se zapisuje ve formátu číselného rozsahu nebo pomocí prefixu.
  - Například maska sítě 255.255.255.0 se může zapsat také jako /24.

- **Broadcast adresa**
    - Speciální adresa, která se používá pro odeslání dat všem zařízením v dané síti. Tato adresa má hodnotu všech bitů sítě nastavenou na 1.
    - Například pokud máme IP adresu 192.168.1.25 a masku sítě 255.255.255.0, broadcast adresa bude 192.168.1.255.
- **Gateway**
    - Adresa sítě, která slouží jako východ pro data směřovaná mimo tuto síť. Tento prvek propojuje jednu síť s jinou a umožňuje zařízením v této síti komunikovat s jinými sítěmi, včetně internetu. Obvykle se jedná o IP adresu routeru nebo brány.

IPv6

- 128 bitů (16 B), odděleno dvojtečkou (:) po 2 B (8 skupin), psáno hexadecimálně.
- Například: fedc:ba98:7654:3210:fedc:ba98:7654:3210
- Standardně 64 bitů část sítě, 64 bitů zařízení.
- Není zpětně kompatibilní s IPv6.
- **Vyhrazené adresy:**
    - ::/128 – nedefinovaná adresa.
    - ::1/128 – lokální smyčka (loopback) .
- **Lze zkrátit:**
    - **Vynecháním nul na začátku:**
        - ..:0010:.. lze přepsat jako ..:10:.. .
    - **Vynecháním nul uprostřed:**
        - 2001:0000:0000:0000:0718... jako 2001::0718....

7.2. Rozdíly mezi IPv4 a IPv6

Link-local - možnost, jak zařízení dokážou komunikovat mezi sebou bez směrovače v jedné síti.

IPv4

- **Celkem adres:** 2^{32} = 4,294,967,295
- **Multicast**
  - Slouží například ke sdílení videí, funguje na adresách 224. - 239..
  - Nefunguje v jiné sítí (TTL je nastaveno na 1).
- **Broadcast**
  - Používá se například pro ARP, či DHCP.
  - Poslední adresa v rozsahu sítě.
- **Veřejné, privátní a link-local adresy**
  - Pro privátní adresy vyhrazeny 3 rozsahy (viz tabulka k IPv4). Používají se 24bitové, 20bitové či 16bitové bloky pro jejich vytvoření.
  - Link-local se nastaví, pokud není žádný DHCP server a mají adresu 169.254.0.0/16.

IPv6

- **Celkem adres:** 2^{128} = 340,282,366,920,938,463,463,374,607,431,768,211,456
- **Běžná délka prefixu:** /64, lze nastavit jakákoliv mezi /0 a /128
- **Multicast**
  - Stejné jako v IPv4, ale má rozšířené adresy.
  - Používá se pro optimalizace dodatkových služeb, přenosu zařízení, konfiguraci.
- **Broadcast**
  - Je nahrazen mutlicastem s hodnotou FF02::1 (All-nodes), jinak byl zrušen.
- **Veřejné, privátní a link-local adresy**
  - **Privátní adresy** v IPv6 by se dle mého názoru neměly používat, protože to jde proti celé filozofii IPv6 (proč mít 340 idk adres) (fun fact: to číslo ani nemá v tabulce SI násobek, protože je moc velké) a používat privátní IPv6 adresy, když tohle se má omezit firewallem. Každopádně stejně přesto existují, protože idk:

- fd00::/8 - prefix pro **lokální privátní sítě**, používá náhodné 40bitové číslo v prefixu.
- fe80::/10 - prefix pro **link-local** adresy.
    - Převádění MAC adresy na identifikátor rozhraní (EUI-64):
    - MAC adresa: 11:22:33:44:55:66.
    - Změníme 1. bit (druhý zprava) na 1.
    - 00010001 -> 00010011 = 13.
    - Změníme první oktet: 13:22:33:44:55:66.
    - Přidáme konstantu FF:FE doprostřed a na začátek FE80::.
    - fe80::13:22:33:ff:fe:44:55:66.

ARP

- Address Resolution Protocol.
- Přiřazení IP adresy k MAC adrese.
- Šířen jako broadcast linkové vrstvy (L2) určený všem KZ v síti.
- ARP odešle dotaz (ARP request) obsahující hledanou IP adresu a údaje o sobě (vlastní IP adresu a MAC adresu).
- Dotaz se posílá linkovým broadcastem – na MAC adresu identifikující všechny účastníky dané lokální sítě.
- ARP dotaz nepřekročí hranice dané podsítě, ale všechna k ní připojená zařízení dotaz obdrží a jako optimalizační krok si zapíší údaje o jeho odesilateli.
- Vlastník hledané IP adresy pak odešle tazateli ARP odpověď (ARP reply) obsahující vlastní IP adresu a MAC adresu.

NDP

- Nahrazuje ARP v IPv6. Ověřuje, zda máme jedinečnou adresu v síti.
- Odpovědný za automatickou konfiguraci adres uzlů, objev zjišťování uzlů na lince, určování adresy linkové vrstvy jiných uzlů, hledání duplicit adres, hledání dostupných směrovačů a DNS serverů.
- Pro objevování sousedů. U IPv6 se využívá pro automatickou konfiguraci.

7.3. Způsoby získání adresy (DHCP, DHCPv6, SLAAC)

DHCP

- DHCP protokol umožňuje prostřednictvím DHCP serveru nastavovat stanicím v počítačové síti sadu parametrů nutných pro komunikaci pomocí IP protokolu.
- **Obsahuje IP adresu, masku sítě, výchozí bránu, DNS.**
- Pokud zařízení nezná DHCP server, vyšle broadcast paket na adresu 255.255.255.255. DHCP server odpoví s přidělenou IP a dalšími informacemi.
- Zařízení je identifikováno pomoci své **MAC adresy**.
- DHCP server může počítači připojovat stále stejnou pevnou IP adresu nebo může IP adresy přidělovat stanicím tak, jak jsou volné a jak o ně stanice DHCP dotazem žádají.
- **Ruční alokace** – nepoužívá se DHCP, ale přidělí se ručně.
- **Statická alokace** – DHCP přiděluje při požádání vždy stejnou adresu.
- **Dynamická alokace** – přidělí z adresního rozsahu nějakou z nepoužívaných.
- **Lease time** – standardně 24 hodin než odpojenému zařízení expiruje jeho IP adresa.
- **Příklady**: Windows Server DHCP, Linux ISC DHCP, Cisco iOS, MikroTik RouterOS (prakticky každý router má svého klienta).

SLAAC (RA)

- Směrovač v síti v pravidelných intervalech informuje všechny připojené uzly v síťovém segmentu, v jaké síti se nacházejí a který směrovač mají použít pro pakety, které mají putovat do Internetu (RA – Router Advertisment).
- Nově připojené zařízení může vyslat do sítě požadavek (RS – Router Solicitation) se žádosti o informaci, ve které síti se nachází a kudy vede cesta ven.
- Celý mechanismus autokonfigurace je součástí specifikace Neighbor Discovery for IP Version 6, a veškerá komunikace probíhá s využitím protokolu ICMPv6.
- Neposkytuje ovšem informace o DNS, takže je celkem useless.

DHCPv6

- Umí spravovat více IP adres pro jedno rozhraní.
- Je jednodušší, protože klient využívá automatické konfigurace lokální linkové IPv6 adresy.
- Klient posílá zprávy na skupinové adresy, nikoliv všesměrovým vysíláním.
- Klient je identifikován prostřednictvím jedinečného identifikátoru DUID (DHCP unique identifier).
- Zprávy pro počáteční přidělení adresy se jmenují: Solicit, Advertise, Request, Reply.
- Nedokáže poskytnout informaci o výchozí bráně (default route, default gateway) – tu klient obdrží pomocí oznámení směrovače (Router Advertisment).

Statická konfigurace

- Musíte nastavit ručně všechny parametry.
- Problém ovšem může nastat, pokud dvěma zařízením nastavíme stejnou IP adresu.

7.4. Základní údaje nutné pro směrování, maska a její použití

Určení adresy sítě a broadcastu (IPv4)

- Broadcast adresu získáváme z masky sítě.
- Pokud je adresa sítě 192.168.1.0 a maska 255.255.255.240, pak broadcast adresa bude 192.168.1.15 (/28 – chybí 4 bity – 2^4 = 16 – 256-16 = 240).

Vliv masky, resp. délky prefixu na velikost sítě

- **Maska -** /26 – na sítě jsou 2 bity, takže 4 podsítě, v každé 62 hostů.
- **Maska -** /28 – na sítě jsou 4 bity, takže 16 podsítí, v každé 14 hostů.

Rozpoznání rozdílných sítí

- Probíhá na základě porovnání adresy sítě, masky sítě a adresy cílového zařízení.

7.5. Řešení nedostatku IPv4 adres (CIDR, subnetting, privátní adresy, NAT, proxy)

CIDR

- **Ve zkratce adresa může mít libovolný prefix. Ne jenom /8 či /16 čí /24.**
- Podle tříd A, B a C existují jen tří možné způsoby rozdělení IP adresy na adresu sítě a adresu uzlu.
- Odstranila se neefektivnost při přidělování IP adres - například síť s pouhými čtyřmi uzly musela dříve dostat jednu skupinu adres třídy C, neboli 256 jednotlivých IP.
- Významným opatřením na cestě ke zpomalení úbytku IP adres bylo odbourání dosavadního členění IP adres na třídy A, B a C, a umožnění jejich přidělování i po jiných jednotkách.
- K IP adresám se připojí explicitní údaj o poloze pomyslné dělící čáry – maska sítě.
- **Důvod zavedení** – zpomalit vyčerpávání IPv4 adres a omezit růst směrovacích tabulek na směrovačích v Internetu.
- **Spíše pro veřejné adresy.**

Dělení sítě na podsítě (Subnetting)

- Vznik podsítí - Rozdělení jedné síťové adresy na několik síťových adres – **spíše pro privátní adresy**.
- Dělící čára se posune dále směrem doprava, než odpovídá její pozice dle příslušné třídy IP adresy.
- Konkrétní posunutí je definováno příslušnou maskou.
- S jedinou síťovou adresou třídy C vystačíme i pro více sítí.
- Nevýhodou je “neviditelnost“ podsítí z původní sítě – zvnějšku.
- **VLSM** – umožňuje použít různé velikosti podsítí – nemusí být všechno rozděleno stejně velce, může být například 1x /25 a 2x /26. Bez VLSM muselo být všechno stejné – tedy 2x /25 nebo 4x /26.

Privátní adresy (privátní síť)

- Privátní adresy jsou běžně používány pro domácí, kancelářské a podnikové lokální sítě (LAN), kde veřejné adresy (tj. globálně směrovatelné v Internetu) nejsou žádoucí nebo nejsou dostupné.
- Privátní rozsahy IP adres byly definovány jako nástroj pro zpomalení vyčerpání IPv4 adres. Nyní jsou též součástí nastupující generace pro Internet Protocol verze 6.
- Privátní adresy jsou označovány jako soukromé, protože nejsou globálně delegované, což znamená, že nejsou přiděleny žádné konkrétní organizaci a jimi adresované IP pakety nemohou být přenášeny přes veřejný Internet.
- Kdokoliv může používat tyto adresy bez jakéholiv schválení.
- Pokud takováto privátní síť potřebuje připojení k Internetu, musí používat buď překlad síťových adres (NAT), nebo proxy server.
- **Musí využít adresy z těchto rozsahů:**
    - **A** - 10.0.0.0 – 10.255.255.255
    - **B** - 172.16.0.0 – 172.31.255.255
    - **C** - 192.168.0.0 – 192.168.255.255

NAT

- **NAT** (Network Address Translation) zajišťuje překlad síťových adres mezi privátní a veřejnou sítí.
- Jedná se o funkci routerů, která umožňuje překládat adresy z vnitřního adresního rozsahu do veřejného a naopak. V důsledku se tak vnitřní adresy nedostanou nikdy do internetu.
- Omezuje přístup do vnitřní sítě.
- Funguje na 3. (síťové) vrstvě ISO/OSI modelu.
- Přesměrovává porty – například můžete pro port 8080 z Internetu spustit službu na vnitřní IP na portu 80 (web).
- **Princip NATu:**
    1. Klient vyšle požadavek na bránu vnitřní sítě.
    2. Router pakety zachytí, změní jejich IP adresu na svou vnější.
    3. Router pakety označí tak, že je odešle z náhodného TCP portu.
    4. Router si do tabulky zapíše, který port zvolil a který klient k němu patří.
    5. Při přijetí odpovědi provede router reverzní akci a pakety vrátí klientovi.

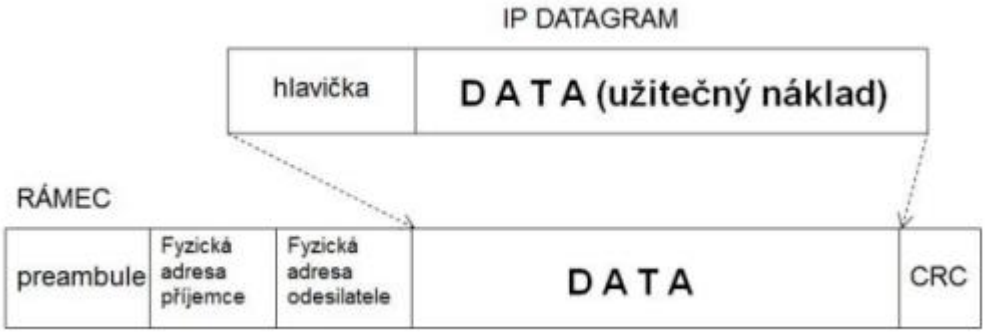
Proxy

- Aplikace předává na server požadavky a ten je vyřizuje, tedy chová se jako prostředník mezi uživatelem a serverem s poskytující službou.
- Pracuje na 7. (aplikační) vrstvě ISO/OSI – protože řeší požadavky aplikací, ne celého systému.
- Lze využít k blokování obsahu.
- Hlavní rozdíl mezi proxy a NAT spočívá v tom, že proxy server je umístěn mezi koncovým zařízením a internetem a slouží jako prostředník, zatímco NAT je umístěn mezi dvěma sítěmi a umožňuje překlad IP adres a portů. Proxy server může být použit k blokování nebo filtrování obsahu, zatímco NAT je obvykle používán k umožnění přístupu k internetu ze zařízení v privátní síti pomocí jediné veřejné IP adresy.
- Reverzní proxy – využití zejména pro webové služby a servery – mám jednu IP a po připojení reverzní proxy určí, na jaký server přistoupím – to může být například u webů podle doménového jména.

7.6. IP datagram (hlavička, TTL/hop limit, ...), fragmentace

IP datagram

- Linková vrstva přenáší **rámce**.
- **V rámci** lze přenést **paket** (objekt síťové vrstvy).
- **Paket** odpovídající protokolu TCP/IP nazýváme **IP datagram**.



Popis základních částí IPv4 a IPv6 hlavičky, velikost hlavičky

- **IPv4**

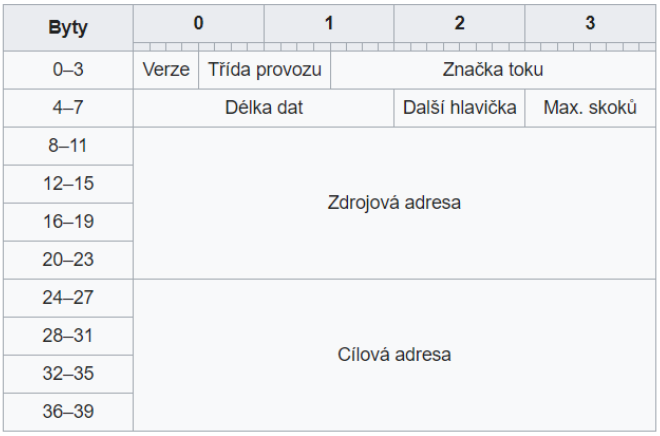
Formát IP datagramu

Bajty	0		1	2	3
Bajt 0 až 3	verze	IHL	typ služby	celková délka	
Bajt 4 až 7	identifikace			příznaky (3 bity)	offset fragmentu (13 bitů)
Bajt 8 až 11	TTL		číslo protokolu	kontrolní součet hlavičky	
Bajt 12 až 15	zdrojová adresa				
Bajt 16 až 19	cílová adresa				
Bajt 20 až ((IHL × 4) - 1)	rozšířená nepovinná nastavení				
...	data				

  - **1 slovo – obecná část**
    - **Verze** - například IPv4 – 0x4.
    - **IHL** - délka hlavičky ve WORDECH (4B), typicky 0x5 (5*4B = 20B) a maximální 0xF (15*4B = 60B).
    - **Typ služby** – umožňuje nastavení charakteru zprávy – nastavení nejmenšího zpoždění, největší šířky pásma či nejlevnější dopravy, spíše se ale nepoužívá.
    - **Celková délka** – délka datagramu v bajtech.
  - **2. slovo – zajištění fragmentace**
    - **Identifikace –** Odesílatel přidělí každému odeslanému paketu jednoznačný identifikátor. Pokud byl datagram při přepravě fragmentován, pozná se podle této položky, které fragmenty patří k sobě (mají stejný identifikátor).
    - **Příznaky:**
      - 1. bit – nevyužit.
      - 2. bit – zakazuje tento paket fragmentovat.
      - 3. bit – 1 - následuje fragment, 0 – poslední fragment.
    - **Offset fragmentu** - udává, na jaké pozici v původním datagramu začíná tento fragment. Jednotkou 8 B.
  - **3. slovo – zabezpečení služby**
    - **TTL** – ochrana proti zacyklení. Každý směrovač zmenší tuto hodnotu o jedničku. Pokud TTL je 0, datagram je zahozen.
    - **Protokol** - určuje, kterému protokolu vyšší vrstvy se mají data předat při doručení – např.: TCP, UDP, ICMP, EGP...
    - **Kontrolní součet hlavičky** – slouží k ověření, zda nedošlo k poškození paketu. **Nekontrolují se tímto data!**

- **4. slovo** – IP adresa odesílatele.
- **5. slovo** – IP adresa příjemce.
- **Záhlaví** – volitelná část.

- **IPv6**



Byty	0		1	2	3
0–3	Verze	Třída provozu	Značka toku		
4–7	Délka dat			Další hlavička	Max. skoků
8–11	Zdrojová adresa				
12–15					
16–19					
20–23					
24–27	Cílová adresa				
28–31					
32–35					
36–39					

- **Verze** – 4 bity, konstanta 6 (0110)
- **Třída provozu** – 8 bitů pro určení priority
- **Značka toku** – 20 bitů pro správu QoS (Quality of Service). Původně určeno pro real time aplikace, nyní se nepoužívá.
- **Délka dat** – 16 bitů pro délku těla paketu.
- **Další hlavička** – 8 bitů, určuje další vnořený protokol, stejné jako u IPv4.
- **Zdrojová a cílová adresa** – 128 bitů pro každou adresu.
- **Hop limit** – 8 bitů, stejné jako TTL u IPv4, přejmenován pro lepší výstižnost.

Fragmentace

- Fragmentace je proces rozdělení IP datagramu na menší části, aby mohl být přenesen po síti, která **nepodporuje přenos datagramů v plné velikosti**. Pokud je IP datagram větší než maximální velikost, kterou může síť přenést, je rozdělen na menší části nazývané fragmenty.
- Každý fragment obsahuje část datagramu a část hlavičky s informacemi potřebnými pro jeho správné složení na cílové stanici. Tyto fragmenty jsou pak přenášeny po síti odděleně a na **cílové stanici jsou složeny do původního datagramu**.

8. Transportní vrstva

- *porty, jejich účel, rozsah*
- *protokoly TCP, UDP a jejich použití*
- *nejznámější porty a jejich služby (21, 22, 23, 25, 53, 80, 110, 143, 443, 3389)*
- *TCP (navázání spojení, segmentace, okénkové potvrzovací schéma)*
- *ICMP, ICMPv6*
- *multicast, vlastnosti a použití, (IGMP, MLD)*

Rámec je vždy označen fyzickou adresou skutečného odesilatele na dané trase a fyzickou adresu nejbližšího příjemce.

Paket je vždy označen IP adresou originálního odesilatele a koncového příjemce **– funguje tedy mezi více sítěmi.** Obsahuje **rámec**. Dá se většinou zaměnit s IP datagramem.

Fragmentace je proces dělení **IP datagramu** na menší kousky, aby se vešel do maximální délky přenášeného **rámce**. **Fragmentace** se provádí na zdrojové stanici, pokud velikost **IP datagramu** přesahuje maximální velikost MTU (Maximum Transmission Unit) v dané síti. MTU určuje největší délku datového rámce, který může být přenesen přes danou síť bez fragmentace.

Při fragmentaci se **IP datagram** rozdělí na menší části a každá z nich se zapouzdří v nový **IP datagram**. Funguje takto pouze v IPv4.

8.1. Porty, jejich účel, rozsah

- Komunikační cesta KZ je většinou jediná (síťové rozhraní), ale **aplikací současné běžících** a **komunikujících je veliké množství**. Je potřeba přiřadit identifikaci dat dle aplikace.
- Nepoužívá se identifikace konkrétně dle jednotlivých procesů, ale dle přechodových bodů – portů.
- **Identifikace porty je softwarová logická záležitost**. Označení je univerzální - na všech OS (platformách) se používají stejně.
- **Port je určen 16bit číslem (0h- FFFFh, 0-65535).**

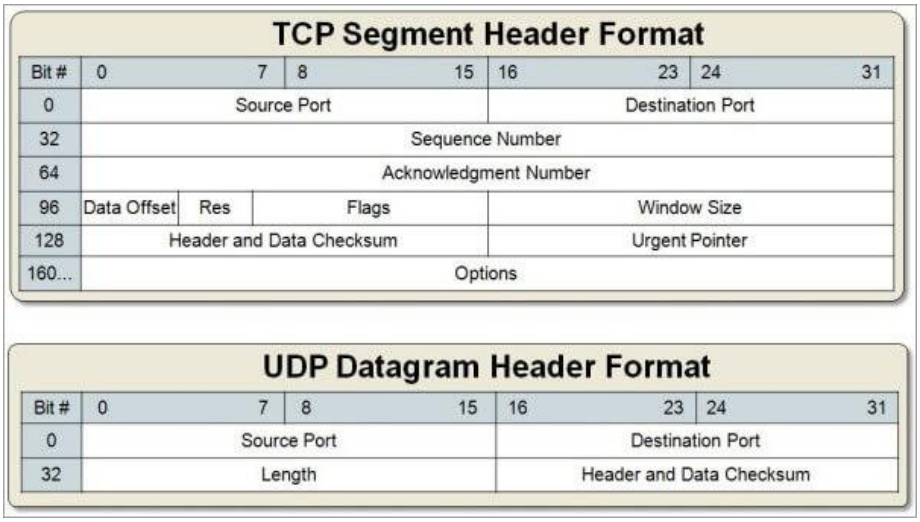
8.2. Protokoly TCP, UDP a jejich použití

TCP (Transmission Control Protocol)

- Vytváří mezi hostiteli relace.
- Zaručuje dodání paketů.
- Je pomalejší, vyšší nároky na objem dat, pouze dvoustranná komunikace.
- Vhodný například pro přenos souborů, web apod.
- TCP segmenty mohou přijít v jiném pořadí než byly vysílány (proto mají Sequence Number).

UDP (User Datagram Protocol)

- Nespojová služba, nevytváří relace.
- Nezaručuje dodání dat ani správné pořadí.
- Je rychlý, s malými požadavky na objem provozních dat.
- Pakety dojdou ve stejném pořadí jako byly vyslány, protože šly všechny stejnou cestou.
- Nevysílá žádné potvrzení o přijetí.
- Vhodné pro real time aplikace (videokonference, hry) či například DNS dotazy.



Rozdíly:

- TCP obsahuje Sequence Number a číslo potvrzení (Acknowledgment Number).

8.3. Nejznámější porty a jejich služby (21, 22, 23, 25, 53, 80, 110, 143, 443, 3389)

- Dobře známé porty – **0** - **1023**
- Registrované porty – **1024** - **49151**
- Ostatní porty – **49152** - **65535**

- **21** – FTP (přenos souborů).
- **22** – SSH přístup (např.: Putty a Linux).
- **23** – Telnet přístup (podobné jako SSH, ale není šifrované, starší).
- **25** – SMTP (odesílání e-mailů).
- **53** – DNS.
- **80** – HTTP.
- **110** – POP3 (smaže e-mail ze serveru).
- **143** – IMAP (nechává e-mail na serveru).
- **443** – HTTPS (secure).
- **465** – SMTPS (secure – TLS).
- **587** – SMTPS (secure - SSL).
- **993** – IMAP with TLS/SSL (secure).
- **995** – POP3 with TLS/SSL (secure).
- **3389** – Windows RDP (Remote Desktop Protocol).

Rozdíl mezi TLS a SSL

- **SSL** (Secure Socket Layer).
- **TLS** (Transport Layer Security).
- **TLS** je zdokonalené **SSL**, je novější, ale spíše se více používá název **SSL**, i když se vlastně už používá **TLS**.

8.4. TCP (navázání spojení, segmentace, okénkové potvrzovací schéma)

Navázání spojení:

- Probíhá ve třech krocích (Three-Way handshake).
- Klient odešle na server datagram s nastaveným příznakem SYN a náhodně vygenerovaným pořadovým číslem (x), potvrzovací číslo=0.
- Server odešle klientovi datagram s nastavenými příznaky SYN a ACK, potvrzovací číslo=x+1, pořadové číslo je náhodně vygenerované (y).
- Klient odešle datagram s nastaveným příznakem ACK, pořadové číslo=x+1, číslo odpovědi=y+1.

Příznaky:

- **SYN** – používá se k navázání spojení.
- **ACK** – slouží k potvrzení o přijetí.
- **FIN** – informace o ukončení spojení.
- **RST** – informace o ukončení z důvodu chyby.

Potvrzování

- TCP používá tzv. kladné potvrzování = příjemce potvrzuje úspěšně přijatá data.
- Na chybně přijatá data příjemce nereaguje => uplyne limit. Odesílatel je odešle znovu.
- Pokud odesílateli přijde potvrzení, tak je logicky neposílá znovu.
- TCP používá tzv. **okénkové potvrzování**.
- To spočívá v tom, že odesílatel může odeslat další bloky ještě dříve, než dostane potvrzení o přijetí bloku předchozího.
- O tom, kolik bloků může vyslat dat “dopředu”, rozhoduje velikost pomyslného “okénka”.

Bez okénkového potvrzování je to velmi neefektivní komunikace.

- Odešlu paket. t = 0 s
- Příjemce přijme, paket a posílá potvrzení. t = 0.5 s
- Přijímám potvrzení a posílám nový paket. t = 1 s
- Odeslání jednoho paketu za 1 sekundu je nemyslitelné.

Okénkové schéma

- Odešlu paket a hned posílám další. t = 0 s
- Příjemce přijímá paket a posílá potvrzení, následně mu přijdou i další pakety a pošle potvrzení i na ně. t = 0.5 s
- Přijímám potvrzení o přijetí prvního. Odesílám nový. Přijímám potvrzení o přijetí dalších. Posílám další. t = 1 s
- Ve chvíli, kdy přijímám potvrzení o přijetí prvního paketu, už může vysílat 101. paket.

8.5. ICMP, ICMPv6

- Obecně musí být ošetřeny nestandardní stavy (chyby apod.) vznikající při přenosu paketu sítí. To je úkolem protokolu **ICMP** (Internet Control Message Protocol).
- **Zprávy ICMP se vysílají například v těchto případech:**
    - Adresa cílové sítě není ve směrovací tabulce.
    - Koncový uzel je nedostupný.
    - Potřeba fragmentovat paket s příznakem nefragmentovat.
    - Vynulování TTL popřípadě Hop Limit.
- ICMP dále používají obslužné programy ping a traceroute. Ošetření nestandardních stavů většinou musí provádět směrovač.
- **Protokol IPv6** označuje zprávy jako **ICMPv6** a má i další role než v IPv4 – například informativní zprávy a podpora skupinového vysílání apod.

- **Funkce ICMPv6:**
    - Překlad IP adres na linkové adresy (v IPv4 řešil ARP).
    - Bezpečnostní opatření.
    - Přebírá funkce IGMP (viz dále).
    - **Hlášky:**
        - **0 - 127** - chybové zprávy.
        - **128 - 255** – informativní zprávy.

8.6. Multicast, vlastnosti a použití, (IGMP, MLD)

- Multicast je způsob doručování datových paketů na více cílových zařízení najednou. To znamená, že paket je doručován pouze těm zařízením, která se aktivně přihlásila do multicastové skupiny. Tím se snižuje zátěž sítě, jelikož se pakety nerozesílají všem připojeným zařízením, ale pouze těm, která se zajímají o obsah těchto paketů. Většinou se jedná o streaming videa a zvuku.
- **IGMP (Internet Group Management Protocol)**
    - Rozšiřuje IPv4 o funkce multicastu.
    - Využívá se pro dynamické přihlašování a odhlašování ze skupiny u multicastového routeru ve své lokální síti.
    - **Zprávy:**
        - **Membership Query** - zpráva odesílaná multicastovou cestou směrem k hostům, kteří jsou připojeni k multicastové skupině. Cílem této zprávy je ověřit, zda hosti stále chtějí zůstat připojeni k dané skupině a zda jsou stále aktivní.
        - **Membership Report** - zpráva, kterou odesílají hostitelé, kteří se připojují k multicastové skupině, aby informovali router o svém zájmu o příjem multicastového provozu z této skupiny.
        - **Leave Group** - zpráva, kterou hostitelé odesílají, když chtějí opustit multicastovou skupinu. Tato zpráva slouží k informování routeru o tom, že daný hostitel již nepotřebuje přijímat multicastový provoz z této skupiny.

- **MLD (Multicast Listener Discovery)**
    - Součást IPv6.
    - Stejný princip jako IGMP.

9. Bezdrátové sítě

- *bezdrátové spoje a její vlastnosti (Wi-Fi, P2P spoje na >10 GHz, optická pojítka)*
- *vlastnosti Wi-Fi (frekvence, kategorie, rychlost, režimy provozu, zabezpečení)*
- *řízení přístupu k médiu u Wi-Fi, problém skrytého uzlu*
- *legislativní omezení provozu Wi-Fi (povolený výkon, frekvenční pásma)*
- *P2P rádiové spoje (vlastnosti, používané frekvence, rychlosti)*
- *P2P optické spoje (vlastnosti, rychlosti)*
- *antény (zisk, polarizace, typy)*

9.1. Bezdrátové spoje a její vlastnosti (Wi-Fi, P2P spoje na >10 GHz, optická pojítka)

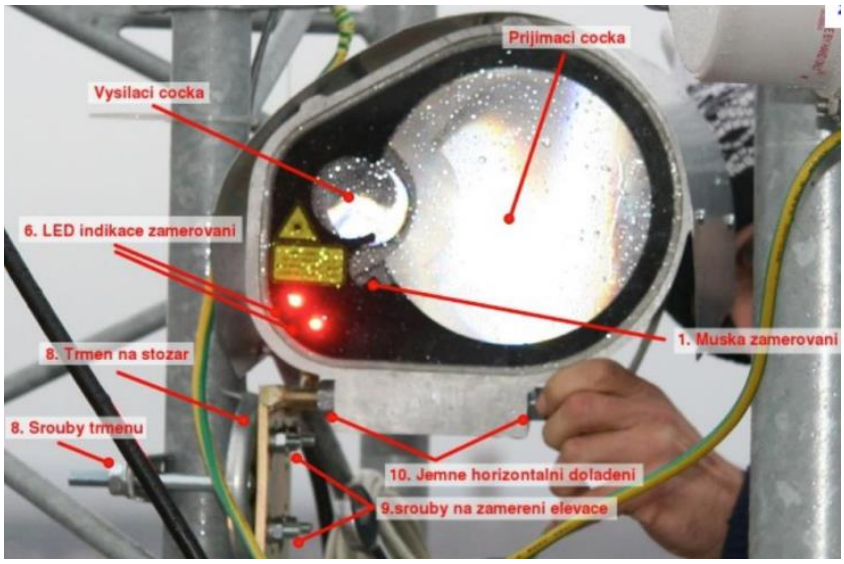
- **Dělí se:**
  - **Rádiová**
    - **Licenční** – nelze využít (např.: 694 – 823 MHz, 832 – 862 MHz – mobilní sítě).
    - **Bezlicenční** – volné využívání (např.. 2.4 GHz, 5 GHz, 443 MHz).
  - **Optická**

- **Wi-Fi**
  - Rádiový, infrastrukturní režim – vysílá kolem sebe pro všechny klienty.
  - Široká dostupnost, nízká cena, pomalejší než ethernet.
  - Čím vyšší frekvence, tím hůře prochází překážkám.
  - **SSID** (Service Set Identifier) – název sítě.
  - **Použití:**
    - Pro připojení mobilů, tabletů, počítačů, televizí, chytrých zařízení.
    - Čím dál více rozšířené, nahrazuje ethernetové připojení (protože nikomu se nechce tahat všude ethernet kabely).

- **P2P spoje na >10 GHz**
    - Peer-to-Peer – “rovný s rovným“ – klient-klient.
    - Vysoká rychlost přenosu dat mezi dvěma body a nejsou k dispozici kabelové spoje například různých budov na velkou vzdálenost (i několik kilometrů).
    - Většinou licencovaná pásma.
    - Oproti WiMAX (ten pracuje i v nelicencovaném pásmu) dosahuje větších rychlostí (až řády Gbit) a nedokáže připojit více než 2 stanice.

Optická pojítka

- **Laserový paprsek** – v podstatě optika bez optického vlákna.
- Podobné jako P2P spoje nad 10 GHz, ale nepoužívá rádiový signál.
- Citlivé na změny počasí – mlha apod.



9.2. Vlastnosti Wi-Fi (frekvence, kategorie, rychlost, režimy provozu, zabezpečení)

Wi-Fi = Wireless Fidelity

Používané frekvence

- **2.4 GHz** – poměrně staré, ale velmi rozšířené.
- **5 GHz** – novější, rychlejší.
- **6 GHz** – velmi nové, v Česku zatím běžně dostupné není, viz Wi-Fi 6E.

Kategorie (**pomůcka**: bagnac AX BE).

IEEE 802.11	Wi-Fi 0	1997	2.4 GHz	2 Mbit
IEEE 802.11b	Wi-Fi 1	1999	2.4 GHz	11 Mbit
IEEE 802.11a	Wi-Fi 2	1999	5 GHz	54 Mbit
IEEE 802.11g	Wi-Fi 3	2003	2.4 GHz	54 Mbit
IEEE 802.11n	Wi-Fi 4	2009	2.4 / 5 GHz	600 Mbit
IEEE 802.11ac	Wi-Fi 5	2013	5 GHz	6928 Mbit
IEEE 802.11ax	Wi-Fi 6	2019	2.4 / 5 GHz	600-9608 Mbit
	Wi-Fi 6E	2020	2.4 / 5 / 6 GHz	
IEEE 802.11be	Wi-Fi 7	N/A		40000 Mbit

Dosah signálu se liší podle verzí, všeobecně **vyšší frekvence snižuje dosah**, maximálně se však dosah pohybuje okolo 100-200 metrů.

Režimy provozu:

- **Infrastrukturní**
  - Komunikace mezi zařízeními pomocí Access Point.
  - Více možností zabezpečení.
  - Většinou rychlejší.
- **Ad-hoc**
  - Přímá komunikace mezi zařízeními (první klient tvoří jakýsi AP, v případě odpojení si roli AP ujímá jiné zařízení, komunikace ale nejde přes AP).
  - Většinou pomalejší.
  - Moc se nepoužívá.

- **Repeater**
  - Opakuje data, zvětšení dosahu.

- **Bridge**
  - Propojuje dvě bezdrátové sítě.

- **Client**
  - Připojí se k jinému bezdrátovému bodu a převádí síť do ethernetu.

Zabezpečení

- Wi-Fi se šíří vzduchem, takže vysílání může každý přijmout, proto je nutné ho šifrovat.

- **WEP**
  - Wired Equivalent Privacy.
  - Zastaralé, prolomené.
  - Používá symetrickou šifrovací metodu pro zabezpečení přenosu dat, kde se pro šifrování i dešifrování dat používá stejný klíč, který je ale na začátku přenášen v plain textu.
- **WPA**
  - Wi-Fi Protected Access.
  - Rychlá náhrada za prolomený WEP, bylo dostupné formou aktualizace prvků využívajících WEP.
  - Algoritmus TKIP.
- **WPA2**
  - Vylepšení zabezpečení podporou CCMP (režim šifrování založený na AES).
  - Nejčastější způsob zabezpečení.
  - **WPA2-Personal (WPA2-PSK)**
    - Připojování pomocí sdíleného klíče.
  - **WPA2-Enterprise (802.1x/EAP)**
    - Podpora Radius serveru.

- **WPA3**
    - Vylepšení ochrany proti útokům.
    - Vylepšení ochrany odposlechu.
    - Větší délka klíče.

- **WPS**
    - Zařízení lze propojit s Wi-Fi pomocí zmáčknutí tlačítek.
    - Na routeru a například tiskárně současně zmáčkneme tlačítka označená jako WPS a následně se zařízení připojí na Wi-Fi.
    - WPS je ale snadno prolomitelné, číselná kombinace zabere maximálně 9 hodin na prolomení (1 pokus za 3 sekundy).

- **802.1x**
    - Používá Radius server.
    - Funguje ovšem i na uživatele připojení pomocí TP kabelu (tedy nejen na Wi-Fi).

9.3. Řízení přístupu k médiu u Wi-Fi, problém skrytého uzlu

Metoda řízení přístupu

- CSMA – metody s vícenásobným kolizním přístupem a nasloucháním nosné.
- Wi-Fi používá CSMA/CA.
- Carrier Sense Multiple Access with Collision Avoidance.
- Před začátkem vysílání paketu stanice určitý čas poslouchá, zda je přenosové médium volné. Pokud ano, může zahájit vysílání. Pokud ne, čeká náhodnou dobu a následně znovu ověřuje, zda může vysílat.
- Neumí detekovat kolize.
- Doručení se potvrzuje pomocí ACK.

Problém skrytého uzlu

- Jedno zařízení nevidí na druhé, proto první nedokáže ověřit, zda není vysíláno, proto začne samo vysílat.

RTS

- Request To Send.
- Speciální paket, ujištění, že klient může vysílat, pokud chce poslat velké množství dat.

CTS

- Clear To Send.
- Potvrzení na RTS, že je médium volné a může začít vysílat.

9.4. Legislativní omezení provozu Wi-Fi (povolený výkon, frekvenční pásma)

- Výkon vysílání je omezen, aby nedošlo k rušení.
- **Max EIRP – vyřazování výkon**
    - **2.4 GHz** – 100 mW = 20 dBm (logaritmická jednotka výkonu).
    - **5 GHz** – 200 mW = 23 dBm (mimo budovy až 1000 mW = 30 dBm).
    - **6 GHz** – 200 mW = 23 dBm (údajně, je relativně nová, není moc informací).

- **Frekvenční pásma**
    - **2.4 GHz**
        - **FHSS (Frequency Hopping Spread Spectrum)**
            - 79 kanálů, po 1 MHz, dnes použitelné jako rušička.

        - **DSSS (Direct Sequence Spread Spectrum)**
            - V ČR 13 kanálů (1-13) po 5 MHz. Pouze 3 kanály se nepřekrývají.
            - Od 2400 MHz do 2483.5 MHz.
        - **OFDM (Orthogonal Frequency Division Multiplexing)**
            - Pásmo v překrývajících podpásmech, každá nese část dat.
            - 4 kanály po 20 MHz a každý kanál má 52 subnosných (312.5 kHz) – pomalý datový tok, ale mnohokrát.

    - **5 GHz**
        - V ČR kanály 36-64 a 100-140 po 20 MHz (asi).
        - Od 5150 MHz do 5725 MHz.

    - **6 GHz**
        - Nestanoveno (viz VO-R/12/11.2021-11).

9.5. P2P rádiové spoje (vlastnosti, používané frekvence, rychlosti)

- Používá Směrové antény.
- **Výhody** - Vyšší rychlost, spolehlivost, dosah.
- **Nevýhody** - Vyšší cena, náročnější instalace a pouze P2P.
- **Frekvence** – 10 – 80 GHz, některé frekvence jsou licencované.
- **Rychlosti** – od 100 Mb až do 1 Gb, full duplex.

9.6. P2P optické spoje (vlastnosti, rychlosti)

- **Dosah** - až několik km, ale náchylné na počasí.
- **Rychlosti** – řády Gbps, dostupné i 30 Gbps.

- Používá se laser (světlo nemusí být viditelné), není možný odposlech ani rušení.
- Vysoká cena (50-100 tisíc).
- V ČR známa RONJA – rychlost 10 Mbps, vymyslel bývalý student Matfyzu.

9.7. Antény (zisk, polarizace, typy)

Zisk

- **Zisk antény** je parametr, který určuje, jak efektivně anténa přenáší nebo přijímá signály v daném směru.
- **Určuje decibel.**
- **Útlum** – **ztráta** (např.: -3 dB).
- **Zisk** – **posiluje** (např.: 3 dB).

- **Výpočet dB**
  - Používání logaritmické měřítka.
  - Decibel – logaritmická bezrozměrná poměrová jednotka.
  - Protože **deci**bel – nutné násobit 10.
  - Poměr výkonů (x1 – vstup; x2 – výstup) - Ap = 10 log $(\frac{P_2}{P_1})$.
  - Napěťové (Au) či proudové zesílení (Ai) - Au = 20 log $(\frac{U_2}{U_1})$.

- **Příklady dB**
  - Zesilovač má na vstupu 20mW a jeho výstupní výkon je 3,5 W. Jaký má zisk v dB?
  - $G = 10.log\frac{3,5}{20.10^{-3}} = 10.log\,175 = 10.2,24 = \underline{22,4dB}$ **(zisk)**
  - Na vstup koaxiálního kabelu je přiveden od vysílače výkon 150 W a na výstupu byl naměřený výkon pouze 112 W. Jaké ztráty v dB má koaxiální kabel?
  - $G = 10.log\frac{112}{150} = 10.log\,0,747 = 10.(-0,127) = \underline{-1,27dB}$ **(útlum)**
  - Logaritmus čísla menšího jak 1 je záporné číslo! Pro nulovou a zápornou hodnotu není logaritmus definován!

Polarizace

- Vliv na příjem a vysílání.
- Směr vlnění se musí shodovat u obou antén.
- Horizontální a vertikální.

Typy

- **Směrové** – přímé míření (např.: 3 až 10 stupňů), signál ve tvaru paraboly (to je kvadratická funkce). Například pro vysílače.
- **Sektorové** – výřez na jednoho úhlu (např.: 90 stupňů). Například pro bazény či haly.
- **Všesměrové** – výřez kolem sebe. Například pro domácnosti a kanceláře.

10. Systém DNS

- *systém DNS (úplné doménové jméno, princip, autority)*
- *registrace doménového jména*
- *cachující, rekurzivní a autoritativní DNS resolver, příklady programů*
- *popis funkce rekurzivního resolveru*
- *základní typy záznamů (A, AAAA, CNAME, MX, TXT, PTR)*
- *DNSSEC (přínos, princip)*

10.1. Systém DNS (úplné doménové jméno, princip, autority)

- Každý webový server (například web školy) má svoji IP adresu (v tomto případě 195.113.165.21). Je ovšem těžké si zapamatovat IP adresu každého webu, na který přistupujeme.
- Z tohoto důvodu se zavedly tzv. domény (doména = oblast působnosti). Proto si nemusíme pamatovat IP adresy, ale použijeme snadno zapamatovatelný název domény (spse.cz, i4.spse.cz, google.com, wikipedia.org, web.dev).
- Pod tuto doménu se uloží záznamy (RR – Resource Records), které nás následně dokážou snadno nasměrovat na daný server dané domény a dané služby.

Úplné doménové jméno

- Mějme následující doménu: public-api.i4.spse.cz. :
  - . – root doménu.
  - cz – národností TLD (Top Level Domain), doména první úrovně.
  - spse – doména druhé úrovně.
  - i4 – doména třetí úrovně.
  - public-api – doména čtvrté úrovně.

Pravidla doménových jmen:

- Jen alfanumerické znaky a pomlčka (jen uprostřed), dříve ještě podtržítko, maximálně 255 znaků, jednotlivý řád maximálně 63 znaků. Například .cn má povolené ale i čínské znaky.

Základní pravidla:

- Řády domény – oddělené tečkou, počítání odprava (vpravo 1. řád).
- Poslední tečka se většinou neuvádí.
- Například majitel .cz domény spravuje všechny subdomény (tedy 2. řádu) a nabízí je k registraci za roční poplatek. U jiných domén to může být až vyšší řád (neco.co.uk).

TLD domény:

- Generické (gTLD) - .com, .net, .biz, .edu, .gov, .mil (military).
- Národní (ccTLD) - .cz, .pl, .sk, .de, .si, .en, .us.
- Sponzorované - .cloud, .fun, .space, .store, .tech.
- Infrastrukturní TLD (.arpa).

Postup překladu:

- Při překladu domény na IP adresu se tazatel dotazuje nameserverů postupně od nejvyššího řádu.
- Každý další nameserver doplní část adresy, kterou zná.
- Poslední nameserver vrátí celou IP adresu na kterou se poté tazatel připojí.
- Při zadání spse.cz – proběhne kontakt root serveru, následně serveru CZ nic a následně DNS upce.cz, ta už dodá informace o IP adrese – toto je tzv. rekurzivní hledání.

Autority

- **IANA**
    - Dohlíží celosvětově na přidělování IP adres, správu kořenových zón DNS a další. IANA spravuje také DNS servery nejvyšší úrovně hierarchického DNS stromu (tzv. kořenové servery). Tento úkol zahrnuje zajištění komunikace se správci domén nejvyššího řádu i kořenové úrovně.
- **CZ.NIC**
    - Správcem domény .cz je CZ.NIC. CZ.NIC provozuje registr doménových jmen .CZ, zabezpečuje provoz domény nejvyšší úrovně .CZ a také například osvětu v oblasti doménových jmen. V současné době se sdružení intenzivně věnuje rozšiřování technologie DNSSEC a IPv6.

10.2. Registrace domény

- **České domény**
  - Doménu je možné si pronajmout u akreditovaného registrátora, který doménu administruje (nastavuje DNS záznamy) a vybírá poplatek.
  - Majitelem domény se může stát jakákoliv fyzická či právnická osoba.
  - **Například:** Wedos, Active 24, Webglobe, Internet CZ (Forpsi), Seznam.
  - Většinou se pronajímá po rocích na 1-10 let.
- **gTLD domény** (generické)
  - Registrátor prochází verifikací **ICANN**.
  - **V Česku tři:** Wedos, Subreg, RegDomains.
  - **Další známí**: Google Domains, Go Daddy, Wix, Bluehost, AWS (Amazon).

10.3. Cachující, rekurzivní a autoritativní DNS resolver, příklady programů

- **DNS resolver** (resolver = překladač)- překládá doménové jméno na IP adresu

Cachující server a **rekurzivní** jsou ve své podstatě **jeden a ten stejný server**. Funkce sice můžou být implementovány jednotlivě, ale vlastně každý rekurzivní DNS server je zároveň i cachující.

- **Cachující**
  - Používají ho například Wi-Fi routery či servery poskytovatele internetu.
  - Nic nepřekládá, zacachovaná odpověď je no-authoritative answer.
  - Přijme dotaz, přepošle ho nadřazenému DNS serveru a zapamatuje si odpověď.
  - Každý dotaz má svoji hodnotu TTL (Time to Live), poté je nutné stáhnout odpověď dotazu znovu.
  - Zrychluje odezvy.
  - **Příklad:** Pi-Hole (ten umí i blokování), Dnsmasq (má i DHCP klienta).

- **Rekurzivní**
  - Server pro ně příslušný záznam získá rekurzivními dotazy u autoritativních DNS serverů a po stanovenou dobu (definovanou pomocí parametru TTL - Time to live) je má uloženy v cache, aby mohl odpovídat klientům rychleji a šetřil zatížení serverů autoritativních.
  - **Příklad:** BIND, Unbound, KNOT.

- **Autoritativní**
  - Jsou na něm trvale uloženy záznamy k dané doméně / zóně. Autoritativních serverů je obvykle více (minimálně dva – primární a sekundární, ale běžně i více).
  - Autoritativní DNS servery jsou obvykle provozovány registrátorem domény nebo poskytovatelem webhostingu.
  - **Příklad:** BIND, KNOW.

- **Alternativní**
  - Dokáže být rychlejší jak DNS servery poskytovatelů.
  - **Známé:** Google (8.8.8.8 a 8.8.4.4), Cloudflare (1.1.1.1 a 1.1.0.0).

10.4. Popis funkce rekurzivního resolveru

- Dotazuje se DNS serverů od nejvyššího řádu. Každý další server mu vrátí tu část domény, kterou zná a odkáže ho dál. Takto si postupně přeloží celou IP adresu a vrátí ji dotazovateli.
- DNS dotazy fungují na **UDP** a portu **53**.

10.5. Základní typy záznamů (A, AAAA, CNAME, MX, TXT, PTR)

- **A** – IPv4 adresa.
- **AAAA** – IPv6 adresa.

- **CNAME** – nasměrování subdomény na doménu či subdoménu, nelze řetězit CNAME za sebou a funguje jen pro A či AAAA.
- **MX** – e-mailový server.
- **TXT** – textové záznamy pro verifikaci (Google Analytics, Facebook Ads apod.), používá se také pro SPF (chrání e-maily před zneužitím).
- **PTR** – reverzní záznam, IP adresa na doménu.

10.6. DNSSEC (přínos, princip)

- Umožňuje zabezpečit informace poskytované DNS proti podvržení a úmyslné manipulaci.
- Klient může pomocí elektronického podpisu ověřit původ dat, jejich integritu (neporušenost) nebo platnost neexistence záznamu.
- Nenahrazuje HTTPS, ale ani HTTPS nenahradí DNSSEC – stále jde SSL certifikát podvrhnout změnou DNS, který používá certifikační server, proto je vhodné kombinovat jak HTTPS, tak DNSSEC.
- Používá se záznam RRSIG.
- Záznam ověřuje každý DNS server a nejlépe i samotné zařízení.

Princip:

- DNSSEC zavádí DNS asymetrickou kryptografii – tedy používání jednoho klíče na zašifrování a jiného klíče na dešifrování obsahu.
- V případě DNSSEC si držitel domény vygeneruje dvojici soukromého a veřejného klíče. Svým soukromým klíčem pak elektronicky podepíše záznamy (technický údaje), které v té doméně jsou. Pomocí veřejného klíče je pak možné ověřit pravost tohoto podpisu.
- Aby byl tento klíč dostupný všem, publikuje jej držitel ke své doméně u nadřazené autority, kterou je pro všechny domény .cz registr domén .cz. I na úrovni registru domén .cz jsou technická data v DNS podepsána a veřejný klíč k tomuto podpisu je opět správcem registru předán nadřazené autoritě.
- Vytváří se tak řetěz, který zajistí důvěryhodnost údajů, pokud není v žádném svém článku porušen, a všechny elektronické podpisy souhlasí, viz následující schéma.

11. Zabezpečení počítačových sítí a VPN

- *princip firewallu (stavový, bezstavový) a jeho využití*
- *princip proxy a její využití*
- *rozdíl mezi NAT a firewall z hlediska zabezpečení*
- *zabezpečení přístupových portů (802.1x, DHCP snooping, ARP inspection, ...)*
- *IDS, IPS (význam, princip)*
- *princip VPN, důvody použití, implementace (IPSec, OpenVPN, ...)*

11.1. Princip firewallu (stavový, bezstavový) a jeho využití

- Firewall pracuje na **síťové** a **transportní** vrstvě (3. a 4. vrstva). Umožňuje blokovat přístup na základě portů a protokolů.
    - **Využití** – zablokování přístupu k HTTP a HTTPS pro výpočetní server pro snížení rizika stažení malwaru zaměstnancem na server.
- Existují i aplikační Firewally na 7. (aplikační) vrstvě. Ty mohou blokovat weby například na základě URL adresy či hlavičky.
    - **Využití** – zablokování maturitních webů na školní Wi-Fi.

Stavový Firewall

- Sleduje a udržuje všechny navázané TCP/UDP relace (pracuje na transportní vrstvě).
- Rozlišuje různé stavy paketů v rámci jednotlivých relací (spojení) a jeho úkolem je propustit pouze takové, které patří do již povolené relace (jiné jsou zamítnuty).
- Při navazování spojení se uloží do stavové tabulky parametry jako zdrojová a cílová IP adresa, porty, protokol, flagy, sekvence, potvrzovací znaky (ACK. NUMBERS), kód a typ ICMP. Poté u každého paketu z již navázaného spojení kontroluje, zda se shoduje se stavovou tabulkou což je efektivnější než u každého paketu kontrolovat sadu složitých nadefinovaných pravidel.
- Pakety jsou rozřazovány do následujících kategorií:
    - **NEW** – tento datagram otevírá novou komunikaci
    - **ESTABLISHED, RELATED** – datagram patří do již navázaného spojení.
    - **INVALID** – datagram nepatří do žádného spojení nebo je neidentifikovatelný.

Bezstavový Firewall

- Bezstavový Firewall pracuje vždy s každým paketem (datagramem) samostatně.
- Neexistuje žádný způsob, jak zjistit, zda je daný paket součástí již existujícího spojení, pokouší se navázat nové připojení nebo se jedná o podvodný paket.
- Např.: ACL (Access Control List).

Bezstavový Firewall je všeobecně méně náročnější na zdroje a nezatěžuje tolik síť, oproti tomu **Stavový Firewall** je daleko účinnější.

11.2. Princip proxy a její využití

- Aplikace předává na server požadavky a ten je vyřizuje, tedy chová se jako prostředník mezi uživatelem a serverem s poskytující službou.
- Pracuje na 7. (aplikační) vrstvě ISO/OSI – protože řeší požadavky aplikací, ne celého systému.
- Lze využít k blokování obsahu.
- Hlavní rozdíl mezi proxy a NAT spočívá v tom, že proxy server je umístěn mezi koncovým zařízením a internetem a slouží jako prostředník, zatímco NAT je umístěn mezi dvěma sítěmi a umožňuje překlad IP adres a portů. Proxy server může být použit k blokování nebo filtrování obsahu, zatímco NAT je obvykle používán k umožnění přístupu k internetu ze zařízení v privátní síti pomocí jediné veřejné IP adresy.
- **Reverzní proxy** – využití zejména pro webové služby a servery – mám jednu IP a po připojení reverzní proxy určí, na jaký server přistoupím – to může být například u webů podle doménového jména.

11.3. Rozdíl mezi NAT a firewall z hlediska zabezpečení

- NAT překládá vnitřní adresy na veřejné a naopak. Ve výsledku se vnitřní adresy nedostanou nikdy na internet.
- NAT neochrání síť a není to jeho účel.
- Firewall obsahuje pravidla pro ochranu sítě.
- Vlastně to jsou dvě úplně jiné věci.

11.4. Zabezpečení přístupových portů (802.1x, DHCP snooping, ARP inspection, ...)

802.1X

- Protokol, který umožňuje zabezpečení přístupu do počítačové sítě.
- Pokud se klient (počítač) připojí k přípojnému bodu (UTP kabelem do síťového portu u switche, ale i k bezdrátovému přístupovému bodu u Wi-Fi), je po něm pomocí IEEE 802.1X vyžadována autentizace (např. uživatelské jméno a heslo).
- Přípojný bod blokuje veškerý ostatní datový provoz klienta do té doby, než je úspěšně autentizován.
- Pro řízení autentizace je u klienta používán **suplikant** (“prosebník“), u přípojného bodu je vyžadována dodatečná podpora (tj. switch s managmentem).

DHCP snooping

- **DHCP snooping** je funkce síťových zařízení, která pomáhá zabránit útokům založených na DHCP (Dynamic Host Configuration Protocol).
- **DHCP snooping** umožňuje síťovému zařízení, jako je například přepínač (switch), sledovat provoz DHCP v síti a udržovat tabulku platných a neplatných adres DHCP. Při každém přidělení nové IP adresy **DHCP snooping** ověřuje, zda je adresa platná a zda ji má právo přiřadit příslušnému zařízení.
- Tímto způsobem může **DHCP snooping** zabránit například útoku typu **DHCP spoofing**, při kterém útočník posílá falešné DHCP nabídky a snaží se tak získat řízení nad IP adresami v síti. **DHCP snooping** rovněž chrání před dalšími typy útoků založených na DHCP, jako například **DHCP starvation attack**, při kterém útočník vyčerpává pool dostupných adres DHCP, aby zabránil přiřazení adres ostatním zařízením v síti.

ARP inspection (respektive někdy Dynamic ARP Inspection – DAI)

- Pro své správné fungování využívá databázi vytvořenou mechanismem **DHCP Snooping**.
- Na portech, kde je ochrana aktivována, jsou kontrolovány všechny pakety protokolu ARP, u kterých je prováděná analýza, zda se údaje v ARP odpovědích (IP a MAC adresy) shodují s příslušným záznamem v **DHCP Snooping** databázi. Tento typ kontroly znemožní připojenému zařízení provést útok typu **ARP poisoning**.
- Další často ceněnou vlastností tohoto mechanismu je fakt, že zařízení nedokáže rozumně používat síť, pokud předem nepožádalo o konfigurační údaje **DHCP server**. To prakticky znemožňuje uživatelům používat vlastnoručně nakonfigurované **statické IP adresy**, což je noční můra mnoha správců.

MAC address flooding

- Útok pomocí zaplavení MAC adresami. Útočník se snaží vyčerpat paměť switche, určenou pro ukládání tabulky MAC adres (CAM tabulka), pomocí zasílání **velkého množství rámců** s unikátními (**neplatnými**) zdrojovými MAC adresami. Ve chvíli, kdy je CAM tabulka plná, tak se nevytváří nové záznamy. **Unicastová komunikace**, která je určená pro cílovou MAC adresu, která se nenachází v CAM tabulce, je zaslána na všechny porty mimo příchozího (tak se chová hub, provoz je jako broadcast).
- Tento útok se používá k tomu, aby útočníkova stanice **dostávala i provoz**, **který není určen jí**. Navíc se zvýší celkový provoz v síti a ve výsledku může způsobit příliš velké vytížení switche, takže se jedná o DoS útok (Denial Of Services).
- **Obrana:** Port Security nebo Port Based Authentication.

11.5. IDS, IPS (význam, princip)

IDS (Instrusion Detection System)

- Obranný systém, který monitoruje síťový provoz a snaží se odhalit podezřelé aktivity.
- Umožňuje detekci neobvyklých aktivit, které by mohly vést k narušení bezpečnosti počítačové sítě a též možný aktivní zásah proti nim.
- IDS se nezabývá jen finálními pokusy o prolomení bezpečnosti, ale i o detekci akcí, které jim předcházejí. Mezi ně patří například skenování portů, sbírání informací potřebných k útoku atd.

- Obsahuje mechanismy pro detekci škodlivých a nebezpečných kódů a jeho činností je odhalování těchto nebezpečí.
- Systém IDS by měl po detekci neobvyklé aktivity vygenerovat varování (Alert), provést zápis do logu, upozornit správce a případně tuto činnost zastavit. Dále by měl být schopen rozlišit, zda se jedná o útok z vnitřní sítě nebo z externích sítí.

IPS (Intrusion Prevention System)

- Hlavní funkce **IPS systémů** jsou identifikace škodlivé činnosti, zaznamenávání informací o jejím průběhu, následném blokování této činnosti a také její nahlašování.
- **IPS systémy** jsou považovány za rozšíření **IDS systémů**, protože monitorují jak provoz na síti, tak i aktivity operačního systému, které by mohly vést k narušení bezpečnosti.
- Hlavní rozdíl oproti **IDS systémům** je, že **systém IPS** je zařazen přímo do **síťové cesty** (in-line), a tak může aktivně předcházet, případně blokovat detekovaný nežádoucí a nebezpečný provoz na síti.
- **IPS** může provádět takové akce jako vyvolání poplachu, filtrování škodlivých paketů, násilné resetování spojení anebo blokování provozu z podezřelé **IP adresy**. Všechny tyto úkony často provádí ve spolupráci s Firewallem.

11.6. Princip VPN, důvody použití, implementace (IPSec, OpenVPN, ...)

VPN (Virtual Private Network)

- Umožňuje propojit počítače prostřednictvím nedůvěryhodné počítačové sítě.
- Propojení počítačů jako by byly fyzicky ve stejné síti a mohou spolu komunikovat už v důvěryhodné síti.
- Při navazování spojení se ověřuje totožnost obou stran pomocí digitálních certifikátů nebo předem sdíleným klíčem, poté dojde k autentizaci.
- Celá komunikace je šifrována, a tak je toto připojení bezpečné.
- VPN pracuje na síťové vrstvě L3 nebo transportní L4.

Některé VPN tunely: OpenVPN, WireGuard, SSTP.

Důvody použití:

- **Připojení do podnikové sítě z domova**, kdy chceme mít jednak přístupná data na serverech firmy a zároveň chceme mít přenos dat zabezpečený, aby nás nikdo nemohl odposlouchávat.
- **Správce sítě o nás nezjistí, jaké weby navštěvujeme** (chodíme například na křesťanskou školu a nechceme, aby se správce sítě dozvěděl, jaká videa sledujeme). POKUD WEB POUŽÍVÁ HTTPS, NIKDY NEMŮŽE ZJISTIT KONKRÉTNÍ STRÁNKY ČI DATA, ALE CELKEM SNADNO MŮŽE ZJISTIT DOMÉNY KVŮLI DNS. To ale neznamená, že správce VPN to nezjistí, předáváme defacto jen tyto informace jiné straně.
- Když použijeme VPN ve firmě, pak můžeme **navštěvovat i weby, které jsou správcem sítě zakázané**. Nebo třeba ve škole se připojit k maturitnímu kontejneru.
- **Obejití blokování obsahu** – chceme se podívat na video, které je geograficky omezené. Nebo jsme v Číně a chceme se podívat na Reddit či Wikipedii.

IPsec

- **IP security** je bezpečnostní rozšíření IP protokolu založeného na autentizaci a šifrování každého IP datagramu.
- V OSI architektuře se jedná o zabezpečení již na 3. (síťové) vrstvě, čímž poskytuje transparentně bezpečnost jakémukoliv přenosu.
- **Bezpečnostní rozšíření:**
    - **Ověřování** – při přijetí paketu dojde k ověření, zda vyslaný paket odpovídá odesílateli a zda vůbec existuje.
    - **Šifrování** – obě strany se předem dohodnou na formě šifrování paketu. Poté dojde k zašifrování celého paketu krom IP hlavičky, případně celého paketu a bude přidána nová IP hlavička.

OpenVPN

- Volně dostupný software, publikovaný pod licencí GNU General Public License.
- Dokáže **vytvořit šifrovaný VPN tunel** mezi hostitelskými stanicemi.
- S využitím architektury klient-server zajistí přímé spojení mezi počítači za NAT a to bez potřeby jakkoliv NAT konfigurovat.
- Ověření navazovaného spojení se prování pomocí předem sdíleného klíče (preshared key), digitálního certifikátu nebo uživatelského jména a hesla.

- Oficiálně má OpenVPN přidělený port **1194**. Standardně komunikuje pomocí protokolu **UDP**, ale lze použít protokol **TCP**.

12. Technologie poslední míle a diagnostika sítě

- *monitorování provozu na síti (síťový analyzátor, Netflow, ...)*
- *SNMP, princip a použití*
- *xDSL (princip, parametry)*
- *pasivní optické sítě (princip, komponenty, parametry)*
- *Wi-Fi (parametry)*

Poslední míle = propojení mezi koncovým bodem telefonní sítě a účastníkem.

12.1. Monitorování provozu na síti (síťový analyzátor, Netflow, ...)

Wireshark

- Nejznámější, nejvíce rozšířený.
- Pro Unix i Windows.
- Wireshark je open source nástroj pro analýzu síťového provozu. Jeho hlavním účelem je zachytávání a dekódování datových paketů, které procházejí po síti, a zobrazování podrobných informací o těchto paketech v uživatelsky přívětivém rozhraní.
- Wireshark může zachytávat pakety z různých zdrojů, včetně sítě Ethernet, Wi-Fi nebo Bluetooth. Když se spustí, Wireshark začne zachytávat všechny pakety, které procházejí přes síťové rozhraní, které uživatel vybere. Zachycené pakety jsou dekódovány a zobrazeny v seznamu, který uživatel může dále analyzovat.
- Uživatel může provádět různé operace s pakety, například filtrovat je podle různých kritérií, vyhledávat v nich určitá data, nebo analyzovat přenosovou rychlost nebo časy odezvy. Uživatel může také uložit zachycené pakety do souboru a následně je analyzovat později.
- Wireshark funguje tak, že zachytává všechny pakety, které jsou posílány přes dané síťové rozhraní, a poté analyzuje každý paket podle specifikace daného protokolu. Wireshark má rozsáhlou databázi dekodérů, které jsou schopny dekódovat mnoho různých protokolů, včetně běžných jako TCP, UDP nebo HTTP a také méně běžných protokolů.

Netflow

- Otevřený protokol vyvinutý společností Cisco Systems, určený původně jako doplňková služba k Cisco směrovačům.
- Jeho hlavním účelem je monitorování síťového provozu na základě IP toků, které poskytuje administrátorům i manažerům podrobný pohled do provozu na jejich síti v reálném čase. Proto tvoří důležitou a nepostradatelnou součást zabezpečení každé počítačové sítě a je užitečný pro poskytovatele (ISP), kteří na základě NetFlow statistik mohou svým zákazníkům účtovat ceny služeb v závislosti na množství přenesených dat.
- S pomocí NetFlow statistik lze odhalovat vnější i vnitřní incidenty, úzká místa v síti, dominantní zdroje provozu, efektivněji plánovat budoucí rozvoj sítě, sledovat, kdo komunikoval s kým, jak dlouho a s pomocí kterého protokolu.

12.2. SNMP, princip a použití

- Simple Network Management Protocol
- Jednoduchý protokol pro správu sítě.
- Pracuje nad IP protokolem a je založen na modelu agent - manager. Pracuje na aplikační vrstvě (7. vrstva).
- Využívá **UDP** port **161**.
- Na tomto protokolu je dnes založena většina prostředků a nástrojů pro správu sítě.
- Skládá se ze správce a agentů (ty jsou v jednotlivých prvcích – switch / router). Manažer pomocí GET / SET Requestů či Reponses nastavuje či získává data (viz vysvětleno dále).

Má 3 části:

- Samotný SNMP protokol.
- **SMI - Structure and Identification of Managment**

    - Typ dat, které je možno předávat mezi managerem a agentem pomocí SNMP protokolu.
    - **Datové typy:** INTEGER, OCTET STRING, OBJECT IDENTIFIER, NULL.
- **MIB - Managment Information Base**
    - Popisuje sadu objektů, které jsou předmětem správy.
    - **Obsahuje tyto oblasti:**
        - **Správa výkonu** - performance management.
        - **Správa konfigurace** - configuration management.
        - **Účetní a evidenční správa** - accounting management.
        - **Správa poruch a chyb** - fault management.
        - **Správa bezpečnosti** - security management.

Jak SNMP funguje

- Protokol SNMP vyžaduje pro komunikaci dvě strany. Jednou entitou je správce (manager) a druhou agent. SNMP pracuje ve dvou režimech činnosti.
    - Správce posílá dotazy agentovi a přijímá odpovědi. Hodnoty tedy může získávat i více správců a mohou se ptát kdykoliv.
    - Agent zasílá oznámení (trapy) na adresu správce. V nějakých definovaných situacích (překročení nějaké hodnoty nebo i v pravidelném intervalu) odesílá agent jednomu správci hodnoty.
- **Protokol SNMP nyní existuje ve třech verzích.**
    - SNMPv1 a SNMPv2c používají pro autentizaci community string, v podstatě **textové heslo**.
    - V SNMPv3 je možno využít autentizaci pomocí **jména** a **hesla** a šifrování.
- SNMP používá pro komunikaci UDP protokol, díky čemuž je velmi rychlé, ale může dojít ke ztrátě (nedoručení) zasílané informace (paketu).
- Od verze 2 je implementována kontrola doručení, takže ke ztrátě by nemělo dojít. Standardně se používá port 161 (SNMP) na straně agenta (pro dotazy) a port 162 (SNMPTRAP) na straně serveru (pro trapy). Klient, který posílá dotaz, zvolí dynamický port, z kterého posílá dotaz na port 161. Agent odpovídá z portu 161 na dynamický port klienta. V praxi je pro každý dotaz použit jiný dynamický port.

12.3. xDSL (princip, parametry)

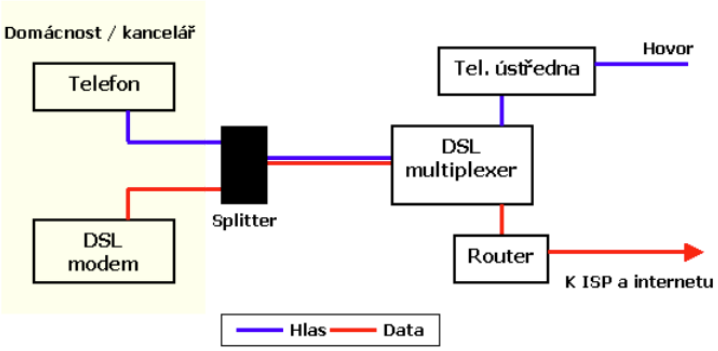
- **DSL – Digital Subscriber Line**. Používá využít současné telefonní vedení pro vysokorychlostní přenos dat.
- Data řazena do **multirámce**.
- V Česku nejvíce rozšířená síť Cetin (bývalá O2).

- **Základní rozdělení:**
  - **Symetrické (Upload (Up Steram) = Download (Down Stream))**
    - HDSL
    - SHDSL
    - VDSL
  - **Asymetrické (Upload (Up Steram) ≠ Download (Down Stream))**
    - ADSL
    - VDSL

VDSL lze konfigurovat libovolně.

Přístup do systému pomocí POTS (Plain Old Telephone Service) splitter

- Odděluje standardní telefonní hovor od ADSL služby.
- Obojí lze přenášet po jediném metalickém vedení.
- Dojde k rozdvojení přicházejícího signálu. Jedna část je přivedena do ADSL modemu, kde je odstraněn standardní telefonní hovor a regenerována data. Druhá část signálu prochází přes dolní propust a jako čistý telefonní signál je přiváděna do telefonního přístroje. Obdobně dochází k oddělení telefonního a ADSL signálu i na straně ústředny.



DSL je potřeba zakončit – na jedné straně **DSLAM** (účastnický koncentrátor – agreguje digitální toky), na druhé uživatel / modem.

- **HDSL**
    - Na rozdíl od ADSL nabízí symetrické rozdělení přenosového pásma, tedy pro příjem i pro vysílání dat je přenosová kapacita stejná.
    - Maximální rychlost 2 Mbps.
    - Dosah 4 km.

- **SHDSL**
    - Standardizace HDSL.
    - Rychlost až cca 2.5 Mbps.
    - Jeden přenosový pár.

- **ADSL**
    - **Asymetrické DSL.**
    - ADSL používá vyšší frekvenční pásmo, díky tomu je možné na stejném vedení provozovat telefonní linku.
    - Telefonní linka (PSTN) slouží primárně k přenosu hlasu, ISDN linka k přenosu digitálního signálu. Na telefonní lince se používají pro potřeby tradičních hlasových hovorů frekvence od 0 do 4 kHz.
    - Vyšší frekvence byly dlouho nevyužity. K provozu ISDN linky se používají frekvence cca 0–50 kHz. U ADSL se pro upload využívají frekvence 138–276 kHz a pro download frekvence 276 kHz – cca 1,1 MHz.
    - Přenášená data se zapouzdří buď do ATM buňky (protokol PPPoA) nebo do Ethernetového rámce (protokol PPPoE).
    - Rychlost u nejnovějších standardů 28 / 3.5 mbps, u původních 8 / 1 mbps.
    - Dosah 2-5 km.

- **VDSL**
    - Symetricky 26 / 26 Mbps.
    - Asymetricky 52 / 6.4 Mbps.
    - Využívá vyšších kmitočtů než ADSL (nad 1 MHz).
    - Lze realizovat pomocí jediného páru telefonních vodičů.
    - Dosah maximálně 1.3 km.

Technologie Bounding

- Od roku 2020 je novou možností nejrychlejšího VDSL internetu **VDSL bonding**.
- Vedení internetu místo po jednom páru po párech dvou, tedy celkem 4 drátech.
- U koncového klienta pak dochází ke spojení těchto dvou linek do jedné formou zapojení speciálního modemu, takzvaného Terminátoru.
- Standardní telefonní zásuvka s koncovkou RJ-11 se předělá na praktičtější ethernetovu zásuvku RJ-45, odkud povede běžný síťový kabel právě do Terminátoru. Ten se postará o sloučení tvou linek, kde je pro vás výstupem opět standardní ethernetový kabel.
- Je ale nutné rozšířit starou internetovou (telefonní) přípojku o další pár drátů.
- V některých lokalitách až 250 Mbps.

12.4. Pasivní optické sítě (princip, komponenty, parametry)

PON (Passive Optical Network)

- Pasivní proto, že mezi ústřednou poskytovatele internetového připojení a koncovým zákazníkem **není nutno používat žádné aktivně napájené síťové prvky**.
- Významnou výhodou jsou **nižší náklady na výstavbu** a provoz oproti sítím aktivním.
- U pasivních sítí dochází jak k úspoře počtu tažených optických vláken (**sdílení přenosové šířky jednoho vlákna více účastníky**), tak **vybavení potřebného pro fungování sítě** (zjednodušení síťových prvků v ústředně poskytovatele).

Komponenty:

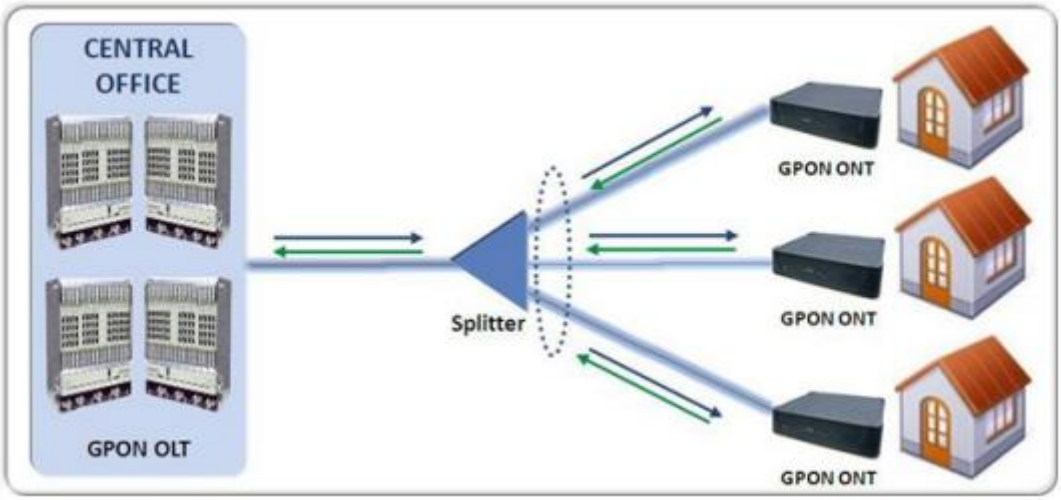
- **Optické linkové zakončení** (Optical Line Termination - OLT) - slouží k zakončení linky na straně internetového poskytovatele. Jeho účelem je konverze elektrického signálu na optický (a zpět) a multiplexování / demultiplexování signálu přenášeného prostřednictvím optického vlákna.
- **Optická distribuční síť** (Optical Distribution Network - ODN) - souborem prostředků (vlákna, síťové prvky) pro přenos mezi síťovými zakončeními.
- **Optická síťová jednotka** (Optical Network Unit - ONU), zakončuje pasivní optickou přístupovou síť na straně zákazníků a stará se o převod signálu (a celkově přenos síťového provozu) mezi domácí sítí koncových zákazníků a přístupovou sítí.
- **Optický síťový zakončovač** (Optical Network Terminal - ONT) - speciální typ **ONU**, které zprostředkovává služby specificky pro jednoho zákazníka.
- **Optický rozbočovač** (Splitter) jednoduché nenapájené zařízení, které umožňuje sdílet více zákazníkům přenosovou šířku jednoho optického vlákna. Přidání každého rozbočovače způsobí zvýšení útlumu na trase.

Funkčnost:

- Pasivní optická síť PON je sítí s topologií **point-to-multipoint**. Z ústředny operátora vede jedno vlákno, jehož signál se dále dělí pomocí optických splitterů a distribuuje přenosovou kapacitu vlákna mezi koncové uživatele (16 až 128 koncových uživatelů ve vzdálenosti 10 – 20 km v závislosti na použité normě a revizi).
- Signál směrem k uživateli je přenášen spolu s daty ostatních uživatelů po jednom vlákně (v zašifrované podobě). K přenosu signálu od uživatele je zapotřebí použít speciální formy **TDM** (časového multiplexu).
- **ONU** leží v různých vzdálenostech od **OLT**, což znamená, že cesta signálu od různých ONU do OLT trvá různě dlouhou dobu. OLT měří zpoždění jednotlivých tras k ONU a na jejich základě vytváří registr. Jakmile je registr

vytvořen, OLT může vysílat jednotlivým ONU tzv. granty. Grant je povolení používat definovaný časový interval pro přenos dat na upstreamu. Mapa grantů je přepočítávána dynamicky každých několik milisekund na základě potřeb pásma jednotlivých ONU.

- Ačkoli lze použít separátně jedno vlákno na downstream a jedno na upstream, používá se téměř výhradně vlákno pouze jedno a data se zmultiplexují pomocí WDM.



Druhy zakončení:

- **FTTC** (Fibre To The Curb) – optické vlákno je přivedeno k uživatelskému rozvaděči, k němuž jsou koncové body sítě připojeny metalickými kabely.
- **FTTB** (Fibre To The Building) – optické vlákno je přivedeno do budovy uživatelů, jednotliví uživatelé jsou však připojení pomocí vnitřní sítě, vnitřních účastnických rozvodů.
- **FTTO** (Fibre To The Office) – optické vlákno je přivedeno až do prostor uživatelů s velkými nároky na přenosovou kapacitu.
- **FTTH** (Fibre To The Home) – optické vlákno je zavedeno přímo do uživatelských zásuvek.
- **FTTN** (Fibre to the Node) – přivádějí se optická vlákna k datovému uzlu Kabinet, k němuž jsou koncové body sítě připojeny metalickými kabely.
- **FTTD** (Fibre to the Desk) – přivádějí se optická vlákna až na “stůl“ účastníků a jsou připojována přímo do zařízení s optickým vstupem.

Normy:

- **APON** - protokol ATM, symetricky cca 150 Mbps, 1998.
- **BPON** – Broadband PON, symetricky cca 150 Mbps, 2001.

- **GPON** - Gigabit PON, 2400 / 1200 Mbps, 2003.
- **EPON** - Ethernet PON, 1200 / 1200, 2004.
- **10G-EPON** – symetricky 10 Gbps, 2006.

12.5. Wi-Fi (parametry)

- Předpokládám, že se má zabývat WISP parametry, protože otázka se zabývá poslední mílí.

WiMax

- Starší rozhraní, dnes se už nepoužívá.
- Rychlosti až 134 Mbps, licenční pásma – 3.5 GHz, 10 GHz, nelicencované 2.4 GHz, 5.7 GHz.

WISP (Wireless Internet Service Provider)

- Používá poskytovatel (ISP) pro bezdrátové (někdy nazývaného jako Wi-Fi) připojení zákazníka.
- Většinou tam, kde není dostupná optika ani xDSL – menší města či vesnice.
- Pracuje na frekvencích 900 MHz, 2.4 GHz, 4.9 GHz, 5 GHz a pak pásma od 6 GHz do 80 GHz. Běžně dostupné u nás 2.4 GHz a 5 GHz.
- Rychlosti okolo max. 100 Mbps, spíše většinou okolo 50 Mbps, na vesnicích ještě méně.
- V ČR cca 900 poskytovatelů WISP, v USA 2000.

Bonus – počítání IPv4 adres

1. **Adresa zařízení 192.168.10.10, maska /26.**
    - **Určíme si velikost bloku a v jakém segmentu se pohybujeme:**
        - /26 – pohybujeme se ve 4. segmentu
        - 26 – 24 = 2 - 2^2 = 4 – rozsah bude rozdělen do **4 bloku** (256/4 = **64 adres na blok**).
        - Nebo to můžeme vzít i jako 32 – 26 = 6 - 2^6 = 64 – (256/6 = 4 bloky).
    - **Můžeme si určit adresu sítě a broadcast adresu.**
        - AS - **192.168.10.0**
        - BA – **192.168.10.63**
    - **Počet hostů:**
        - 64 – 2 = **62** (pokud síť nebudete mít gateway).
    - **Maska:**
        - 256 - 2^6 = 192 ve čtvrtém segmentu.
        - **255.255.255.192**
        - Popřípadě jako: 1111 1111 . 1111 1111 . 1111 1111 . 1100 0000

2. **Adresa zařízení 20.117.15.152, maska /13.**
    - **Určíme si velikost bloku a v jakém segmentu se pohybujeme:**
        - 2. blok (8-16).
        - Bude rozděleno do 2^5 = **32 bloků** – **8** (*255 * 255) **adres** na blok.
    - **Určíte si adresu sítě a broadcast adresu.**
        - AS – **20.112.0.0**
        - BA – **20.119.255.255**
    - **Počet hostů:**
        - 8 * 256 * 256 – 2 (pokud síť nebudete mít gateway).
    - **Maska:**
        - 256 – 2^3 = 248
        - **255.248.0.0**
        - Popřípadě jako: 1111 1111 . 1111 1000 . 0000 0000 . 0000 0000