**13. POČÍTAČOVÉ SÍTĚ I**

Modely vrstev počítačových sítí (ISO/OSI, TCP/IP): funkcionalita a součinnost vrstev, adresace. Fyzická vrstva, signály a jejich kódování, řízení přístupu k médiu.

***PB156***

Počítačová síť je skupina počítačů a zařízení propojená komunikačními kanály, které napomáhají vzájemné komunikaci mezi uživateli a umožňují jim sdílet dostupné zdroje. Základní součástí je přenos dat. Nejznámější počítačovou sítí je Internet.

**Základní vlastnosti sítí:**

* vlastní doručení dat (delivery)
* správnost doručení (accuracy)
* včasnost doručení (timeliness).

**Základní součásti komunikačního systému:**

* odesílatel
* příjemce
* zpráva
* přenosové médium
* protokol

**Základní parametry síťových toků:**

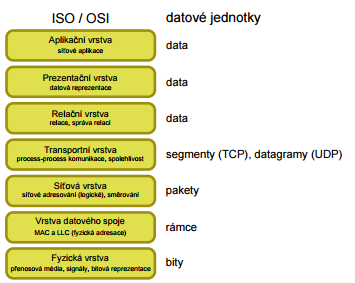
* propustnost
* ztrátovost paketů
* zpoždění přenosu (latence)
* rozptyl (jitter, variabilita v doručování paketů)

**Požadované vlastnosti:**

* efektivita
* spravedlivost
* decentralizovaná správa
* rychlá konvergence při adaptaci na nový stav
* multi/demultiplexing
* spolehlivost
* řízení toku dat

MODELY VRSTEV POČÍTAČOVÝCH SÍTÍ

ISO/OSI Model



* 7-vrstvý model navržen k zajištění **kompatibility** a **interoperability** (schopnost spolupráce mezi různorodými a organizačně nezávislými komponentami) komunikačních systému různých výrobců
* tento model nebyl komunitou široce akceptován což vedlo k **modelu TCP/IP**

**Funkcionalita vrstvené architektury:**

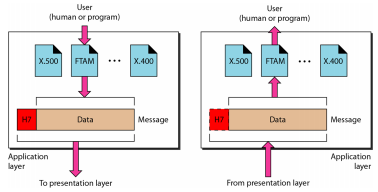
* Každá z vrstev je zodpovědná za určitou (definovanou) funkcionalitu. Aby mohla vrstva požadovanou funkcionalitu zajistit, přidává si do přenášených dat své řídící informace.
* Každá vrstva komunikuje pouze se svými přímo sousedícími vrstvami.
* Každá vrstva využívá služeb poskytovaných vrstvou nižší a poskytuje své služby vrstvě vyšší.
* Funkcionalita je izolována v rámci příslušné vrstvy (pokud dojde ke změně vrstvy, je zapotřebí upravit pouze vrstvy s ní přímo sousedící).
* Z logického pohledu se komunikace odehrává pouze mezi stejnými vrstvami (tzv. peery) obou komunikujících stran; ve skutečnosti však zasílaná data prochází všemi nižšími vrstvami.
* Vrstvy jsou pouze abstrakcí funkcionality – skutečné implementace se více či méně liší.

# 

# 

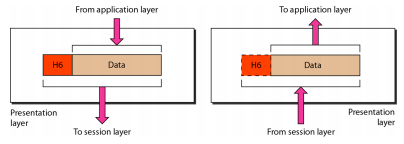
# L7 Aplikační vrstva

* Představuje rozhraní mezi uživatelem (člověkem) a počítačovou sítí.
* Zahrnuje **síťové aplikace (programy)** a **síťové protokoly**.
* Data požadovaná síťovou aplikací jsou balena do aplikačních protokolů a předána prezentační vrstvě (L6).



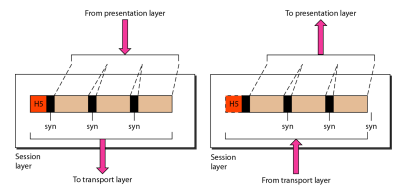
# L6 Prezentační vrstva

* Zajišťuje jednotnou reprezentaci dat na obou komunikujících stranách
* např.: převod kódů abeced EBCDIC ↔ ASCII, přizpůsobení pořadí bajtů, serializace složitých datových struktur do jednoho řetězce (třeba pomocí XML), vytváření společného mezitvaru dat
* V rámci TCP/IP modelu se předpokládá, že tato funkcionalita je zajištěna samotnou aplikací.



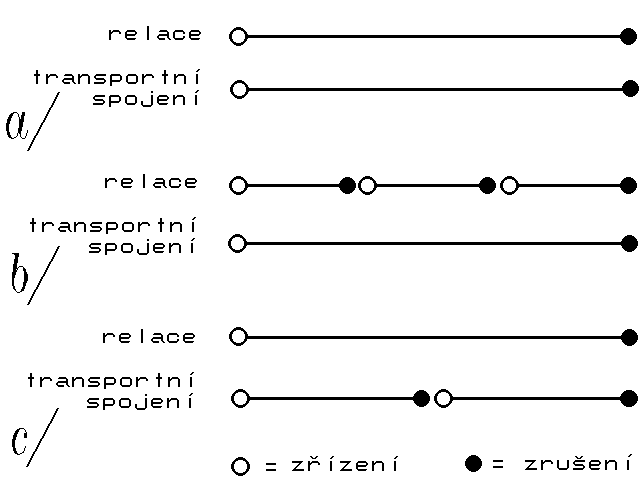
# L5 Relační vrstva

* Spravuje ustavená spojení (relace, dialog, session) mezi komunikujícími aplikacemi.
* V rámci TCP/IP modelu se předpokládá, že tato funkcionalita je zajištěna samotnou aplikací, aplikačním protokolem



## Rozdíl mezi relační a transportní vrstvou:

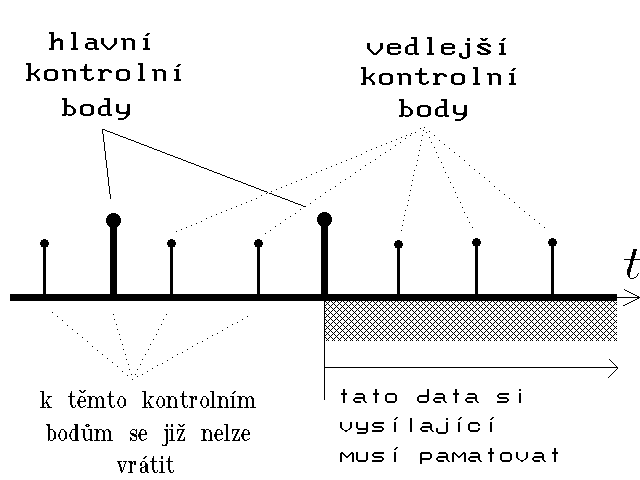
* Analogie s telefonním hovorem kdy telefonní spojení zajišťuje transportní spojení transportní vrstvy a rozhovor dvou účastníků je relace relační vrstvy.

1. Většinou jedno transportní spojení = jedna relace.
2. Na jednom spojení, ale můžeme po sobě proběhnout více relací = odpovídá to rozhovoru dvou lidí, kteří by bez toho, aby položili sluchátko předali telefon někomu jinému a proběhl by zcela nový rozhovor na tomtéž spojení.
3. Během rozhovoru může dojít ke ztrátě spojení. Rozhovor, ale stále není dokončený a tak se vytvoří nové spojení a v rozhovoru se pokračuje.

## Řízení relace:

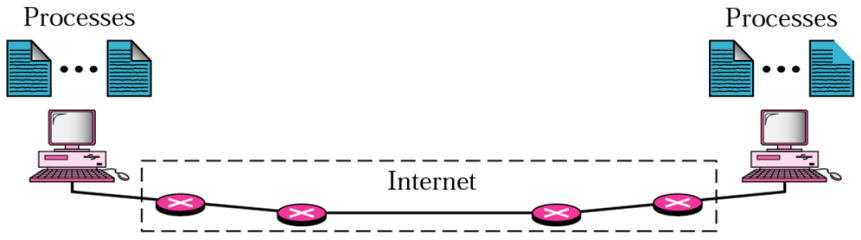
* **Simplexní**
  + Umožňuje komunikaci (přenos informací) pouze v jednom směru.
  + Rozhlas, vysílání rádia/TV, odposlech, pager, GPS atd.
* **Poloduplexní**
  + Komunikace z obou stran – střídají se. Předávání **pověření**.
  + Např. vysílačka
* **Duplex**
  + Současná komunikace obou stran.

## Synchronizace (checkpointing):

* Pro situaci, kdy došlo k chybě na straně příjemce (např. zaseklý papír v tiskárně, chyba na disku), transportní spojení je v pořádku, ale přijemce si nemohl uložit část dat, která v pořádku došla.
* Dva typy bodů: **hlavní** (major) a **vedlejší** (minor)
* Odesílatel si musí pamatovat vše po hlavním bodu. Relační vrstva může vyžádat návrat ke kontrolnímu bodu (hlavnímu nebo vedlejšímu) a nové vyslání dat ležících za tímto bodem.

# L4 Transportní vrstva

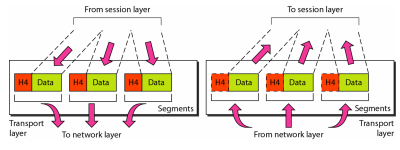
* Komunikace konkrétních aplikací (identifikovány transportní vrstvou) na konkrétních uzlech sítě (identifikovány síťovou vrstvou) – na uzlech tak může běžet více služeb
* **Kde se pohybujeme?:**



* **Služby:**
  + Tvorba paketů
  + Řídí spojení
  + Adresace
    - adresy entit transportní vrstvy (síťových aplikací/služeb) jsou tzv. porty
    - aplikace jsou v síti jedinečně identifikovány dvojící IP\_adresa:port
    - porty: 16bitové číslo kde adresy 0-1023 (210) – well-known ports, 1024-49151 – registrované porty, 49152-65535 dynamické porty
  + Zajištění spolehlivosti přenosu dat s požadovanou kvalitou, transparentnosti
  + Vyrovnává různé vlastnosti a kvalitu přenosových sítí (řízení zahlcení sítě).

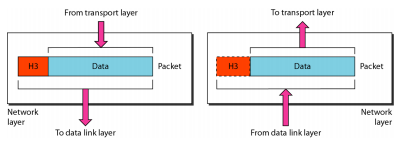
## Řízení spojení:

* **Spojované služby:**
  + na začátku přenosu se vytvoří spojení, které se udržuje po dobu přenosu dat
  + pakety se číslují a je nutné potvrzení o doručení/nedoručení
* **Nespojované služby:**
  + pakety zasílány cílové aplikaci bez ustaveného spojení
  + pakety se nečíslují, mohou dorazit se zpožděním, mimo pořadí nebo se ztratit



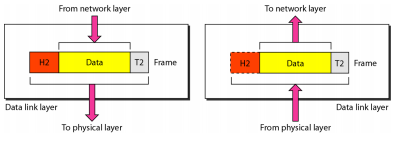
# L3 Síťová vrstva

* Zajišťuje identifikaci (adresaci) a doručení paketů mezi dvěma komunikujícími uzly.
* Součástí je také nalezení vhodné cesty mezi komunikujícími uzly (směrování).
* **Kde se pohybujeme?:**
  + host-to-host delivery
  + propojování lokálních sítí (LAN) do větších, komplexních sítí (WAN např.: Internet)
* **Služby:**
  + propojování fyzických sítí (internetworking)
  + fragmentace/tvorba paketů – segmenty ↔ pakety
  + adresace – IP adresy
  + mapování IP adres na/z fyzické adresy
  + směrování – nalezení nejvhodnější cesty
  + metody základního monitoringu sítě – informace o stavu sítě, uzlů, doručitelnosti paketů



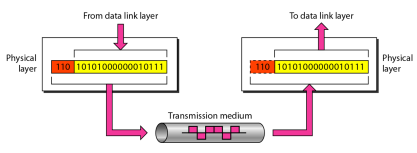
# L2 Vrstva datového spoje

* Zajišťuje přenos dat (rámců) mezi dvěma komunikujícími uzly propojenými sdíleným přenosovým médiem včetně řízení přístupu k tomuto sdílenému médiu.
* **Kde se pohybujeme?:**
  + node-to-node delivery
  + lokální sítě (LAN)
  + přenosové médium sdílené více stanicemi (nutnost adresace stanic)
* **Služby:**
  + tvorba rámců – rámec ↔ paket
  + adresování – fyzické/MAC adresy
  + chybové řízení
  + řízení toku – zabraňuje zahlcení příjemce
  + řízení přístupu k fyzickému médiu – nezbytné v prostředí, ve kterém přenosové médium sdílí více entit; eliminuje kolize způsobené násobným vysíláním



# L1 Fyzická vrstva

* řídí děje v přenosovém médiu
* cíl zajistit přenos jednotlivých bitů (obsah rámců)
* **Kde se pohybujeme?:**
  + pouze point-to-point spoje
  + bez možnosti adresace stanic
* **Služby:**
  + kódování bitů na signál
  + bit-rate control
  + synchronizace bitů
  + multiplexing – proces rozdělení linky (fyzického média) na logické kanály
  + přepínání okruhů



TCP/IP MODEL

# 

* Sedm vrstev modelu ISO/OSI nebylo komunitou široce akceptováno, vznikl TCP/IP model.
* TCP/IP sjednotilo úlohy prvních dvou vrstev ISO/OSI
* protože v Internetu existuje spousta různých aplikací s různými možnosti, dospěli tvůrci TCP/IP k závěru, že bude nejlepší, když si každá aplikace nastaví přenos tak, jak potřebuje a proto jsou také poslední tři vrstvy (aplikační, prezentační a relační) ISO/OSI spojeny do jedné aplikační vrstvy

ADRESACE

# L2 Vrstva datového spoje

* příklad Ethernetového rámce:



* **preambule:**identifikace počátku rámce
* **adresace:** každá stanice (síťová karta) je jednoznačně identifikována MAC adresou (12 hex čísel – např.: 01:23:45:67:89:ab)
* MAC adresa není jednoznačná

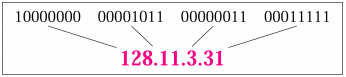
# L3 Síťová vrstva

* požadavek **jednoznačné identifikace** každého zařízení připojeného k internetu
* nutnost systematického **přidělování adres**
* každému zařízení/rozhraní přiřazena internetová adresa **IPv4** (32 bitů) a/nebo **IPv6** (128 bitů)

# Přidělování adres IPv4

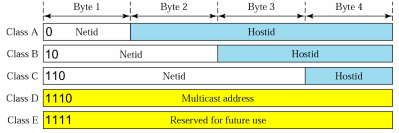
## Typy adres IPv4:

* **Individuální (unicast) adresy** – identifikace jednoho síťového rozhraní (jeden odesílatel/příjemce)
* **Broadcast adresy** – pro zasílání dat všem možným příjemcům do dané LAN
* **Skupinové (multicast)**
  + pro adresování skupiny příjemců, kteří o data projevili zájem
  + data směrovači rozesílána všem členům skupiny
  + zdrojová adresa datagramu (identifikace odesílatele) je unicastová



## Classful Addressing:

* zcela první metoda přidělování adres – pro IPv4
* dvou-úrovňová hierarchie (adresa sítě + adresa uzlu)
* adresní prostor rozdělen do 5 tříd: A - E



**Adresa sítě (NetID)** – identifikuje danou síť

**Adresa uzlu/rozhraní (HostID)** – identifikuje jedinečný uzel v síti NetID

* problém classful adresování je nedostatečná granuralita – každá třída rozdělena na pevný počet sítí s maximální velikostí → plýtvání adresním prostorem → dá se řešit přidělováním více menších tříd → nárůst směrovacích tabulek
* používané řešené jsou **subnetting** a **supernetting**

### subnetting

* možnost tříúrovňové hierarchie (adresa sítě + podsítě + uzlu)
* zvenčí vypadá jako 1 síť (1 záznam ve směrovací tabulce), podsítě se rozlišují až na hraničním směrovači

### supernetting

* spojuje několik původně samostatných IP adres v jednu výslednou (musí být sousední)

### Maska sítě/podsítě:

* subnetting i supernetting využívají masku sítě (obsahuje 1 v bitech, které odpovídají síťové části adresy, 0 - relativní adresa uzlu v rámci sítě)
* adresa sítě = IP adresa uzlu && maska sítě

## Classless Addressing:

* zobecnění a rozšíření sub/supernettingu
* zcela variabilní délka bloku adresy (maska sítě nutná)
* přiřazováno hierarchicky

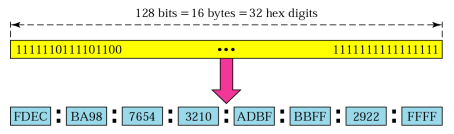
### CIDR – Classless Inter-Domain Routing

* nahrazuje třídy (A, B a C)
* rozdělení do CIDR bloků (velikost dána maskou)

### NAT – Network Address Translation

* pro domácí uživatele
* skrývá vnitřní sítě za jednu externí adresu
* překlad adres procházejících síťovým prvkem (např.: NAT směrovačem)

# IPv6



* úvodní nuly lze ze zápisu každé skupiny vynechat
* sekvenci po sobě jdoucích nulových skupin lze vynechat **ale pouze jednou**

## Struktura:



* globální směrovací prefix ≈ adresa sítě
* IPv6 je pouze classless (CIDR)

## Typy adres IPv6:

* **Individuální (unicast) adresy** – totéž co IPv4
* **Skupinové (multicast) adresy** – totéž co IPv4
* **Výběrové (anycast) adresy**
  + nově v IPv6
  + také označují skupinu příjemců
  + data se však doručí jen jedinému jejímu členovi (tomu, který je nejblíže)
  + použití např.: pro aktualizace tabulek DNS
* Broadcast adresy v IPv6 nejsou, byly nahrazeny speciálními multicastovými skupinami

# Interakce L3 a L2

* mechanismus doručení dat v IP sítích – hop-by-hop
* vlastní předání/doručení zprávy na základě fyzických (MAC) adres
* 2 alternativy:
  + **odesílatel a příjemce na stejné LAN** – IP datagram obsahuje IP adresu příjemce, rámec L2 vrstvy MAC adresu **příjemce**
  + **odesílatel a příjemce na různých LAN** – IP datagram obsahuje IP adresu příjemce, rámec L2 vrstvy MAC adresu **směrovače →** směrovač po přijetí (a zpracování) datagramu jej vloží do nového rámce s MAC adresou dalšího směrovače ve snaze přiblížit se cíli (odtud hop-by-hop)
* nutnost mapování IP adres na fyzické (MAC) adresy
  + **statické mapování** – vytvoření tabulek s páry (IP adresa, MAC adresa), obtížné spravovatelné
  + **dynamické mapování** – pomocí **ARP** (Address Resolution Protocol)

## ARP (Address Resolution Protocol):

* protokol pro zjištění MAC adresy uzlu/směrovače na základě IP adresy
* existuje i **RARP** (Reverse Address Resolution Protocol - z MAC na IP adresu), ale už se nepoužívá

### mechanismus:

1. zaslání tzv. ARP request paketu všem uzlům na dané LAN (broadcast) – paket obsahuje IP & MAC adresu odesílatele a IP adresu hledaného uzlu
2. paket zpracován všemi uzly; odpoví jen ten, jehož IP adresa se shoduje s hledanou, ostatní paket zahodí
3. hledaný uzel žadateli odpovídá tzv. ARP reply paketem

# L4 Transportní vrstva

* adresy entit transportní vrstvy (síťových aplikací/služeb) jsou tzv. porty
* aplikace jsou v síti jedinečně identifikovány dvojící IP\_adresa:port
* porty: 16bitové děleno do tříd:
  + **well-known ports** – přidělované organizací IANA, identifikují známou službu, rozsah 0-1023
  + **registrované porty –** lze u IANA (Internet Assigned Numbers Authority) registrovat, volně použitelné, rozsah 1024-49151
  + **dynamické porty** – dynamicky přidělované porty, využity zejména jako zdrojové porty odesílacích aplikací, rozsah 49152-65535
* Mechanismus adresace L4 představuje formu **multiplexingu** a **demultiplexingu**:
  + **multiplexing –** na odesílací strane mnoho aplikací a jeden transportní protokol, odesílací aplikace identifikovaná zdrojovým portem
  + **demultiplexing** – na přijímací straně jeden transportní protokol, výběr vhodné aplikace pro doručení, přijímající aplikace identifikovaná cílovým portem

(TCP a UDP platí pouze pro architekturu TCP\IP)

**TCP** – Zajišťuje přenos dat se zárukami, který vyžadují aplikace, kde nesmí „chybět ani paket“. Jedná se o přenosy souborů, e-mailů, WWW stránek atd. Záruka se vztahuje na řešení ztrát přenášených paketů, zachování jejich pořadí a odstranění duplikace. Jednotkou posílané informace je na této vrstvě **TCP segment**.

**UDP** – Zajišťuje přenos dat bez záruk, který využívají aplikace, u kterých by bylo na obtíž zdržení (delay) v síti způsobené čekáním na přenos všech paketů a ztráty se dají řešit jiným způsobem (např. snížení kvality, opakování dotazu). Využívá se pro DNS, VoIP, streamované video, internetová rádia, vyhledávání sdílených souborů v rámci sítě DC++, on-line hry atp. Jednotkou posílané informace je na této vrstvě **blok dat**.

FYZICKÁ VRSTVA

* pouze point-to-point spoje
* bez možnosti adresace stanic
* přenáší dat ve formě bitů mezi komunikujícími uzly
* přenosové médium je pasivní entita, žádná logika řízení

# Služby

* **kódování bitů na signál** – reprezentace bitů signálem
* **bit-rate control** – množství bitů poslaných za sekundu
* **synchronizace bitů** – časování bitových přenosů (synchronizace bitů poskytováním časovacích mechanismů, které kontrolují odesílatele a příjemce)
* **multiplexing** – proces rozdělení linky (fyzického média) na logické kanály
* přepínání okruhů

# Signál

* data se transformují na elektromagnetické (optické) signály, aby se mohla přenášet médiem
* signál – časová funkce reprezetující změny fyzikálních (elektromagnetických) vlastností přenosového média
* defekty signálu – **slábnutí** (způsobeno odporem média), **zkreslení** (rozdílnou rychlostí šíření různých frekvencí), **šum** (vliv cizorodé energie)
* digitální data určená k přenosu (bity) lze přenášet **analogovým** nebo **digitálním** signálem

## Analogový signál:

* spojitý v čase – pozvolná změna
* dá se šířit vodiči nebo bezdrátově
* např.: zvuk
* digitální data při přenosu modulují analogový signál (digitální modulace), k čemuž slouží modem (MOdulátor/DEModulátor)
* modulace může být amplitudová (mění se amplituda – výška amplitudy), frekvenční (mění se frekvence – rychlost opakování) nebo fázová (mění se fáze nosného signálu).

## Digitální signál:

* je diskrétní – mění se skokově
* šíří se jenom vodiči[[1]](#footnote-0)
* např.: data v diskrétních hodnotách, bity!
* binární data je potřeba na něj měnit – kódování

## Kódovaní:

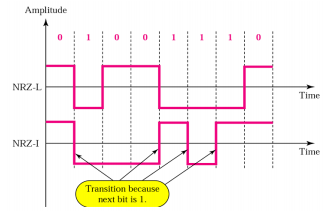
* největším problémem kódování je synchronizace signálu mezi vysílačem a přijímačem
* změnu úrovně signálu (0⟶1, 1⟶0) lze využít pro synchronizaci hodin, ale dlouhé posloupnosti 0 a 1 představují problém
* typy kódování jsou **přímé**, **NRZ**, **Manchester**, **4B/5B**

### Přímé kódování

* 1 představuje kladnou a 0 nulovou hodnotu amplitudy
* žádná samosynchronizovatelnost

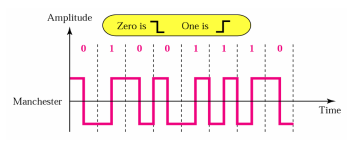


### NRZ (Non Return to Zero) kódování

* NRZ-L – 1 = záporná, 0 = kladná amplituda
* NRZ-I – 1 = změnu polarizace amplitudy, 0 = žádná změna 

### Manchester

* každý bit je kódován 2 prvky signálu
* snížení efektivní přenosová kapacita
* plná samosynchronizovatelnost



### 4B/5B

* uměle zavedená redundance pro zabezpečení synchronizace včetně možnosti detekce chyb
* substituce 4-bitových bloků nahrazeny 5-bitovými vzorky (max 3 nuly za sebou, vlastní přenos pomocí NRZ-I)
* každý vzorek může začínat maximálně jednou nulou a končit maximálně dvěma

# Přenosová média

* poskytují prostředí pro činnost fyzické vrstvy
* jsou voděná (kroucená dvoulinka, koaxiál, optické vlákno) a nevoděná (rádiové, mikrovlné nebo infračervené signály)

## Multiplexing:

* technika sdílení dostupné přenosové kapacity přenosového média souběžnými komunikacemi
* efektivnější využití média
* zejména optické vlákna a bezdrátové média
* pro analogové signály (**FDM** a **WDM**) i pro digitální (**TDM**)

### Analogové signály:

* **FDM (Frequency-Division Multiplexing)** – každý signál je modulován samostatným nosným signálem s unikátní frekvencí, signály se kombinují do nového signálu (např.: telefonní spoje mezi ústřednami)
* **WDM (Wave-Division Multiplexing)** – FDM pro optické signály, každá barva světla (vlnová délka) reprezentuje 1 kanál

### Digitální signály:

* **TMD (Time-Division Multiplexing)** *–* v libovolném okamžiku kanál využívá výhradně jeden vysílající

ŘÍZENÍ PŘÍSTUPU K MÉDIU

* MAC (Medium Access Control) je funkcionalita odpovědná za koordinaci přístupu více stanic ke sdílenému přenosovému médiu
* snaží se eliminovat kolize pří vysílání, tj. zamezit souběžnému vysílání do jediného přenosového prostředí
* protokoly řízení přístupu se dělí na protokoly **neřízeného přístupu**, **řízeného přístupu** a **multiplexově řízeného přístupu**

## MAC protokoly neřízeného přístupu

* **Aloha**
  + stanice vysílá kdykoliv má připravený rámec
  + kolize detekovány nepřijetím potvrzení o přijetí v definovaném časovém intervalu
  + po kolizi náhodnou dobu vyčká a zkusí vysílat znovu
  + neefektivní
* **CSMA/CD (Carrier-Sense Multiple Access)** 
  + upravená Aloha – stanice vysílá jen když zjistí klid v médiu
  + současně na médiu naslouchá pro detekci případné kolize (CD = Collision Detection)
  + aplikace v klasickém LAN Ethernetu; nepoužitelné v nevoděném médiu
* **CSMA/CA** 
  + obcházení kolizí (CA = Collision Avoidance)
  + použitelné v nevoděném médiu

## MAC protokoly řízeného přístupu:

* stanice smí vysílat jen tehdy, když k tomu získá právo od řídící stanice.
* **rezervace –** vysílání v předem domluvených intervalech
* **polling (vyzývání) –** centrální stanice zjistí, jestli stanice chce vysílat – pokud ne, přechází k další
* **token ring (předávání příznaku) –** ten, kdo vlastní token, má právo k vysílání

## Protokoly multiplexově orientovaného přístupu:

Zpřístupňují fyzické vrstvě multiplexing – logické rozdělení na více kanálů.

**FDMA, TDMA** - viz výše.

TOPOLOGIE SÍTÍ

Fyzické uspořádání stanic na médiu.

## Sběrnice (bus topology):

Jednoduše instalovatelná. CSMA/CD jako protokol řízení k přístupu. Náchylná k defektům: výpadek kabelu = výpadek sítě. Kolizní doména tvořena všemi stanicemi.

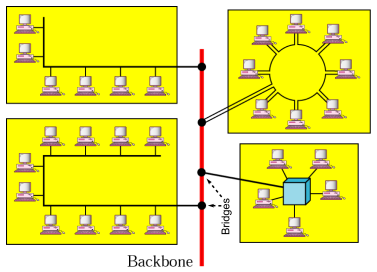
## Kruhová (ring topology):

Všechny zprávy putují v jednom směru. Kolizní doména tvořena všemi stanicemi. Právo vysílat určuje metoda peška. Velmi náchylná k defektům: výpadek kabelu = výpadek sítě.

## Hvězdicová topologie (star topology):

Centrální propojovací bod (hub, bridge, switch). Hůře instalovatelná. Kolizní doména závisí na propojovacím bodu: hub (všechny stanice), bridge/switch (pouze dvě sousední stanice). Nepříliš náchylná k defektům.

## Budování L2 sítí:

* **můstek:**transparentní propojení sítí, všechen provoz přechází přes něj, odděluje sdílená média, může mít více jak dvě připojení; **přepínač** = víceportový můstek
* založeno na MAC adresách: Backward Learning Algorithm – můstek se učí umístění stanic nasloucháním na médiu

1. Li-Fi - <https://en.wikipedia.org/wiki/Li-Fi> [↑](#footnote-ref-0)