AP4PS – Počítačové sítě

Obsah

[1. Používané číselné soustavy 2](#_Toc65793670)

[2. Základní síťová terminologie 3](#_Toc65793671)

[3. Historie počítačových sítí 5](#_Toc65793672)

[4. Dělení počítačových sítí 6](#_Toc65793673)

[5. Média pro přenos síťových informací 8](#_Toc65793674)

[6. Koaxiální kabel 10](#_Toc65793675)

[7. Kroucená dvojlinka 11](#_Toc65793676)

[8. Strukturovaná kabeláž 13](#_Toc65793677)

[9. Optický kabel 14](#_Toc65793678)

[10. Komunikace vzduchem 19](#_Toc65793679)

[11. Přenos signálu 24](#_Toc65793680)

[12. Topologie sítí 28](#_Toc65793681)

[13. Principy přístupových metod 31](#_Toc65793682)

[14. Normování počítačových sítí 34](#_Toc65793683)

[15. Datagramová služba a virtuální spoj 38](#_Toc65793684)

[16. Potvrzování PDU (Protocol Data Unit) 39](#_Toc65793685)

[17. Síťové protokoly 41](#_Toc65793686)

[18. Adresování v TCP/IP sítích 44](#_Toc65793687)

[19. TCP/IP port a socket 49](#_Toc65793688)

[20. Propojování počítačových sítí 50](#_Toc65793689)

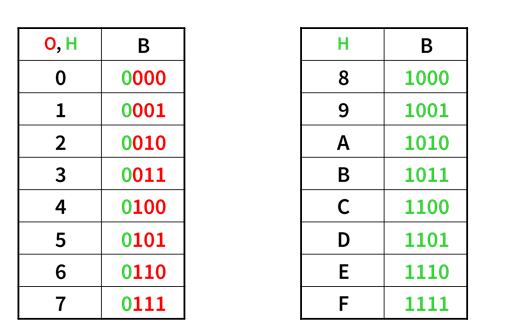
[21. Síť Ethernet 54](#_Toc65793690)

[22. Internet 62](#_Toc65793691)

# 1. Používané číselné soustavy

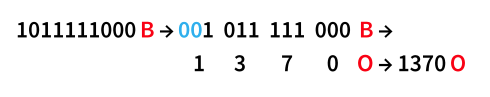
* **Dvojková** (Binární, číslice 0 a 1, označení za číslem B)
* **Osmičková** (Oktálová, číslice 0 až 7, označení za číslem O)
* **Desítková** (Dekadická, číslice 0 až 9, označení za číslem žádné nebo D)
* **Šestnáctková** (Hexadecimální, číslice 0 až 9 a písmena A až F, označení za číslem H)

### Převod číselných soustav



#### Převod z Binární na Oktálovou

* Binární číslo rozdělíme po trojicích zprava (nejvýznamnější bit(y)
* Doplníme zleva nulami na trojici a binární trojice převedeme na oktálové čísla

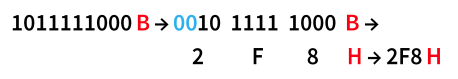


#### Převod z Oktálové na Binární

* Místo oktálových číslic napíšeme odpovídající binární trojice, nevýznamné nuly zleva nepíšeme

#### Převod z Binární na Hexadecimální

* Binární číslo rozdělíme po čtveřicích zprava (nejvýznamnější bity)
* Doplníme zleva nulami na čtveřici a binární čtveřice převedeme na hexadecimální čísla



#### Převod z Hexadecimální na Binární

* Místo hexadecimálních číslic napíšeme odpovídající binární čtveřice, nevýznamné nuly zleva nepíšeme

# 2. Základní síťová terminologie

#### internet

* Jakákoliv soustava vzájemně propojených sítí (např. i v jednom pokoji)
* internetů je velké množství
* internet má vlastníka (např. vnitřní síť firmy)

#### Internet

* Jméno jedné konkrétní soustavy vzájemně propojených sítí
* Internet je pouze jeden
* Jako celek nemá žádného vlastníka
* Své vlastníky mají jen dílčí sítě internetu

#### Intranet

* Tvoří příslušnou část sítě organizace, slouží pro samotnou organizaci, poskytuje aplikace a služby uvnitř organizace

#### Extranet

* Tvoří příslušnou část sítě organizace sloužící pro poskytování aplikací a služeb externím organizacím a uživatelům

#### Typy sítí a jejich rozlehlost

* PAN (Personal Area Network) – metry (až desítky metrů)
* LAN (Local Area Network) – desítky až stovky metrů
* CAN (Campus Area Network) – stovky metrů až kilometry
* MAN (Metropolitan Area Network) – kilometry až desítky kilometrů
* GAN (Global Area Network) – globální
* VLAN (Virtual LAN)
* WLAN (Wireless LAN)
* VPN (Virtual Private Network)
* SAN (Storage Area Network)

### Data přenášená po síti

#### Zpráva

* Balík dat (mail, web, soubor…), který přenášíme po síti
* Balíky dat většinou nemají stejnou délku

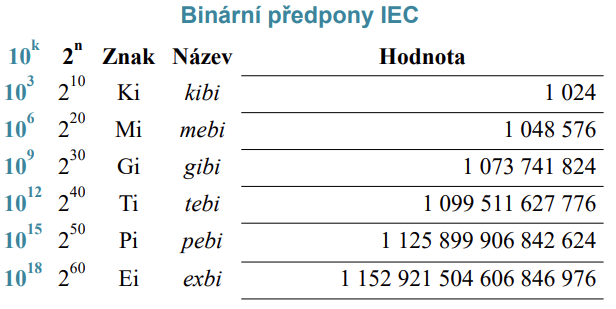
#### Segment, datagram, paket a rámec

* Balík dat o stanovené pevné délce na různých úrovních síťového SW a HW

### Přenosová a modulační rychlost

#### Přenosová rychlost

* Používají se mocniny při základu 10, tedy dle SI: kb/s, Mb/s, Gb/s
* Hodnoty s mocninami při základu 2 se používají pro označení kapacity paměti – KiB, MiB, GiB..
* Přenosovou rychlost měříme na přenosovém médiu (throughput), nebo na úrovní síťové aplikace (goodput) Goodput je throughtput mínus provozní režie pro zřízení relací, potvrzení a zapouzdření.



#### Modulační rychlost

* V Bd, udává počet změn signálu za sekundu
* Přenosová rychlost se až na vyjímky nerovná modulační rychlosti (např. u Ethernetu 10 Mb/s je modulační rychlost rovna dvojnásobku přenosové rychlosti, tedy 20MBd)

### Typy přenosů

#### Simplexní přenos

* Data jsou přenášená jen jedním směrem – většina přenosů na optických vláknech (existují i složitější technologie, které umožňují na jednom optickém vlákně plně duplexní provoz)

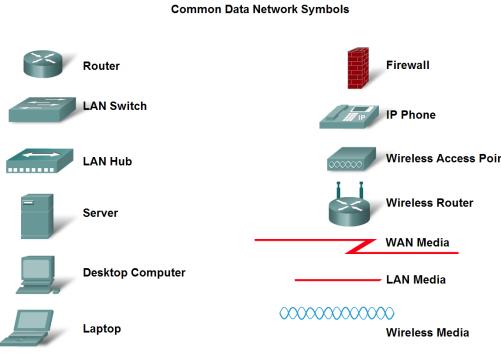
#### Polo duplexní přenos

* Data jsou přenášena oběma směry, ale v daném okamžiku jen jedním směrem – Ethernet do 1 Gb/s

#### (Plně) Duplexní přenos

* Data jsou přenášena oběma směry současně – Ethernet 10 Gb/s

### Symboly síťových zařízení

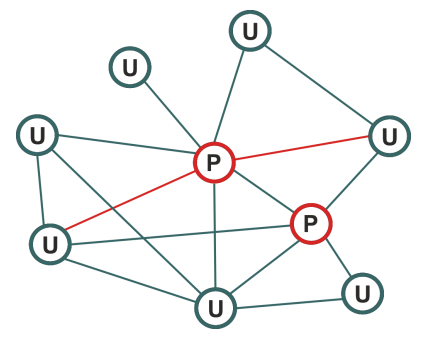
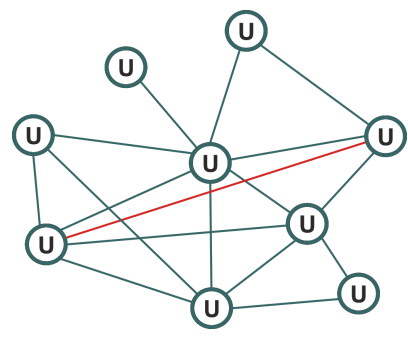


# 3. Historie počítačových sítí

### Počátky počítačových sítí

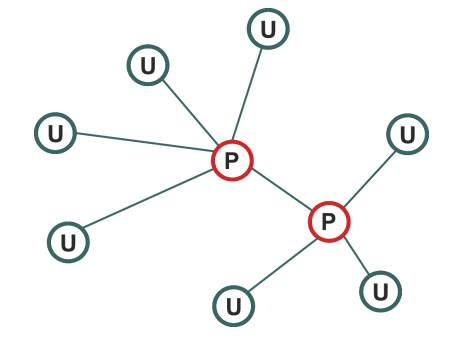
* V počátku 70. let vznikaly první izolované počítačové sítě různých výrobců
* Později vznikají sítě s polygonální strukturou – první přepojovací uzly

#### Síť bez přepojovacích uzlů Síť s přepojovacími uzly



#### Nadbytečná propojení Nezbytně nutná propojení





### Další vývoj počítačových sítí

* Vznik PC (1981) – požadavek na vznik LAN
* Propojování LAN navzájem
* Připojování LAN do WAN
* Internet překračuje území USA (1983)
* Připojování LAN a WAN v dalších zemích do Internetu
* Bezdrátové a optické sítě

# 4. Dělení počítačových sítí

### Homogenní a nehomogenní PS

#### Homogenní

* Stejná HW platforma
* Všechny počítače v síti mají stejný OS
* Je používán stejný přenosový protokol

#### Nehomogenní

* Různá HW platforma
* Počítače v síti používají různé OS
* Jsou používány různé přenosové protokoly

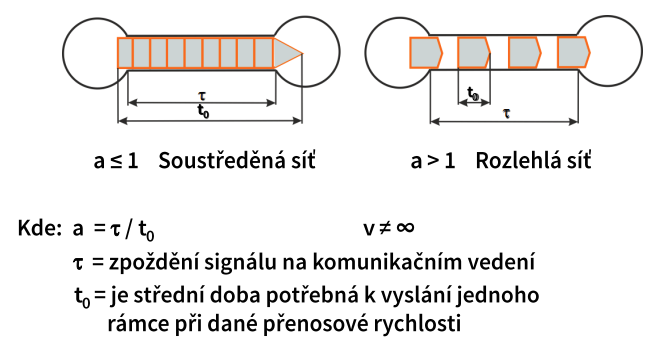
### Rozlehlé a soustředěné PS

#### Rozlehlé (WAN)

* Na vedení se může v daném okamžiku šířit více rámců

#### Soustředěné (LAN)

* V daném okamžiku se na vedení může šířit pouze jeden rámec



### PS Client to server a Peer to peer

#### Client to server

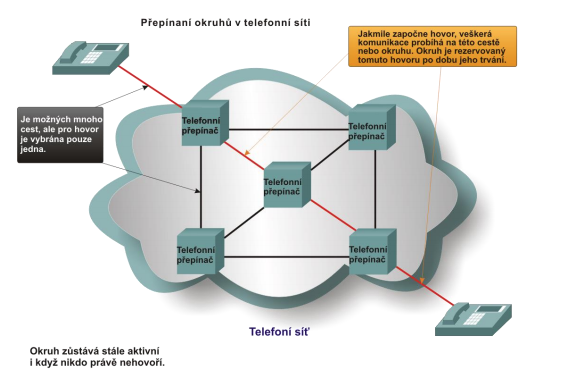
* Ostře vyhraněné funkce počítačů
* Většina komunikace probíhá mezi klientem a serverem
* Server zprostředkovává komunikaci mezi klienty

#### Peer to peer

* Nejsou ostře vyhranění funkce počítačů
* Každý počítač může pracovat jako klient i jako jednoduchý server

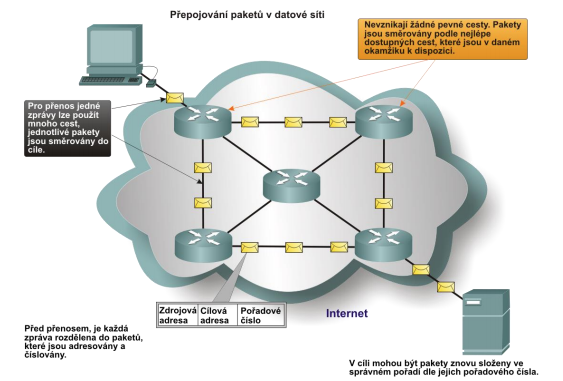
### PS s přepojováním okruhů

* Rezervované spoje mezi dvěma koncovými uzly
* Po celou dobu spojení máme pro sebe volný komunikační kanál
* Paket nepotřebuje žádnou hlavičku – pakety přijdou v pořadí, v jakém byly vyslány, je jednoznačné, kdo pakety odeslal, a tedy komu přijde případná odpověď
* Nevýhodou je blokování celého komunikačního kanálu po dobu spojení pro datové přenosy jiných koncových uzlů



### PS s přepojováním paketů

* Pakety se posílají z uzlu na uzel, když je volný komunikační kanál
* Přepojovací uzly pracují systémem store and forward
* Komunikační kanál může přenášet data od více druhů síťového provozu, nebo více koncových uzlů
* Jednotlivé pakety se mohou přenášet alternativními cestami
* Vzhledem k alternativním cestám a různém zpoždění na přepojovacích uzlech je nutné zavést hlavičku paketu
* Použito např. v GAN Internet a v navzájem propojených kancelářských LAN



### Metalické, optické a bezdrátové PS

#### Metalické PS

* Komunikačním médiem jsou měděné vodiče – kroucená dvojlinka a koaxiální kabel
* Informace přenáší elektrický proud ve vodičích

#### Optické PS

* Komunikačním médiem jsou optická vlákna – skleněná, nebo plastová
* Informace přenáší infračervené záření šířící se optickými vlákny

#### Bezdrátové PS

* Komunikačním médiem je „vzduch“
* Informace přenáší rádiové vlny

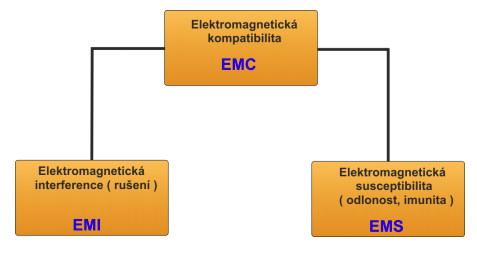
# 5. Média pro přenos síťových informací

### Nejběžnější přenosová média

* Fyzická média, kterými jsou přenášena data ze zdroje ke svému cíli
* Elektrické vodiče (obvykle měděné)
  + Koaxiální kabel (silný, tenký)
  + Kroucená dvojlinka
* Optická vlákna
* Vzduch (bezdrátový přenos)

### Základní charakteristiky přenosového média

* Odolnost proti vnějšímu elektromagnetickému rušení – EMS (Electromagnetic Susceptibility)



* Náhodná energie z vnějších zdrojů, která může interferovat se signály přenášenými komunikačním médiem
* Zdrojem mohou být např. motory, lékařské přístroje, fluorescenční osvětlení, mobilní telefony, atmosférická elektřina…

#### Šířka pásma

* Vztahuje se k množství dat, které lze přenést komunikačním kanálem, udává se:
  + b/s (bps) – pro digitální signály
  + Hz – pro analogové signály

#### Útlum

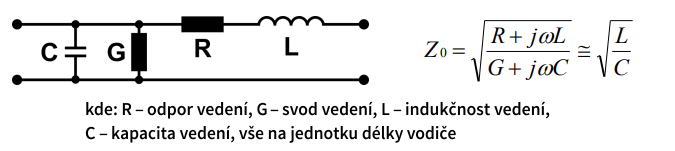
* Snížení intenzity signálu na médiu se vzdáleností
* Udává se v dB na délku média (100 m, 1 km)
* - 6 db/ - 3 dB značí 50% útlum napětí/ výkonu

#### Zesílení

* Analogický výpočet, kladná hodnota

#### Impedance (charakteristická impedance)

* Velikost odporu vodiče střídavému elektrickému proudu, která pomáhá určit útlumové vlastnosti vodiče
* Značí se Z0 a jednotkou je Ω (Ohm)
* Dále předpokládáme sinusový signál, kdy Z0 je funkcí frekvence. Pro zjednodušení pak předpokládáme homogenní bezztrátové vedení (R a G = 0)



#### Přeslech mezi vodiči

* Rušení signálem ze sousedního vedení
* Udává se v dB
* a = 10 x log10 (P1/ P2), kde P1 je vyzářený výkon a P2 je pohlcený výkon
* Čím vyšší je kladná hodnota **a**, tím nižší je toto vzájemné rušení

#### Možnost odposlechu

#### Cena

### Přenos dat v základním a přeloženém pásmu

#### Základní pásmo (Baseband)

* Přenáší se pouze jedny data (data se většinou kódují)

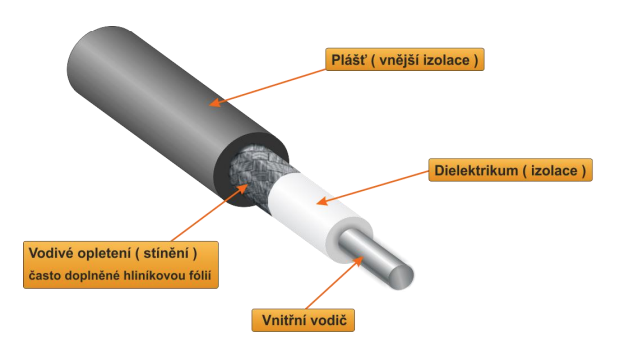
#### Přeložené pásmo (Broadband)

* Může se přenášet více dat současně na různých nosných frekvencích (data se musí modulovat)

# 6. Koaxiální kabel

* Nazývaný též jako coax (Common axis)
* Vykazuje poměrně dobré parametry při frekvencích pod 1 GHz, nad 1 GHz jen kratší úseky

### Konstrukce



#### Vnitřní vodič

* Vyrobený většinou z mědi, může být i postříbřený
* Plný, nebo splétaný
* Jeho průměr (popř. počet vláken) je jedním z faktorů ovlivňujících útlum

#### Dielektrikum

* Izolační vrstva vyrobená z dielektrika, které je umístěno kolem vnitřního vodiče
* Jako dielektrikum se používá upravený polyetylen, nebo teflon pro vyšší teploty

#### Fóliové stínění

* Stínění z tenké fólie kolem dielektrika, bývá pod vodivým opletením, pokud jej kabel má
* Obvykle z hliníku
* Toto stínění nemají všechny koaxiální kabely
* Malá ohebnost kabelu, určeno pro pevné rozvody

#### Splétané stínění, vodivé opletení

* Splétaný měděný vodič
* Může sloužit vnitřnímu vodiči jako zemnění
* Spolu s fóliovým stíněním chrání vnitřní vodič před cizími EM poli

#### Plášť

* Vnější kryt, dříve vyroben z PE a PVC, dnes většinou z LSZH (Low Smoke Zero Halogen)
* Pro vyšší teploty se používá teflon

### Vlastnosti koaxiálního kabelu

* Asymetrické přenosové médium
* Signál se přenáší jako rozdíl napětí mezi středním vodičem a stíněním
* Stínění se připojuje na kostru zařízení (ukostřuje), má tedy nulovou hodnotu napětí
* Koaxiální kabely se vyrábějí s různou hodnotou impedance, např:
  + Ethernet (muzeum) a bezdrátové sítě (pigtail): 50 Ω
  + TV, kabelový internet a VKV 75 Ω
  + Arcnet (muzeum) 93 Ω

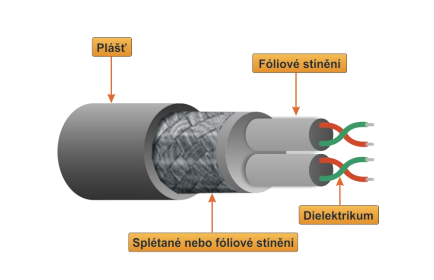
#### Výhody

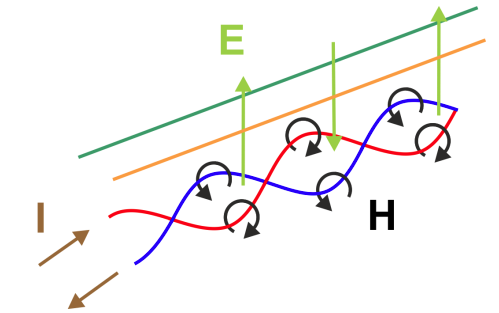
* Velká EMS, malé EMI
* Relativně snadná instalace
* Může sloužit i k přenosu hlasu a videa

#### Nevýhody

* Náchylný k poškození – deformace dielektrika a stínění, přetržení fóliového stínění…

# 7. Kroucená dvojlinka

* Označována též jako TP (Twisted Pair)
* Může přenášet data s rychlostí do 10 Gb/s do 100 m
* Dva vodiče jsou vždy vzájemně kolem sebe obtočeny (minimalizuje EMI a ztráty způsobené kapacitním odporem, tj. tendencí nevodiče uchovávat elektrický náboj, maximalizuje EMS)
* Symetrické přenosové médium
* Signál je přenášen jako rozdíl napětí mezi těmito dvěma vodiči (způsobuje menší náchylnost k rušení a útlumu)
* Eliminace elektrického a magnetického pole



### Konstrukce

#### Vodiče

* Vždy v párech vzájemně kolem sebe obtočeny
* Obvykle z mědi
* Mohou být plné, nebo splétané
* Počet párů je různý (2, 4, 6, 8, 25, 50, 100), pro síťové aplikace jsou použity 2 páry (Ethernet 10 Mb/s a 100 Mb/s), nebo 4 páry (Ethernet 1 Gb/s a 10 Gb/s), dielektrikum je polyetylen, nebo teflon pro vyšší teploty

#### Stínění

* Fóliové stínění každého páru vodičů
* Splétané, nebo fóliové stínění kolem všech párů

#### Plášť

* Vnější kryt z PVC, LSZH, nebo teflonu pro vyšší teploty

### Dělení dle stupně stínění

* Impedance všech typů je 100 +- 15 Ω
* Písmeno před lomítkem určuje typ stínění celého kabelu
* Písmeno před TP určuje typ stínění krouceného páru

#### UTP (Unshielded Twisted Pair)

* U/UTP
* S/UTP
* F/UTP

#### STP (Shielded Twisted Pair)

* U/STP
* S/STP
* F/STP

#### FTP (Foiled Twisted Pair)

* U/FTP
* S/FTP
* F/FTP

### Výhody

* Snadné připojování jednotlivých zařízení
* Možno využít i pro telefonní rozvody (popř. jiné) – strukturovaná kabeláž
* S/FTP má velmi dobrou EMS a nízké EMI
* Snadná instalace
* Nízká cena

### Nevýhody

* S/FTP je silný a obtížně se s ním pracuje
* U/UTP má horší EMS než koaxiální kabel
* U/UTP signály nemohou bez regenerace (zesílení a čištění) být přenášeny na větší vzdálenost ( ve srovnání s jinými typy kabelů)

### Kategorie (CAT) kroucených dvojlinek (ŠP – šířka pásma)

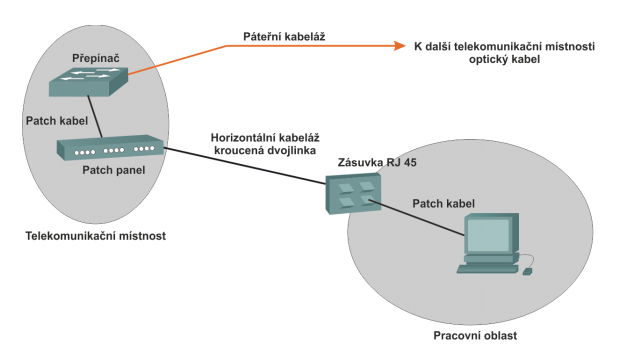
* 1 – přenos hlasu do 1 Mb/s, PTSDN, ISDN, zvonek
* 2 – ŠP 1,5 MHz, 4 Mb/s, Token Ring
* 3 – ŠP 16 MHz, 10 Mb/s, Ethernet
* 4 – ŠP 20 MHz, 16 Mb/s, Token Ring
* 5 – ŠP 100 MHz, data do 100 Mb/s Ethernet, 155 Mb/s ATM
* 5E – ŠP 100 MHz, 1 Gb/s Ethernet
* 6 – ŠP 250 MHz, 10 Gb/s Ethernet s problémy
* 6A – ŠP 500 MHz, vyvinut pro 10 Gb/s Ethernet
* 7 – ŠP 600 MHz, data do 10 Gb/s Ethernet
* 7A – ŠP 1000 MHz, data do 10 Gb/s Ethernet, CATV

### Konektory RJ45

* RJ10 – 4 pozice, 2 osazené (4P2C)
* RJ10 – 4 pozice, 4 osazené (4P4C) – tel. Sluchátko
* RJ11 – 6 pozic, 4 osazené (6P4C) – telefon
* RJ12 – 6 pozic, 6 osazených (6P6C)
* **RJ45 – 8 pozic, 8 osazených (8P8C) – LAN Ethernet**
* RJ48 – 10 pozic, 10 osazených (10P10C) – stejné vnější rozměry a provedení jako RJ45, kamerové a pokladní systémy

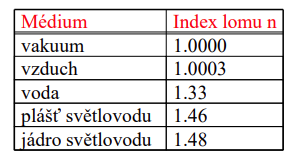
# 8. Strukturovaná kabeláž

### Datové rozvody



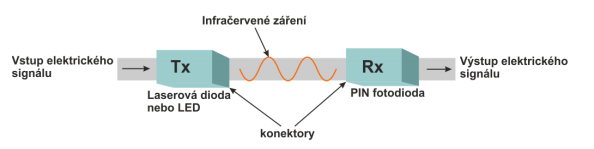
# 9. Optický kabel

### Index lomu

* Data se přenáší pomocí optického vlákna označovaného též jako FO (Fiber Optic)
* Jedno optické vlákno může přenášet data rychlostí až 16 Tb/s
* Index lomu je definován jako podíl rychlosti světla ve vakuu k rychlosti světla v materiálu:
  +  n = c/ v

### Optická trasa

* **Vysílač (Tx)** převádí elektrický signál na světelný a vysílá jej do vlákna (elektrický signál z metalického vedení je třeba upravit na vhodný tvar a průběh pro přenos přes optické vlákno – změna kódování)
* Obsahuje světelný zdroj (laserovou diodu, nebo LED)



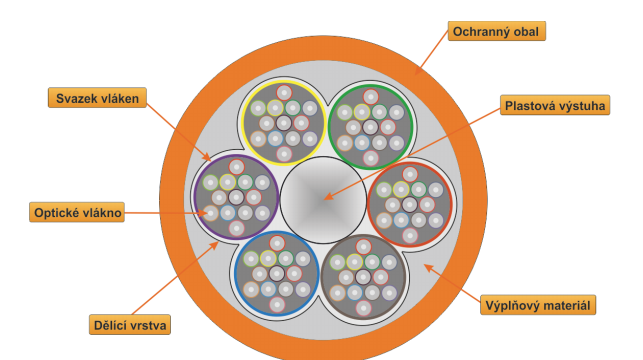
* **Přijímač (Rx)** je složen z:
  + Fotodetektoru – převádí optický signál do elektrického tvaru
  + Zesilovače – zesilují signál a převádí jej do tvaru připraveného pro zpracování
  + Procesoru – reprodukuje původní signál – změna kódování

#### Optické vedení

* Informace se přenáší pomocí optických vláken, která se sdružují do optických kabelů
* Liší se ve svých rozměrech, složení a také vlnových délkách světla, které mohou přenášet
* Vysoká EMS
* Světelný signál podléhá pouze minimálnímu odporu – malý útlum
* Optické kabely mohou být použity pro přenos na velkou vzdálenost – cca 100 km bez nutnosti regenerace signálu
* Informace je možné přenášet rychlostí až 100 Gb/s na jedné vlnové délce
* Vyráběn většinou se sudým počtem vláken pro simplexní provoz na jednotlivých vláknech ( v současnosti je možný i plně duplexní provoz na jednom vlákně)

## Optické vlákno

#### Řez optickým kabelem



### Konstrukce optického vlákna

#### Jádro

* Ze skla, nebo plastu
* Plastová vlákna jsou jednodušší na výrobu, ale je možné je použít pouze na kratší vzdálenosti (podstatně větší útlum)
* Průměr jádra se pohybuje od 2 do několika set mikronů (µm)
* Jádro má v průřezu konstantní, nebo proměnlivou hodnotu indexu lomu

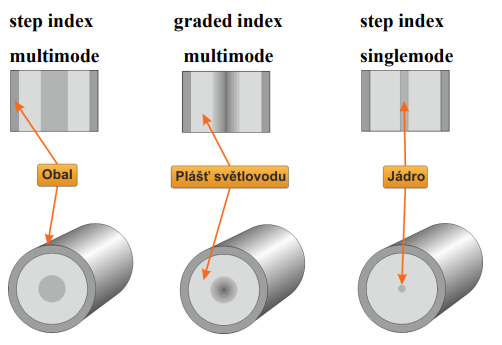
#### Plášť světlovodu

* Ze skla, nebo plastu
* Vyroben jako jedna část společně s jádrem
* Jedná se o ochrannou vrstvu s nižším indexem lomu světla, než má jádro
* Jeho rozměry jsou od 100 µm do 1 mm

#### Obal

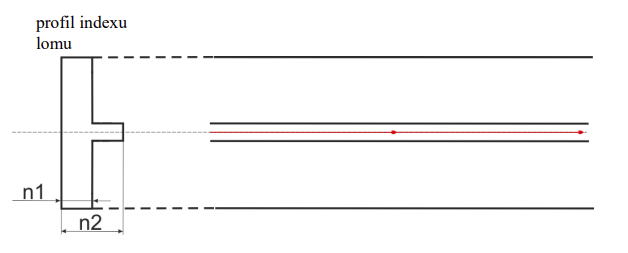
* Vnější ochranné neprůhledné barevné plastové pouzdro, 2 vrstvé, zvyšuje pružnost vlákna

### Typy optických vláken



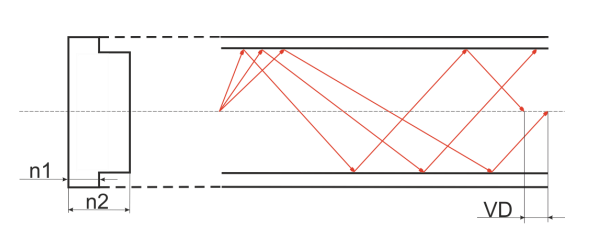
#### Jednovidové (Singlemode) se skokovou změnou indexu lomu

* Jádro je velmi tenké (méně než 10 µm)
* Světlo může v jádru postupovat jen jednou cestou – zdrojem infračerveného záření je laserová dioda, dříve laser
* Má velmi malý útlum, žádnou vidovou disperzi
* Obtížněji se instaluje (vyžaduje větší přesnost)
* Přenosové rychlosti až 100 Gb/s
* V současné době nejčastěji používaný typ optického vlákna vzhledem k vyrovnání ceny s mnohovidovými vlákny



#### Mnohovidové (multimode) vlákno se skokovou a průběžnou změnou indexu lomu – společné vlastnosti

* Mají tlustší jádro než jednovidové vlákno
* Světelný paprsek má více prostoru a může probíhat v jádru více cestami – zdrojem infračerveného záření je LED
* Více vidů (světelných průběhů) v přenosu může vést k rušení signálu na straně přijímače
* Jako veličina tohoto rušení se používá **vidová disperze (VD)**, která se udává v ns/km a představuje rozdíl mezi nejrychlejším a nejpomalejším světelným průběhem
* Nejjednodušší a nejlevnější typ optického vlákna
* Jádro má průměr 50 až 125 µm, plášť světlovodu až 140 µm
* Vhodné pro přenosové rychlosti 200 Mb/s – 3 Gb/s



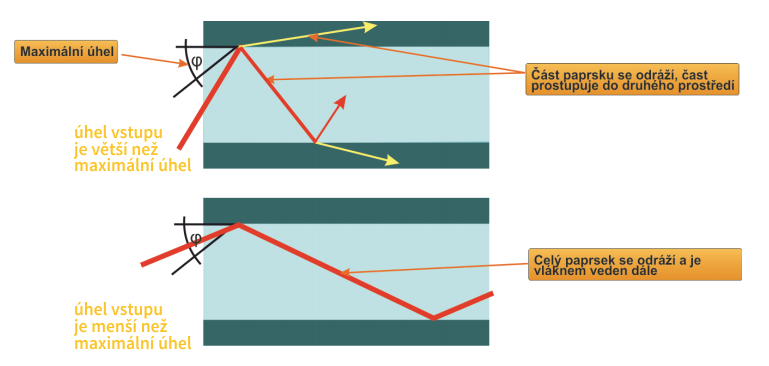
#### Mnohovidové (multimode) s průběžnou změnou indexu lomu

* Vlákno s postupnou změnou indexu lomu, jádro složeno s tisíce tenkých vrstev, které se liší indexem lomu
* Průběžná změna indexu lomu se používá pouze u mnohovidových vláken
* Vede lépe světelný signál než mnohovidové vlákno se skokovou změnou indexu lomu, také má nižší útlum a vidovou disperzi

### Podmínky pro šíření světla optickým vláknem

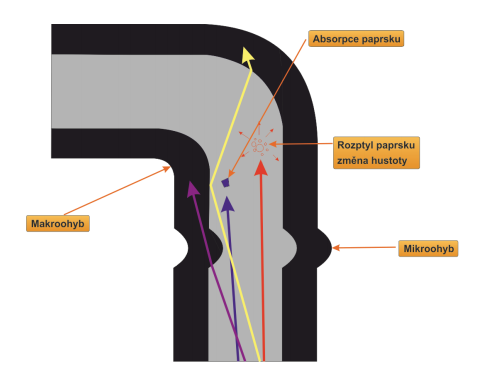
* Je nezbytné, aby při vysílání byla dodržena tzv. numerická apertura (NA) – míra schopnosti vlákna ze svého okolí navázat do svého jádra optický svazek infrazáření z laserové diody nebo LED
* NA je určena maximálním úhlem (ϕ), pod kterým ještě může světelný paprsek vstoupit do světlovodu, aniž by docházelo k neúplným odrazům ve vlákně
* NA = n\*sin(ϕ)
  + Kde n je index lomu materiálu, ze kterého světlo navazuje do vlákna

#### Numerická apertura

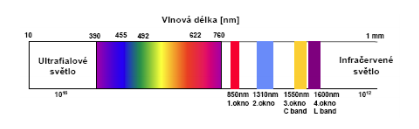


### Útlum na optickém vlákně

* U nejkvalitnějších kabelů (sklo, jednovidový) je asi 0,2 dB/km při 1550 nm, plastové 50 až 100 dB/km
  + **Vnitřní** způsobený nečistotou ve vlákně:
    - Rozptylem – dominantní část vnitřního útlumu
    - Absorbcí
  + **Venkovní** způsobený venkovními mechanismy
    - Macro-ohybem – vzniká nevhodným ohybem kabelu
    - Micro-ohybem – vzniká drobnými nerovnostmi na rozhranní jádro – plášť světlovodu



### Vlnová délka

* Jádro absorbuje záření na různých vlnových délkách odlišně
* U skla se používají vlnové délky v oblasti 3 absorpčních minim:
  + 850 nm
  + 1300 nm
  + 1310 nm
  + 1550 nm
  + 1625 nm
  + (Viditelné spektrum je cca 400 až 800 nm)

### Technologie WDM, WWDM, CWDM, DWDM

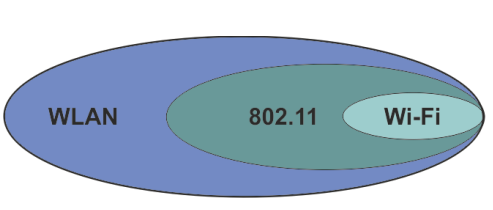
* Wawelength Division Multiplexing, Wide/ Coarse/ Dense)
* Přes optické vlákno přenášíme paralelně více světelných paprsků s odlišnou vlnovou délkou
* Každá nová vlnová délka nese vlastní data
* Jednosměrný, nebo obousměrný přenos jedním vláknem na stejných (nutno použít cirkulátory), nebo odlišných vlnových délkách
* WDM – 2 vlnové délky, WWDM – 4 vlnové délky, CWDM – 8 až 18 vlnových délek, DWDM – v současné době systém nabízí až 160 odlišných vlnových délek na jednom vlákně, každou s přenosovou kapacitou 100 Gb/s, tedy až 16 Tb/s

### Specifikace optických kabelů

* Jsou specifikovány počtem vláken a parametry vláken ve tvaru průměr jádra/ průměr pláště světlovodu:
  + 8/125 nebo 9/125 µm: Jednovidový kabel, vhodný pro vlnové délky 1300, 1310, nebo 1550 nm (infralaserová dioda)
  + 50/125 nebo 62,5/125 µm: Dříve nejpoužívanější konfigurace, vhodný pro 850, 1300, nebo 1310 nm (infra LED)

# 10. Komunikace vzduchem

### WLAN (Wireless LAN)

* Obecné označení pro bezdrátové sítě

### IEEE 802.11 (Insitute of Electrical and Electronics Engineers)

* Pouze jedna z technologií, která může být použita v rámci WLAN
* Dalšími technologiemi jsou např. Bluetooth, HiperLAN, HomeRF
* Technologie IEEE 802.11 jsou dnes používány i mimo WLAN např. v prostředí WirelessMAN, WirelessMAN
* Pro tyto účely nebyly původně určeny
* Nesprávně označovány jako „Bezdrátový Ethernet“

### Wi-Fi (Wireless Fidelity)

* Není to samé jako WLAN, nebo IEEE 802.11
* Wi-Fi je pouze „nálepka“
* Uděluje se produktům, které vyhovují standardům IEEE 802.11 a splňují požadavky na vzájemnou kompatibilitu
* Uděluje je organizace Wi-Fi Alliance

### Licencovaná pásma

* Licencovaná pásma pro datové sítě 3,5, 26 a 28 GHz. Je možné použít i jiná licencovaná pásma 4, 6, 8, 11, 13, 15, 18, 23, 32, 38 a 42 GHz. Většinou pro firemní poslední míli, dvoubodové spoje (Point to point) a páteřní spoje providerů internetu. U licencovaného pásma je nutná platná licence od ČTÚ

### Bezlicenční pásma

#### Pásmo 2,4 GHz

* Primárně určeno pro budování WLAN, které přinášejí uživatelům možnost připojení kdekoliv v objektech a lokalitách s bezdrátovým pokrytím, či dokonce možnost pohybu, bez ztráty připojení do sítě.
* V ČR je toto frekvenční pásmo využívání telekomunikačními operátory i jako alternativní řešení, nejčastěji pro zajištění přístupu jejich zákazníků na internet. Ovšem vzhledem k přetížení tohoto pásma a ke stále většímu vzájemnému rušení jednotlivých přenosů (nelicencovaný charakter pásma), telekomunikační operátoři stále více přechází do pásma 5 GHz a licencovaných pásem 3,5 a 26 GHz

#### Pásmo 5 GHz

* Dříve licencované, později bezlicenční s částečnými omezeními – jen pro použití uvnitř budov (možná kolize s jinými telekomunikačními zařízeními). Dnes část pásma uvolněna i pro venkovní použití

#### Pásmo 10,5 GHz

* Toho pásmo je primárně určeno pro realizaci propojení bod-bod (páteřní spoje rozsáhlejší bezdrátové sítě). Díky relativně vysokým nákladům je vhodná spíše pro vysokorychlostní služby od 2 Mb/s výše

#### Frekvenční pásmo 2,4 GHz (2,4000 – 2,4835)

* Rozděleno do 14-ti částečně se překrývajících kanálů (USA 11 kanálů, Evropa 13 kanálů, Japonsko 14 kanálů) se šířkou 22 MHz, prakticky se používají kanály o šířce 20 MHz
* V Evropě se umožňuje provoz max 3 sítí „vedle sebe“ na nepřekrývajících se kanálech 1, 7 a 13
* Obsazení kanálů lze zjistit pomocí různých SW
* Maximální vyzářený výkon 100 mW (20 dBm)
* Přídavné zesilovače zakázány
* Povolena pouze homologovaná zařízení
* Právo na kanál má ten, kdo přijde první

#### Frekvenční pásmo 5 GHz (5,150 – 5,250; 5,250 – 5,350 a 5,470 – 5,725)

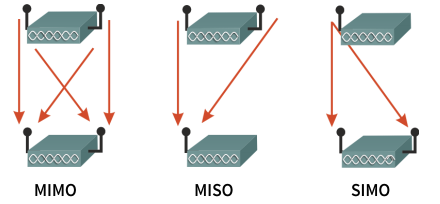
* V Evropě 19 nepřekrývajících se kanálů o šířce 20 MHz, z toho 8 kanálů v prvních dvou subpásmech a 11 kanálů v třetím subpásmu
* 5,250 – 5,350 GHz
  + Omezení na provoz jen uvnitř budov
  + Maximální vyzářený výkon 200 mW EIRP (Equivalent Isotropically Radiated Power) – celkový výkon, který by bylo nutné vyzářit izotropní anténou
* 5,250 – 5,350 GHz
  + Totéž, co v předchozím případě
  + Navíc zařízení musí podporovat automatickou regulaci výstupního výkonu a dynamický výběr frekvencí
* 5,470 – 5,725 GHz
  + Bezlicenční pásmo i mimo budovy
  + Maximální vysílací výkon je zde 1 W, ale musí být vhodně rozložen
  + Maximální střední spektrální hustota EIRP je 50 mW/ MHz v libovolném 1 MHz úseku
  + Ostatní jako v předchozím případě

### Standard IEEE 802.11

* 802.11b (WiFi 1) – max 11 Mb/s, 2,4 GHz
* 802.11a,h (WiFi 2) – max 54 Mb/s, 5 GHz
* 802.11g (WiFi 3) – max 54 Mb/s, 2,4 GHz
* 802.11n (WiFi 4) – max 600 Mb/s, 4 kanály, 2,4 nebo 5 GHz, 20 nebo 40 MHz/ kanál, MIMO
* 802.11ac (WiFi 5) – max 6,77 Gb/s, 8 kanálů, 5 GHz a zpětně kompatibilní s 2,4 GHz
* 802.11ax (WiFi 6) – max 9,6 Gb/s

#### Dosažení vyšší přenosové rychlosti

* MIMO – Multi Input, Multi Output
* MISO – Multi Input, Single Output
* SIMO – Single Input, Multi Output
* SISO – Single Input, Single Output



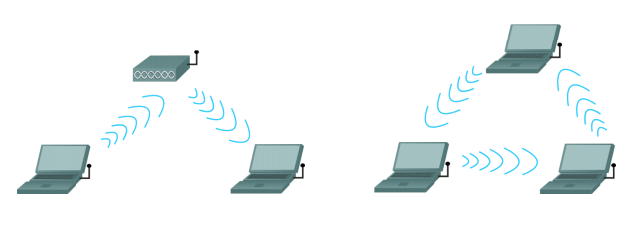
### Bezpečnost

#### Šifrování

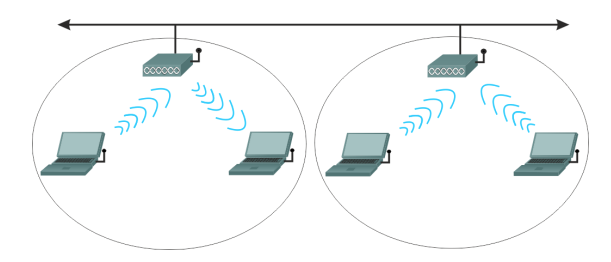
* Implementován šifrovací protokol WEP (Wired Equivalent Privacy)
  + Délka klíče 64, 128, 152 a 256 bitů
  + Nedostatečné – úspěšné útoky
* U novějších zařízení se používá šifrovací protokol WPA (Wi-Fi Protected Access), který používá šifrování TKIP (Temporal Key Integrity Protocol).
* WPA byl upraven do verze WPA2 a TKIP byl nahrazen AES (Advanced Encryption Standard)
  + WPA a WPA2 lze použít jen v sítích s infrastrukturou (nikoli v sítích ad-hoc)

### Architektura

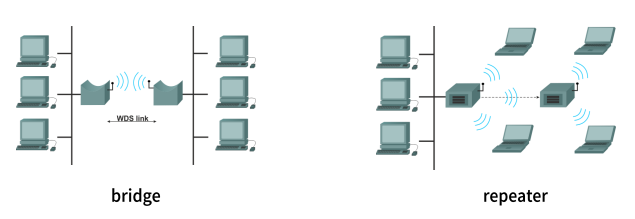
#### Dvoubodový spoj v režimu infrastruktura a Peer to Peer



#### WDS (Wireless Distribution System)



#### WDS – bezdrátové bridge a repeatery



### Mikrovlnné spoje

#### „Poslední míle“

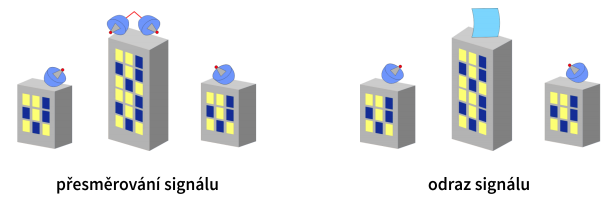
* Připojení sítě, nebo PC do internetu
* Všesměrové antény (tyčové), nebo široce směrové antény (segmentové, panelové) u providera
* Úzce směrové antény (parabolické, yagi) u uživatele
* Radiový modem – převod mezi radio signálem a LAN
* Nutná přímá viditelnost mezi anténami, nebo retranslace
* Všechna dříve uvedená frekvenční pásma
* Maximální dosažitelné vzdálenosti kolem 10 km
* K těmto účelům nebyly bezdrátové sítě IEEE 802.11 původně určeny

#### Propojení dvou vzdálených sítí nebo PC

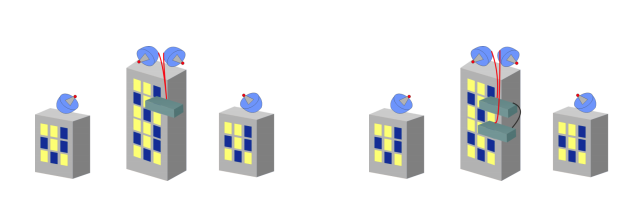
* Většinou propojení dvou vzdálených sítí jedné firmy
* Úzce směrové antény na obou stranách spoje
* Jinak platí totéž jako u „poslední míle“

#### Pasivní retranslace

* Přesměrováním signálu
* Odrazem signálu



#### Aktivní retranslace

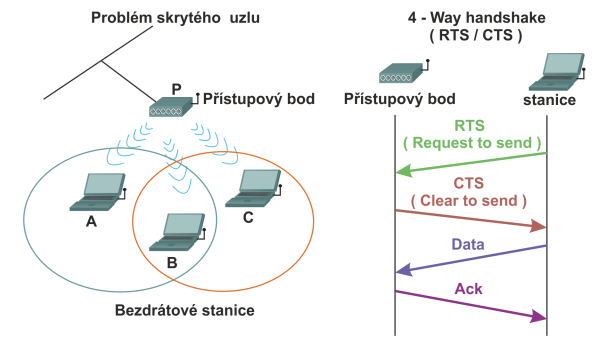
* AP – s jedním centrálním prvkem
* AP – se dvěma aktivními prvky

### Zisk antén

* Udáván v dB
* dBd, d – dipól a udává nám kolikrát silnější signál je anténa schopna získat ve srovnání s referenční anténou – reálným půl vlnným dipólem
* dBi, i – izotropní dipól (zářič), tento zisk je o 2,15 dB větší než v předcházejícím případě, neboť referenční anténou je izotropní dipól – všesměrový zářič vysílající z jednoho bodu – matematická abstrakce, nelze reálně vyrobit

### Problém skrytého uzlu

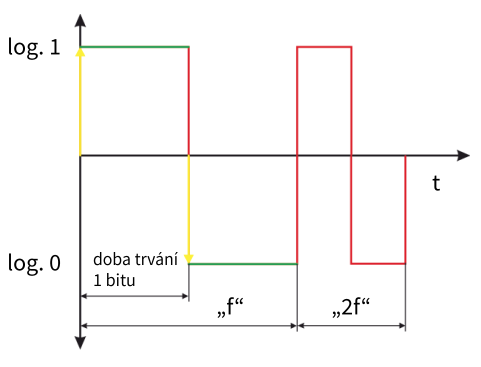
* Dvě stanice, které na sebe nedosáhnou, mohou tím pádem zahájit současně vysílání v domnění, že je komunikační kanál volný
* Řešení – CSMA/CA je rozšířena o řídící rámce RTS/CTS (Request To Send/Clear To Send), pomocí kterých přiděluje AP komunikační kanál stanicím. Součástí těchto řídících požadavků je i předpokládaná doba vysílání.

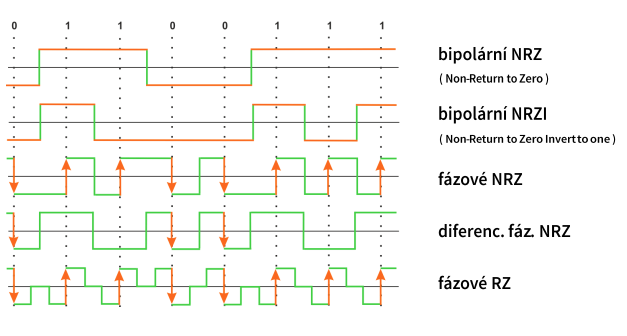


# 11. Přenos signálu

### Přenos signálu v základním pásmu (Baseband)

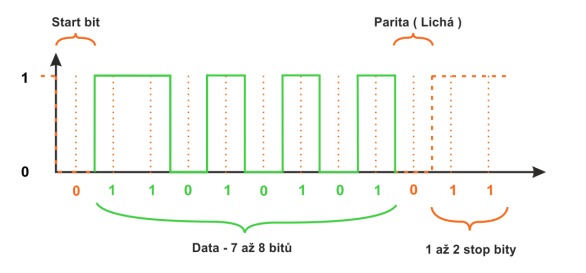
* Nemodulovaný přenos
* Signál kódujeme
* Přes komunikační kanál můžeme přenést jen jeden signál
* Signál by měl zabírat co nejmenší kmitočtové spektrum
* Neměl by mít stejnosměrnou složku
* Měl by umožňovat fázovou synchronizaci přijímající strany na vysílaný signál
* Teoreticky je možné přenést binární signál o rychlosti n vzorků (bitů) za sekundu v kmitočtovém pásmu n/2 Hz – doba trvání bitů = T/2.
* Prakticky přeneseme n vzorků (bitů) za sekundu v kmitočtovém pásmu 1\*n Hz – potřebujeme v rámci hodinového signálu vygenerovat např. pomocné hrany
* Vyhodnocovat u digitálního signálu můžeme:
  + Úrovně – amplitudu (na obrázku zeleně)
  + Počet změn úrovně signálu po dobu trváni bitu – frekvenci nebo dobu periody (na obrázku červeně)
  + Hrany (vzestupně a sestupně) – fázi (na obrázku žlutě)





#### Příklady kódování

* Bipolární NRZ (Non-return to Zero) – sériový přenos PC COMx
  + Log. 0 = +U (+3 až +15 V)
  + Log. 1 = -U (-3 až -15 V)
* NRZI (NRZ Invert to One) – LAN internet
  + 100 Mb/s optické spoje
  + Log. 0 = zůstává napěťová úroveň předcházejícího bitu
  + Log. 1 = mění se napěťová úroveň na opačnou
* Fázové NRZ (Manchester) – LAN Ethernet 10 Mb/s
  + Log. 0 = sestupná hrana
  + Log. 1 = vzestupná hrana
* Diferenciální fázové NRZ (dif. Manchester) – LAN Token Ring
  + Log. 0 = sestupná, nebo vzestupná hrana
  + Log. 1 = beze změny úrovně (uprostřed intervalů jsou synchronizační hrany)
* Fázové RZ – LAN Arcnet
  + Každá logická úroveň je vyjádřena sledem dvou opačných pulsů s mezerou



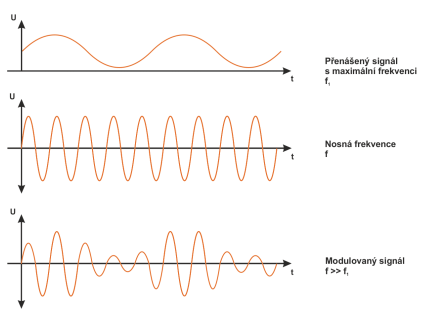
#### Zkreslení signálu přenosovým kanálem



### Přenos kanálu v přeloženém pásmu (Broadband)

* Modulovaný přenos – modulujeme nosnou frekvenci
* Přes komunikační kanál můžeme přenášet více signálů ( s dostatečným odstupem nosných frekvencí)
* Přenášený signál můžeme modulovat:
  + Amplitudovou modulací
  + Frekvenční modulací
  + Fázovou modulací
* Např. průmyslová síť MAP (Manufacturing Automation Protocol) a optické spoje

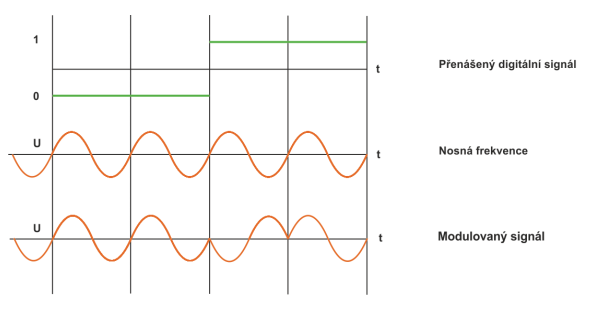
#### Amplitudová modulace



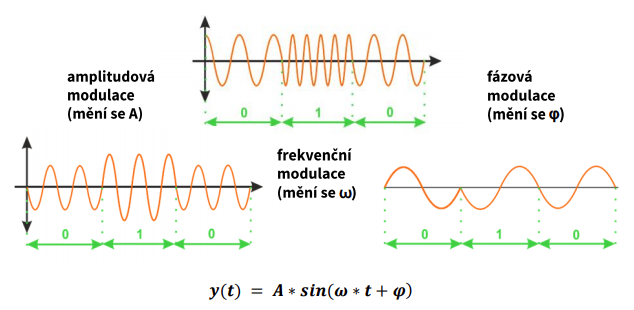
#### Frekvenční modulace



#### Fázová modulace



#### Souhrnný přehled modulací



# 12. Topologie sítí

#### Fyzická topologie

* Je dána zapojením kabelů, způsoben propojení jednotlivých uzlů a způsobem šíření signálu

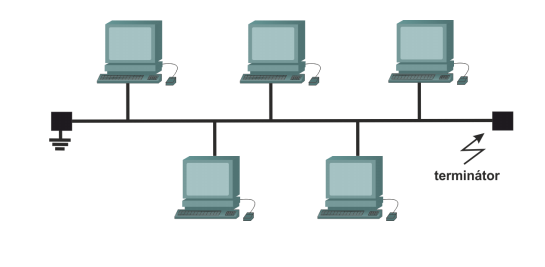
#### Logická topologie

* Je dána způsobem vzájemné komunikace (předáváním dat např. pešek) mezi jednotlivými uzly
* Nemusí být shodná s fyzickou topologií

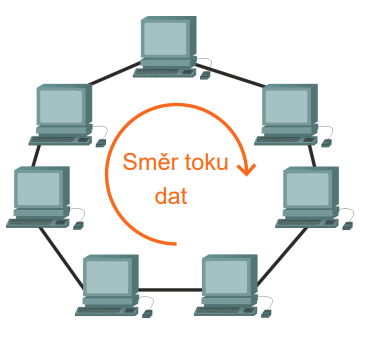
### Fyzické topologie

#### Fyzická topologie Sběrnice

* Všechny uzly jsou připojeny na jedno společné médium – sběrnici
* Každý uzel má přímý přístup ke sběrnici (tzn. nikoliv přes jiný uzel)
* Připojení uzlů je realizováno pomocí odboček, což umožňuje snadné připojování uzlů k síti, nebo naopak jejich odpojování, aniž by byla ovlivněna správná činnost sběrnice
* Zpráva vyslaná z uzlu se šíří ke všem ostatním uzlům na sběrnici
* Neobsahuje aktivní prvky

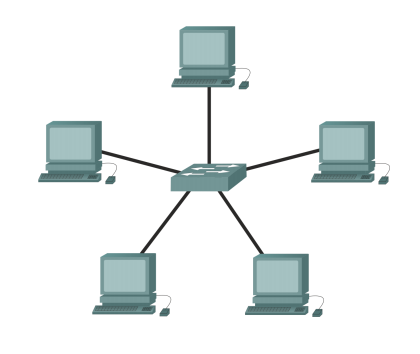


#### Fyzická topologie Kruh

* Každý uzel je propojen přímo s následujícím a s předchozím uzlem
* Kabelové linky jsou většinou uspořádány tak, že po jedné lince uzel signál posílá a po druhé přijímá
* Data se tímto způsobem pohybují v kruhu od odesílatele postupně přes všechny následníky až k příjemci
* Každý uzel je připojen k síti aktivně – přijatá data určená jinému převezme a pošle dál. Při tom rovněž dochází k elektrické i logické regeneraci signálu
* Na rozdíl od sběrnicové topologie (s obousměrným šířením signálu), existuje v kruhové síti řízený jednosměrný tok dat
* Neobsahuje aktivní prvky

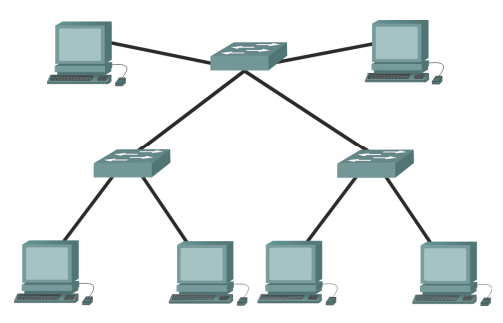
#### Fyzická topologie Hvězda

* Středem sítě je centrální uzel, stanice, nebo servery jsou k němu paralelně připojeny
* Veškerá komunikace pak probíhá přes tento centrální uzel
* Centrálním uzlem je switch, nebo hub
* Je-li uprostřed propojovacím uzlem hub, je signál vysílaný kterýmkoliv počítačem šířen po celé síti jako u sběrnice
* Je-li centrálním propojovacím uzlem switch, je signál většinou šířen jen k cílovému uzlu
* Výpadek stanice ani kabelu neohrozí funkci zbytku sítě
* Vypadne-li centrální uzel, havaruje celá síť
* Jedná se o nejstarší topologii počítačových sítí (používala se pro propojování terminálů k sálovému počítači, nebo minipočítači – nešlo ale o počítačovou síť)
* Typickým příkladem je jednoduchá síť Ethernet s kroucenou dvojlinkou



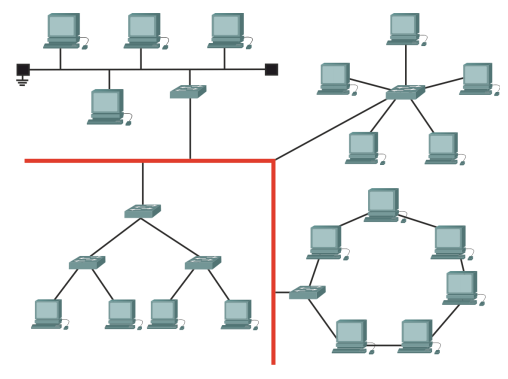
#### Fyzická topologie Strom

* Na pozici kořene a propojovacích uzlů stromu je switch, nebo hub
* Komunikace není vždy vedena přes kořen, i když v případě hubů se šíří signál po celém stromu
* Pokud dojde k havárii kořene, síť se rozpadne na několik sítí, stanice a servery připojené přímo na kořen jsou odpojeny od zbytku sítě
* Výpadek propojovacího uzlu způsobí výpadek části sítě
* Typickým příkladem je síť Ethernet s kroucenou dvojlinkou



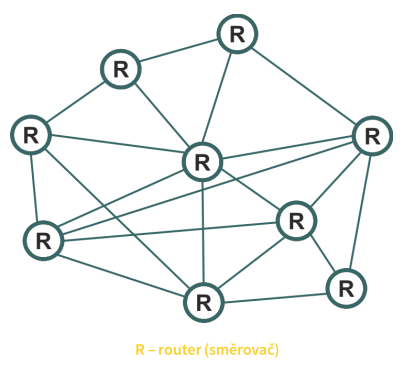
#### Fyzická topologie Backbone

* Jako páteř používaná síť s vysokou rychlostí přenosu, na níž jsou připojeny jednotlivé LAN, CAN a MAN (s libovolnou topologií)
* Nasazována zejména ve WAN sítích
* Spojuje jednotlivé sítě LAN, CAN a MAN navzájem
* Pokud probíhá komunikace uvnitř některé LAN, CAN a MAN, neprobíhá komunikace přes páteř
* Páteřní síť se dostane ke slovu až v okamžiku, kdy je nutné uskutečnit datový přenos z jedné sítě LAN, CAN a MAN do druhé
* Typickým příkladem je páteřní síť CESNET2 (Czech Education and Scientific Network) v ČR



#### Neomezená fyzická topologie

* V rámci této topologie mohou být použity všechny doposud probrané fyzické topologie
* Využívaná zejména ve WAN sítích v rámci internetu
* Často jsou využívána redundantní spojení (záloha, rozložení zatížení, zvýšení přípojné kapacity…)
* Typickým příkladem je síť CESNET v ČR



### Logické topologie

#### Dvojbodový spoj

* Data (ne signál) jsou zasílána jen mezi dvěma uzly

#### Sběrnice

* Data jsou zasílána všem uzlům
* Jednotlivé uzly obdrží data v přibližně stejné okamžiky

#### Kruh

* Data jsou zasílána sekvenčně, podle předem daného pořadí z uzlu na uzel bez ohledu na fyzickou topologii

# 13. Principy přístupových metod

### Statické přidělování FDMA a TDMA

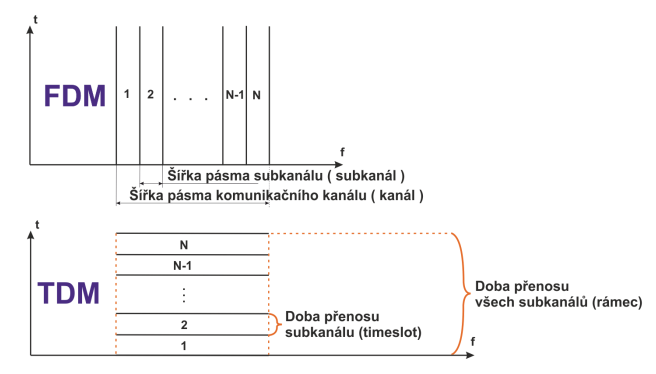
* Kapacita přenosového spoje je pevně rozdělena do částí přidělených k použití jednotlivým účastníkům:

#### Frekvenční multiplex FDM (Frequency Division Multiplex)

* FDMA (Freq. Div. Multiple Access) rozdělí celkovou kmitočtovou šíři kanálu do několika částí přidělených jednotlivým stanicím

#### Časový multiplex TDM (Time Division Multiplex)

* TDMA (TD Multiple Access) rozděluje sdílenou přenosovou kapacitu na posloupnost časových úseků, z nichž každý je plně přidělen jen jedné stanici
* FDMA i TDMA využívají např. mobilní GSM sítě



### Centrální přidělování

* Centrální stanice je pověřena úkolem přidělovat kapacitu kanálu těm podřízeným stanicím, které ji skutečně potřebují:

#### Na žádost

* každá stanice má pro sebe vyhrazenou malou část přenosové kapacity kanálu, po které může kdykoliv žádat centrální stanici o přidělení volného přenosového kanálu, po potvrzení od centrální stanice pak zahájí přenos dat, uvolnění kanálu oznámí opět centrální stanici. Tuto metodu využívají např. družicové spoje Comsat a Intelsat

#### Na výzvu

* centrální stanice se periodicky dotazuje všech podřízených stanic, zda nemají připravena data k vysílání, pokud ano, dotazovaná stanice je ihned odešle, jinak odpoví centrální stanici pouze potvrzovacím paketem, nebo neodpoví vůbec. Součást standardů bitově orientovaných protokolů SDLC (Synchronous Data Link Control) a HDLC (High-level Data Link Control)

### Náhodný přístup

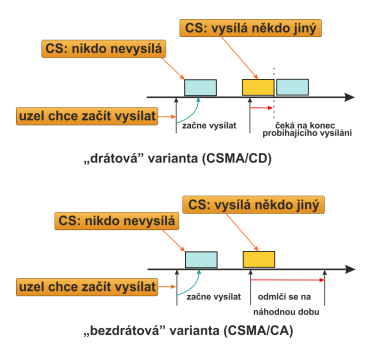
* Využívá se náhodný přístup, není třeba žádné centrální stanice

#### Metody ALOHA

* každá stanice, která má data k vysílání, je odešle bez ohledu na současný stav společného komunikačního kanálu. Propustnost je přibližně 18%, při zahájení vysílání jen na začátcích určitých časových úseků se propustnost zvýší na 36% - tzv. taktovaný ALOHA. Tuto metodu používají některé radiové sítě

#### Příposlech nosné CSMA (Carrier Sense Multiple Access)

* posloucháme co se děje na společném komunikačním kanálu, když je kanál volný, zahájíme vysílání dat. Problém je se vzdálenými stanicemi, které mohou zahájit vysílání současně, v domnění, že je komunikační kanál volný. Dvě základní metody:
  + **CD (Collission Detection)** – např. Ethernet na metalickém vedení
  + **CA (Collission Avoidance)** – např. bezdrátové sítě IEEE 802.11



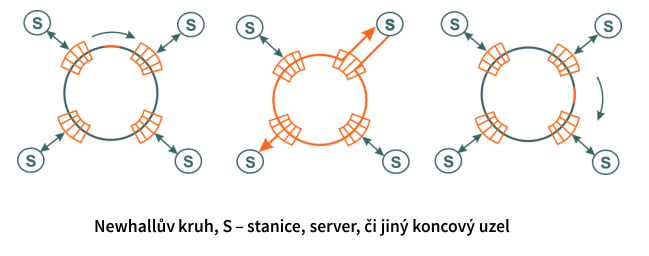
#### CSMA/CD

* je-li po stanovenou dobu kanál volný, zahájí stanice vysílání. Po detekci nosné stanice čeká až právě vysílající stanice odvysílá data (prakticky nosnou stanici testuje periodicky s pevně stanovenou délkou intervalu) a pak zahájí bezprostředně po uplynutí mezirámcové mezery vysílání – Ethernet.
* Během vysílání porovnává vysílaná data s daty na komunikačním kanále. V případě detekce kolize vyšle kolizní posloupnost – „jam“ k urychlení reakce sítě na kolizi. Po obdržení jamu se stanice odmlčí na náhodně stanovenou dobu. Odmlčí se stejně i stanice, která vyslala „jam“

### Distribuované přidělování

#### Newhallův kruh (fyzický kruh)

* Posuvný registr nemusí mít velikost rámce
* V síti vždy jen jeden rámec
* V kruhu koluje pešek (rámec token), nebo datový rámec
* Stanice, která má připravena data k vyslání po obdržení peška změní příznak peška na data, rozpojí kruh a zahájí vysílání datového rámce. Stanice, které je datový rámec určen přečte a potvrdí, vysílající stanice odejme datový rámec z kruhu, spojí kruh, vygeneruje a vyšle peška svému následovníkovi v kruhu

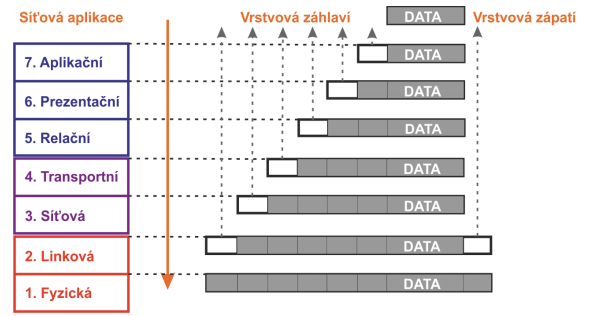


# 14. Normování počítačových sítí

### Model OSI

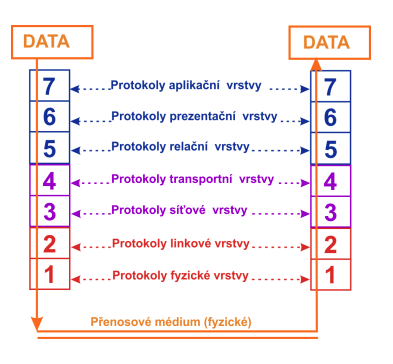
#### Referenční model ISO/ OSI (International Standards Organization/ Open System Interconnection)

* Vývoj zahájen 1977 a 1984 přijat organizací ISO ve formě mezinárodní normy ISO 7498
* Rozděluje počítačovou sít do sedmi vrstev
* Každá vrstva má přidělenou činnost
* Každá vrstva má dvě rozhraní pro vertikální komunikaci – služby poskytované vyšší vrstvě a služby poskytované do nižší vrstvy
* V každém rozhranní jsou definovány vstupní body SAP (Service Access Point) – umožňují paralelní poskytování nezávislých služeb několika síťovým procesům současně

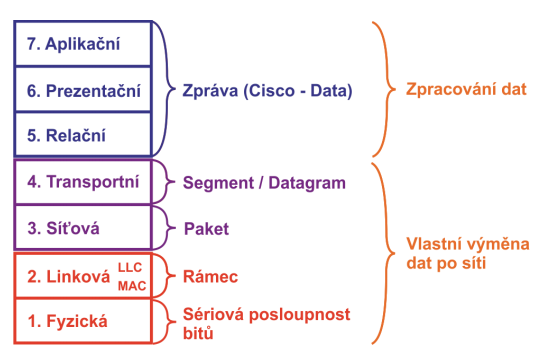


* Každé vrstvě OSI je přiřazena sada protokolů, které plní její funkce. Tyto protokoly komunikují se stejnými protokoly protilehlého systému – tzv. horizontální komunikace, pomocí vrstvových záhlaví a zápatí datových celků PDU (Protocol Data Unit)

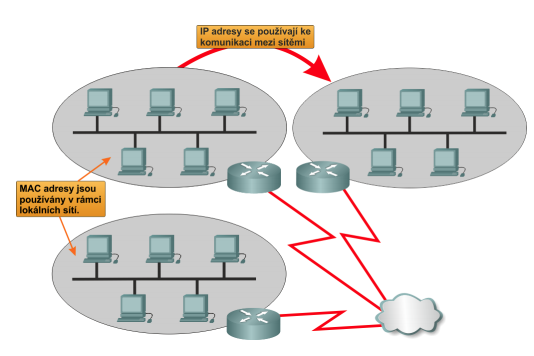
#### Horizontální komunikace



#### PDU (Protocol Data Unit)

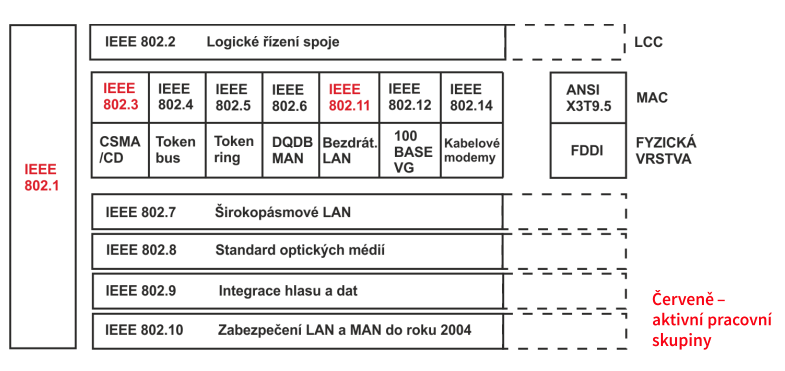


#### Vrstvy

* 1) Fyzická vrstva
  + Přenáší zakódovanou, nebo modulovanou posloupnost bitů mezi dvěma přímými sousedy komunikačním médiem v LAN s 1. vrstvou OSI, např. PC – PC, PC – HUB, PC – Switch…
  + Zabývá se elektrickými a mechanickými vlastnostmi přenosového média
  + Definuje přenosové médium, druhy konektorů, kódování, modulaci a úrovně signálu
  + Je implementována HW – NIC (Network Interface Controller)
* 2) Linková vrstva
  + Pracuje s MAC (Media Access Control) adresami – fyzickými adresami
  + Poskytuje spojení mezi dvěma koncovými uzly v rámci jedné LAN
  + Zajišťuje přepravu rámců mezi dvěma přímými sousedy v LAN s 2. vrstvou OSI, např. PC – PC, PC- Switch, Switch – Switch …
  + Převádí pakety na rámec a naopak
  + Převádí rámce na sériovou posloupnost bitů a naopak
  + Hodní podvrstva LLC (Logical Link Control) – je nezávislá na použitém typu média a použitých přístupových metodách. Je implementována SW použitým síťovým protokolem TCP/IP (Transmission Control Protocol/ Internet Protocol), IPX/SPX (Internet Packet Exchange/ Sequenced Packed Exchange)
  + Dolní podvrstva MAC pracuje s MAC adresami, je implementována HW – NIC a SW ovladačem NIC
  + Může zabezpečovat potvrzování dat
* 3) Síťová vrstva
  + Pracuje s adresami konkrétního síťového protokolu – logickými adresami
  + Poskytuje spojení mezi koncovými uzly, nacházejí se v různých LAN (mezi nimi je router)
  + Zajišťuje přepravu paketů mezi dvěma přímými sousedy v LAN s 3. vrstvou OSI např. PC – PC, PC – router atd
  + Stará se o směrování v síti a síťové adresování
  + Řeší výběr nejvhodnější cesty
  + Vytváří pakety ze segmentů nebo datagramů
  + Je realizována datagramovou službou (IP protokol z rodiny protokolů TCP/IP) nebo virtuálním spojem
* 4) Transportní vrstva
  + Pracuje s porty
  + Provozuje transportní spoje, které zajišťují potvrzovanou výměnu mezi dvěma koncovými uzly, nebo nepotvrzovanou nespojovanou datagramovou službu
  + Rozkládá zprávy na úseky o stejné délce a naopak
  + Vytváří z těchto úseků segmenty nebo datagramy
* 5) Relační vrstva
  + Zabývá se povolením přístupu uživatele k aplikačním programům
  + Ověřuje přístupová práva, eviduje provoz na síti
  + Vytváří relace (časový úsek, v němž probíhá aktivita uživatele), běžně 1 relace = 1 transportní spoj
* 6) Prezentační vrstva
  + Transformuje data do tvaru, které používají síťové aplikace, např. video a obrázky
  + Zajišťuje převod znakových kódů a datových struktur
  + Stanovuje formáty souborů jako např. MPEG, GIF, JPG a PNG
  + Zajišťuje kompresi a dekompresi zpráv a utajování informací
  + U rodiny protokolů TCP/IP není reprezentována žádným protokolem
* 7) Aplikační vrstva
  + Poskytuje síťovým aplikacím přístup ke komunikačnímu síťovému systému a umožňuje tak jejich spolupráci
  + Obsahuje části síťové aplikace vyžadující standardizaci (např. program FTP (File Transfer Protocol) klient se obrací na FTP protokol z aplikační vrstvy)

### Standardy IEEE 802 (Insitute of Electrical and Electronics Engineers)

* Pro počítačové sítě má největší význam standardizační orgán, založený v rámci IEEE v únoru 1980 (a proto označovaný IEEE 802), který je specificky zaměřen na problematiku standardů LAN
* IEEE 802 si pak vytvořil pracovní skupiny pro jednotlivé oblasti, které do této problematiky spadají, např. pracovní skupinu IEEE 802.3



#### 802.1

* 802 architektura LAN/ MAN
* Propojení mezi 802 LAN, MAN a WAN sítěmi
* Zabezpečení linkové vrstvy
* Celková správa sítě
* Protokoly ve vrstvách nad vrstvami MAC a LLC

#### 802.2

* Logické řízení spoje – podvrstva LLC linkové vrstvy

#### 802.3

* LAN s přístupovou metodou CSMA/CD
* Využívá síť Ethernet (více u LAN Ethernet)

#### 802.4

* LAN s přístupovou metodou Token Bus
* Toto doporučení využívá např. průmyslová síť MAP
* LAN Arcnet používala typ kódování a jiný typ rámce

#### 802.5

* LAN s přístupovou metodou Token Ring
* Tomuto doporučení odpovídá LAN IBM Token Ring

#### 802.6

* Sítě typu MAN DQDB (Distributed Queue Dual Bus)

#### 802.7

* LAN s přenosem v přeloženém pásmu (širokopásmové sítě)

#### 802.11

* Bezdrátové sítě

#### 802.15

* **Bluetooth** – sítě Peer to Peer, bezdrátové propojení dvou zařízení do maximální vzdálenosti cca
  + 100 m – Class 1, 20 dBm (100 mW)
  + 10 m – Class 2, 4 dBm (2,5 mW)
  + 1 m – Class 3, 0 dBm (1 mW)

#### 802.16

* Bezdrátovou síť WiMax (Worldwide Interoperabillity for MIcrowave Access) s technologií BWA (Broadband Wireless Access) a zabudovaným QoS (Quality of Service)

#### ANSI X3T9.5/ FDDI

* FDDI (Fiber distributed data interface) síť s kruhovou topologií. Byla to první síť s přenosovou rychlostí 100 Mb/s a byla původně navržena pro sítě MAN. Vyvinuta v 80. letech intitutem ANSI (Americal National Standards Institution). Síti bylo přiřazeno mezinárodní označení ISO 9314

# 15. Datagramová služba a virtuální spoj

### Datagramová služba

* 3. vrstva modelu OSI, např. protokol IP z rodiny protokolů TCP/IP
  + Není navazováno spojení, posíláme jen datagramy.
  + Datagram je paket, který má ve vrstvovém záhlaví mimo jiných servisních informací cílovou a zdrojovou adresu použitého síťového protokolu. Tím pádem je každý datagram schopen samostatného pohybu po síti
  + Data mohou být potvrzována
  + **Výhody**
    - Síť nezatěžujeme servisními pakety
    - Pakety mohou být dynamicky směrovány méně zatíženými cestami
  + **Nevýhody**
    - Každý datagram může cestovat k cíli jinou cestou a tím pádem mohou dorazit v nesprávném pořadí

### Virtuální spoj

* 3. vrstva modelu OSI
  + Posíláme pakety, které mají ve vrstvovém záhlaví mimo jiných servisních informací identifikátor virtuálního spoje, nikoliv adresy jako v případě datagramové služby
  + Před zahájením spojení je vyslán servisní paket, který zanechá stopu na každém přepojovacím uzlu (routeru), cílová stanice potvrdí spojení a všechny následné pakety projdou stejnou cestou
  + Není implementován v rodině protokolů TCP/IP
  + Na konec je vyslán servisní paket, který vytyčenou cestu na přepojovacích uzlech zruší
  + Data mohou být potvrzována
  + **Výhody**
    - Data jsou doručena ve správném pořadí
  + **Nevýhody**
    - Zatěžování sítě servisními pakety
    - Nemožnost dynamického směrování jednotlivých paketů méně zatíženými cestami

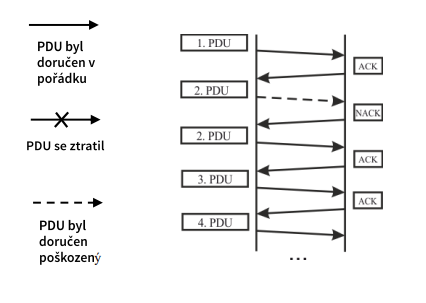
# 16. Potvrzování PDU (Protocol Data Unit)

### Typy potvrzování

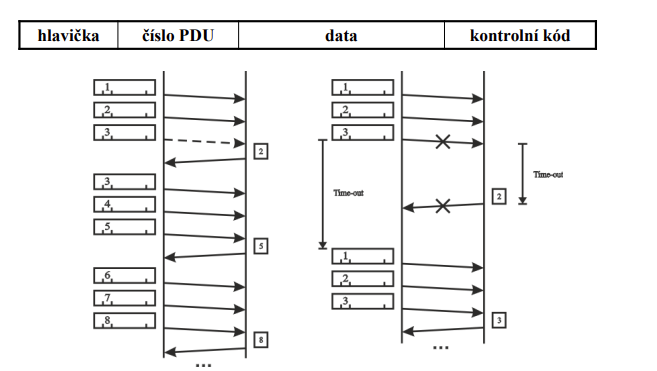
* Potvrzování je nutné pro zaručeně bezchybný přenos informací
* Potvrzovat můžeme rámce, pakety, nebo segmenty
* PDU jsou v hlavičkách cyklicky číslovány např. 0 až 127
* Základní typy potvrzování PDU:
  + **Samostatné potvrzování**
    - Pozitivní potvrzování – PDU nemusí být vyčíslovány, pokud vyřešíme zdvojení paketů
    - Negativní potvrzování – prakticky se používá jen v kombinaci s pozitivním potvrzováním
    - Skupinové (okénkové) potvrzování
  + **Nesamostatné potvrzování**

#### Pozitivní potvrzování

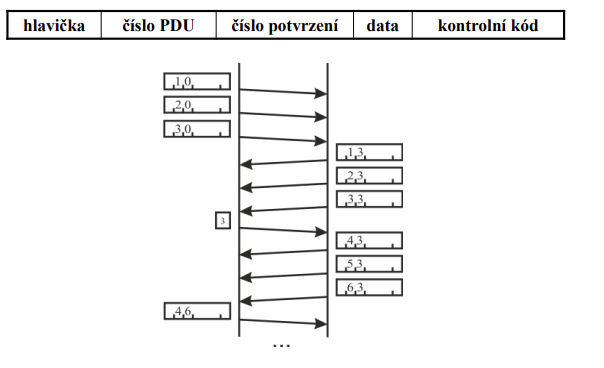
#### Pozitivní potvrzování – negativní



#### Skupinové potvrzování

* Okénko = 3

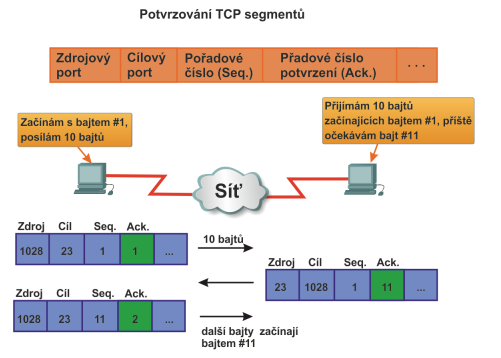
#### Nesamostatné potvrzování

* Okénko = 3

### Potvrzování v praxi – protokol TCP/IP

#### Transportní vrstva, protokol TCP

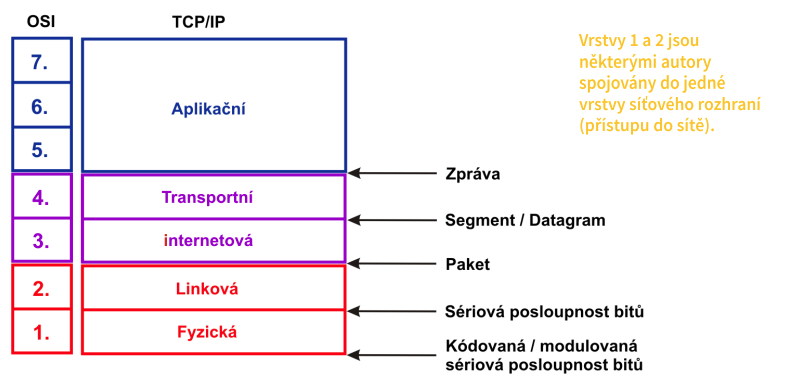
* Potvrzujeme segmenty v rámci transportního spoje
* Pořadovým číslem segmentu je pořadové číslo prvního byte dat v segmentu v rámci číslování byte ve zprávě
* V potvrzení je pořadové číslo byte ze zprávy, které se od odesílatele očekává, tedy pořadové číslo naposled správně přijatého byte + 1
* Využívá se metoda okénka, při výskytu chyb se hodnota okénka zmenšuje až na 1
* Samostatný potvrzovací segment má pořadové číslo segmentu stejné jako očekávaný datový segment. Pro počítadla jako by přenášel 1 B dat



# 17. Síťové protokoly

### TCP/IP

* TCP/IP vytvořen 1970 DARPA (Defense Advanced Research Projects Agency)
* Je také někdy označován jako Internet Reference Model, DoD (Department of Defense) Model nebo ARPANET Reference Model
* Pokrývá SW 2. až 7. vrstvu modelu OSI, u 2. vrstvy jen podrvrstvu LLC
* Někteří autoři přesouvají část protokolů TCP/IP z 3. na 2. vrstvu modelu OSI



### Protokoly TCP/IP v modelu TCP/IP

#### Internetová vrstva

* **ARP** – k IP adrese získá MAC adresu síťového rozhraní, dvojice IP a MAC adresy se uchovají v ARP cache
* **RARP** – opak ARP (MAC -> IP), slouží ke zjištění své IP adresy, na základně znalosti vlastní MAC adresy. Postupně nahrazen protokolem BootP a později protokolem DHCP
* **IP** – datagramová nespojovaná, nepotvrzovaná služba
* **ICMP** – umožňuje routerům posílat chybové a řídící zprávy ostatním routerům i počítačům, je součástí IP
* **IGMP** – umožňuje skupinové adresování počítačů na úrovni internetové vrstvy, je součástí IP
* **BootP** – získání vlastní IP adresy a dalších informací na základě znalosti vlastní MAC adresy
* **DHCP** – totéž i dynamicky
* **RIP** – interní směrovací protokol routerů, algoritmus DVA (Distance Vector Algoritmus)
* **OSPF** – totéž, algoritmus LSA (Link State Algoritmus)
* **BGP** – externí směrovací protokol routerů mezi autonomními systémy, algoritmus Path Vector
* **MTU (Maximum Transmit Unit)** – maximální délka paketu, kterou je schopen komunikační kanál přenést. V případě, že je paket delší, je rozdělen na menší části – fragmenty. Tyto fragmenty spojuje až koncový uzel. U Ethernetu typicky 1500 B, což je maximální velikost paketu, který se vejde do Ethernetového rámce (46 až 1500 B)
* **TTL (Time To Live)** – nastavuje odesílací uzel. Na každém routeru se hodnota sníží o 1, při dosažení 0 se paket zahodí a odešle ICMP chybovou zpráva odesílateli. Na těchto chybových zprávách je založen příkaz Traceroute

#### Transportní vrstva

* **TCP** – spojovaná, potvrzovaná služba, vytváří transportní spoje
* **UDP** – Datagramová nespojovaná, nepotvrzovaná služba

#### Aplikační vrstva

* **SMTP** – odesílání elektronické pošty
* **POP3** – příjem elektronické pošty
* **FTP** – přenos vzdálených souborů
* **TFTP** – jednoduchý protokol pro přenos souborů, zavádění OS do bezdiskových stanic ze serveru, zálohování konfigurací aktivních prvků
* **HTTP** – přenos hypertextových stránek WWW v nešifrované formě
* **HTTPS** – přenos hypertextových stránek WWW v šifrované formě (šifrování protokoly SSL, nebo TLS)
* **Telnet** – síťový virtuální terminál
* **DNS** – převod doménových jmen na IP adresy a naopak
* **SNMP** – vzdálená správa síťových prostředků
* **NTP** – robustní synchronizace času mezi několika počítači
* **LDAP** – přístup k datům na adresářovém serveru, např. ověřování stejných logovacích informací na více zařízení

### Protokoly TCP/IP v modelu OSI

#### Síťová vrstva

* **ARP/RARP** – Address Resolution Protocol/ Reverse ARP
* **DHCP** – Dynamic Host Configuration Protocol
* **DVMRP** – Distance Vector Multicast Routing Protocol
* **ICMP/ICMPv6** – Internet Control Message Protocol
* **IGMP** – Internet Group Management Protocol
* **IPv4** – Internet Protocol version 4
* **IPv6** – Internet Protocol version 6
* **MARS** – Multicast Address Resolution Server
* **PIM** – Protocol Independent Multicast-Sparse Mode
* **RSVP** – Resource ReSerVation Protocol
* **VRRP** – Virtual Router Redundancy Protocol

#### Transportní vrstva

* **Mobile IP**
* **RUDP** – Reliable UDP
* **TALI** – Transport Adapter Layer Interface
* **TCP** – Transmission Control Protocol
* **UDP** – User Datagram Protocol
* **Van Jacobson** – Compressed TCP
* **XOT** – X.25 over TCP

#### Relační vrstva

* **BGMP** – Border Gateway Multicast Protocol
* **DIS** – Distributed Interactice Simulation
* **DNS** – Domain Service Name
* **ISAKMP/IKE** – Internet Security Association and Key Management Protocol and Internet Key Exchange Protocol
* **SCSI** – Small Computer Systems Interface
* **LDAP** – Lightweight Directory Access Protocol
* **MZAP** – Multicast-Scope Zone Announcement Protocol
* **NetBIOS/IP**

#### Aplikační vrstva

* **COPS** – Common Open Policy Service
* **FANP** – Flow Attribute Notification Protocol
* **Finger** – User Information Protocol
* **FTP** – File Transfer Protocol
* **HTTP** – Hypertext Transfer Protocol
* **IMAP4** – Internet Message Access Protocol rev 4
* **IMPPpre/IMPPmes** – Instant Messaging and Presence Protocols
* **IPDC** – IP Device Control
* **IRC** – Internet Relay Chat Protocol
* **ISAKMP** – Internet Message Access Protocol
* **SSH** – Secure Shell
* **NTP** – Network Time Protocol
* **POP3** – Post Office Protocol rev 3
* **Radius** – Remote Authentification Dial In User Service
* **RLOGIN** – Remote Login
* **RTSP** – Real-time Streaming Protocol
* **SCTP** – Stream Control Transmission Protocol
* **HTTP-s** – Secure Hypertext Transfer Protocol
* **SLP** – Service Location Protocol
* **SMTP** – Simple Mail Transfer Protocol
* **SNMP** – Simple Network Management Protocol
* **X**-**Window**

#### Routování (síťová vrstva)

* **EGP** – Exterior Gateway Protocol
* **BGP** – Border Gateway Protocol
* **RIP** – Routing Transformation Protocol
* **IGRP** – Interior Gateway Routing Protocol
* **TRIP** – Telephony Routing over IP

#### Tunelování (llinková vrstva)

* **ATMP** – Ascend Tunnel Management Protocol
* **L2F** – Layer2 Fowarding Protocol
* **L2TP** – Layer2 Tunneling Protocol

#### Zabezpečení

* **AH** – Authentication Header
* **ESP** – Encapsulating Security Payload
* **TLS** – Transport Layer Security Protocol

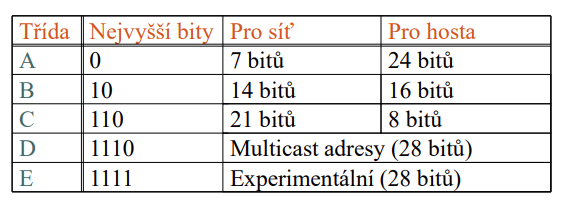
# 18. Adresování v TCP/IP sítích

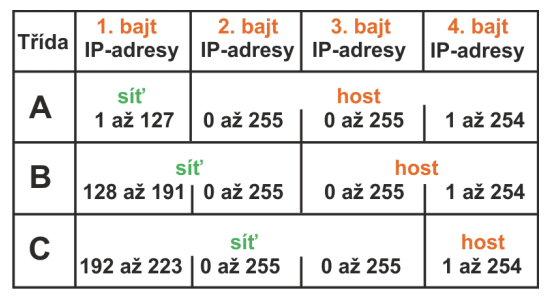
### IPv4

#### Adresa

* 32 bitová adresa
* Obvykle se zapisuje dekadicky ve formě 4 čísel v intervalu 0-255 oddělených tečkami
* Skládá se ze dvou částí
  + Síťové části adresy – prefixu
  + Části adresy adresující hosta (síťové rozhraní počítače, routeru, tiskárny..)

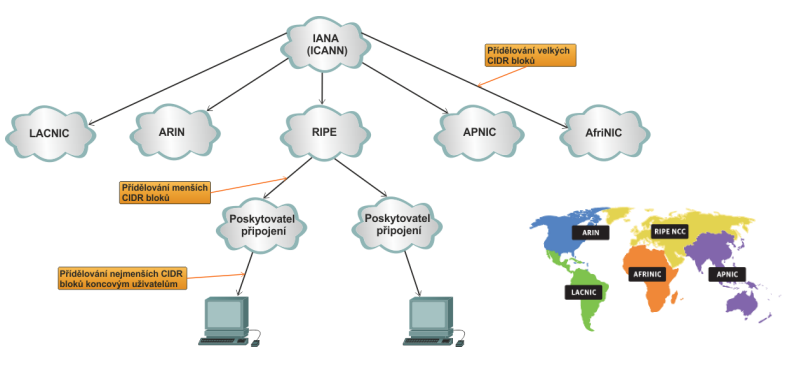
#### Původní koncepce

* Rozlišovala 5 tříd IP adres.
* Třídy A, B a C byly určeny pro adresování jednotlivých hostů – unicast adresy.
* Třída D pro adresování skupiny počítačů – multicast adresy.
* Třída E se dodnes nepoužívá



#### Současná koncepce

* Nerozlišuje adresy ve třídách A, B a C, ale pracuje s nimi jako s rovnými
* Síťové adresy jsou ve formě CIDR (Classless Inter-Domain Routing) bloků přidělovány pro jednotlivé části světa organizací IANA, v Evropě organizací RIPE pro jednotlivé státy evropy
* V jednotlivých státech přidělují CIDR bloky národní provideři



#### Speciální vyhrazené IP adresy

* **0.0.0.0**
  + Např. host před dotazem na DHCP server, defaultní cesta na směrovačích, rezervován je bohužel celý rozsah 0.0.0.0 až 0.255.255.255
* **Loopback softwarová zpětnovazební adresa**
  + Prakticky se používá jen adresa 127.0.0.1, rezervován je celý rozsah
* **Link-local adresy**
  + Pro automatické nastavení IP adresy v LAN pokud nelze nalézt DHCP server, směrovače pakety s těmito adresami zahazují, rezervován je rozsah adres 169.254.0.0 až 169.254.255.255
* **TEST-NET adresy**
  + Pro výuku a studijní účely v LAN, směrovače paket s těmito adresami zahazují, rezervován je rozsah 192.0.2.0 až 192.0.2.255

#### IPv4 vyhrazené neveřejné IP adresy

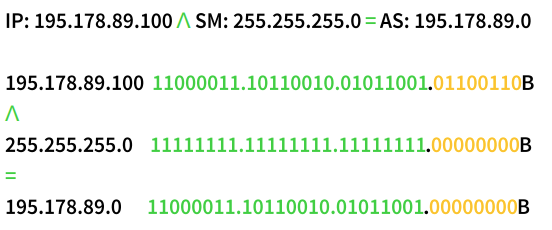
* Každý přímo připojený host sítě v Internetu musí mít jedinečnou veřejnou IP adresu
* Vyjímka:
  + Za NATem nebo PATem (Port Address Translation) – překladem adres můžeme přidělovat libovolné IP adresy z tříd A, B a C bez ohledu na to jestli jsou v internetu již použity



#### IPv4 síťová a subsíťová maska

* Síťová (SM) a subsíťová maska (SSM) slouží k určení adresy sítě (AS), subsítě (ASS) z IP adresy hosta
* Čtyřbajtové číslo, zapisuje se v desítkové soustavě stejně jako IP adresa
* Maska vyjádřená v dvojkové soustavě má v bitech určujících síťovou část adresy jedničky a ve zbývajících bitech nuly
* Adresu sítě z IP adresy získáme logickým součinem binárních tvarů IP adresy hosta se síťovou nebo subsíťovou maskou

#### Příklad



* Maska se stále častěji nahrazuje počtem jedničkových bitů masky (délka prefixu). Uvádí se za IP adresou, oddělovačem je lomítko
  + 195.178.89.100/24
* **Třída A** používá pro adresu sítě první bajt – síťová maska pro adresy třídy A má v prvním bajtu jedničky a ve zbylých bajtech nuly
  + 11111111.00000000.00000000.00000000
  + Desítkově: 255.0.0
  + Odpovídá /8 za IP adresou
* **Třída B** používá pro adresu sítě první dva bajty
  + 11111111. 11111111.00000000.00000000
  + Desítkově: 255.255.0.0
  + Odpovídá /16 za IP adresou
* **Třída C** využívá pro adresu sítě první tři bajty
  + 11111111. 11111111. 11111111. 00000000
  + Desítkově: 255.255.255.0
  + Odpovídá /24 za IP adresou

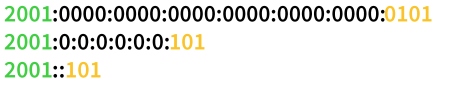
#### IPv4 Dělení sítí na subsítě

* Během rozvoje internetu začal být nedostatek síťových adres a počet IP adres v jednotlivých třídách většinou nebyl u reálných sítí naplnitelný. Proto byly jednotlivé sítě dále děleny na subsítě, tedy jedna síť je rozdělena na několik subsíťí s menším počtem IP adres (dělíme CIDR blok na více menších CIDR bloků)
* Na subsítě můžeme rozdělit kteroukoliv síť tříd A, B a C
* V podstatě rozšíříme počet bitů pro síťovou část adresy (prefix) na úkor části adresy pro klienta
* Součet IP adres subsítí je roven počtu IP adres dělené sítě na subsítě, počet použitelných adres pro adresaci síťových rozhraní je ale menší, např. pří dělení sítě /24 na subsítě /30 (4 IP adresy) je jen poloviční

### IPv6

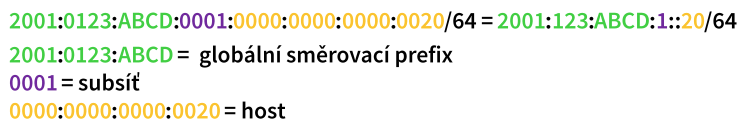
#### Formát IPv6 adresy

* Aby se zápis zkrátil, lze v jednotlivých čtveřicích vynechávat nevýznamné nuly zleva
* Pokud se vyskytne několik po sobě jdoucích nulových skupin, lze je nahradit dvojicí dvojteček. Ta se však v zápisu každé adresy smí objevit jen jednou, aby byl zápis jednoznačný



#### Globální unicast adresy

* V rozsahu 2000::/3 (2000 - 3FFF)
* Odpovídají veřejným unicastovým adresám IPv4
* Prvních 48 bitů zleva v arese je globální směrovací prefix, dalších 16 bitů je ID subsítě a posledních 64 bitů je určeno pro ID uzlu
* Tedy v každé síti může být 216 subsítí a v každé subsíti může být 264 uzlů



#### Link-local unicast adresy

* V rozsahu FE80::/10 (FE80 – FEBF)
* Slouží ke komunikaci hostů v rámci LAN včetně routeru
* Paket s link-local adresami neprojde přes router do jiné LAN, tedy adresy se mohou v různých LAN připojených na router opakovat
* Pokud není link-local adresa přidělena hostu ručně, je generována automaticky bez ohledu na to, jestli host má či nemá přidělenou globální unicastovou adresu

#### Unique local

* V rozsahu FC00::/7 (FC00-FDFF)
* Částečně podobné vyhrazeným neveřejným adresám v IPv4, nepoužívají se pro NAT a PAT, protože v IPv6 je dostatek globálních unicastových adres
* Používají se pro lokální adresování místní LAN, nejsou routovatelné veřejné části IPv6 internetu

#### Multicast adresy

* V rozsahu FF00::/8
* Skupinové adresování

#### Broadcast adresy

* IPv6 nepoužívá broadcastové adresy
* Pro rozeslání paketu všem uzlům v LAN lze použít multicastovou adresu FF02::1

#### Host ještě nezná svoji adresu

* ::/128

#### Loopback

* ::1/128

#### Přidělování adresy hostu

* **Statické (ručně)**
  + Přidělíme hostu celou IPv6 adresu, tedy včetně části pro hosta
  + Staticky lze přidělovat hostu jak globální unicastová adresa, tak Link-local adresa
  + V případě přidělení jen globální unicastové adresy na síťovém rozhraní, přebírá Link-local adresa část pro hosta z globální unicastové adresy
* **Dynamicky bez DHCP serveru**
  + Síť s routerem bez DHCP serveru
  + Host obdrží od routeru prefix a jeho délku (/64) přidělované adresy a část pro hosta vygeneruje:
    - Algoritmem UEI-64: převezme si Ethernet MAC adresu síťového rozhraní (6 B) a doprostřed MAC adresy přidá řetězec FFFE, vznikne 64 bitová část adresy pro hosta. Dále invertuje bit 7 v levém byte
    - Generátorem náhodných čísel s kontrolou duplicity v LAN vygeneruje všech 64 bitů části adresy pro hosta



* **Dynamicky s bezstavovým DHCP serverem**
  + Síť s routerem a bezstavovým DHCP serverem (neeviduje přidělené adresy hostům)
  + Host obdrží od routeru prefix a jeho délku (/64) přidělované adresy a část pro hosta vygeneruje jako v předchozím případě. Zbylé informace např. adresu brány, DNS serverů.. získá po odkazu z routeru od DHCP serveru
* **Dynamicky se stavovým DHCP serverem**
  + Síť s routerem a stavovým DHCP serverem (eviduje přidělené adresy hostům)
  + Veškeré síťové parametry získá host po odkazu z routeru od DHCP serveru

# 19. TCP/IP port a socket

#### Port

* Malé kladné celé číslo, které slouží k rozlišení síťového aplikačního procesu na počítači

#### Socket

* Uspořádaná dvojice sestávající se z IP adresy a z portu
  + 195.178.89.100:80

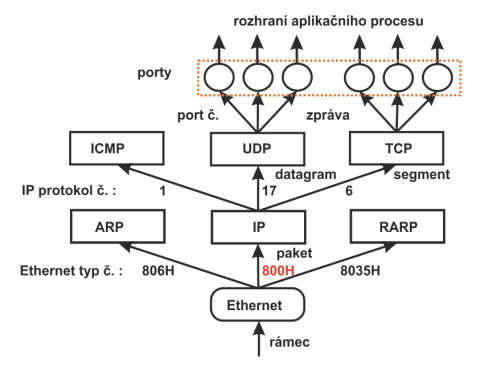
#### Rozdělení portů

* Všeobecně známé porty
  + 0 až 1023
* Registrované porty (registrátor IANA)
  + 1024 až 49151
* Dynamické a soukromé porty
  + 49152 až 65535

#### Příklady přiřazení portů aplikačním procesům

* 20 – FTP – vlastní přenos dat
* 21 – FTP – řízení
* 22 – SSH
* 23 – TELNET
* 53 - DNS
* 80 – HTTP
* 110 – POP3
* 143 – IMAP4
* 443 – HTTPS

#### Princip demultiplexování



# 20. Propojování počítačových sítí

### Kolizní doména

* Část sítě, ve které se šíří signál vyslaný síťovým rozhraním
* V této částí sítě může dojít ke kolizi se signálem vyslaným jiným síťovým rozhraním
* Kolizní domény oddělují např. bridge, switche a routery, tedy zařízení pracující na 2. a vyšší vrstvě modelu OSI

### Broadcastová doména

* Část sítě, ve které se šíří rámec s MAC broadcastovou (všeobecnou) adresou
* U Ethernetu FF-FF-FF-FF-FF-FFH
* Broadcastové domény odděluje např. router, tedy zařízení pracující na 3. a vyšší vrstvě modelu OSI

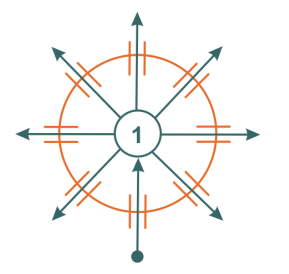
### Dělení síťových propojovacích zařízení

* Dle toho, na které vrstvě OSI dochází k přenosu dat děláme propojovače na:
  + 1. vrstvě: repeatery, huby
  + 2. vrstvě: bridge, switche
  + 3. vrstvě: routery, L3 switche
  + 7. vrstvě: zařízení bývá pojmenováno jako gateway bez udání úrovně
  + N-té vrstvě: gateway úrovně N, tedy např. router je gateway úrovně 3

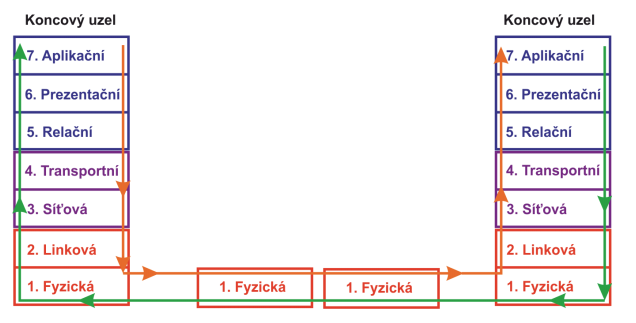
### Repeater a hub

* Převádí data na 1. vrstvě modelu OSI – jsou nezávislé na přenášeném protokolu
* Repeater zesílí a opraví signál a převede jej do druhé části sítě
* Huby – multirepeatery navíc rozvětvují signál, výjimkou jsou pasivní huby, které signál pouze rozbočují bez zesílení a opravy – LAN Arcnet
* Nerozdělují kolizně ani broadcastově síť – vytváří v Ethernetu kolizní a broadcastovou doménu
* Pro koncové a přepojovací uzly jsou neviditelné
* Ethernet – teoreticky maximálně 4 repeatery mezi dvěma koncovými uzly s omezeními, prakticky maximálně 2 repeatery

#### Šíření dat přes hub



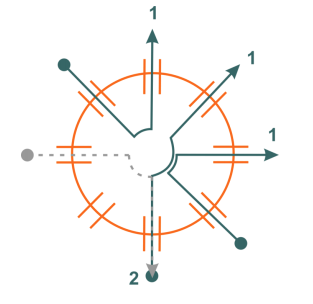
#### Model OSI



### Bridge a switch

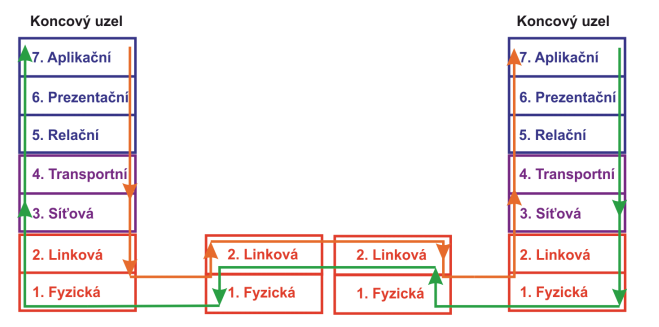
* Převádí data na 2. vrstvě modelu OSI – jsou nezávislé na přenášeném protokolu
* Směrují do druhé sítě všechny data, které do ní patří, pokud neznají adresáta, nebo v případě broadcastové adresy fungují po logické stránce jako repeatery nebo huby
* Musí přijímat všechny rámce
* Dynamicky se učí – aktualizují MAC tabulky pomocí BLA (Backward Learning Algorithm) – neznají-li adresáta, rozešlou rámec všemi směry a z odpovědi adresáta zjistí, na kterém portu adresa sídlí

#### Šíření dat přes switch

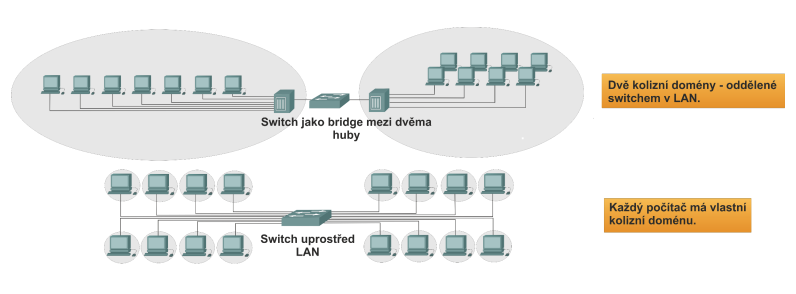


* Položky v MAC tabulce (port a MAC adresa/y) se uchovávají typicky 5 minut
* Rozdělují kolizně síť – rozdělují u Ethernetu kolizní doménu na více kolizních domén
* Nerozdělují broadcastově síť – vytváří v Ethernetu broadcastovou doménu
* Pro koncové a přepojovací uzly jsou neviditelné
* Ethernet – jejich počet není omezen
* Předchozí obrázek platí pro polo duplexní provoz, při plném duplexu by mohly rámce na dolním portu být přijmuty a odeslány ve stejný časový okamžik

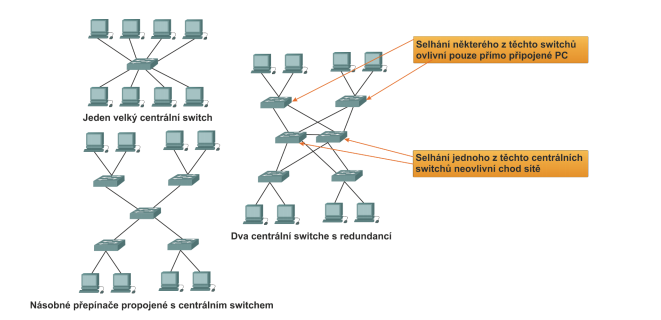
#### Model OSI



#### Nahrazení hubů switchem



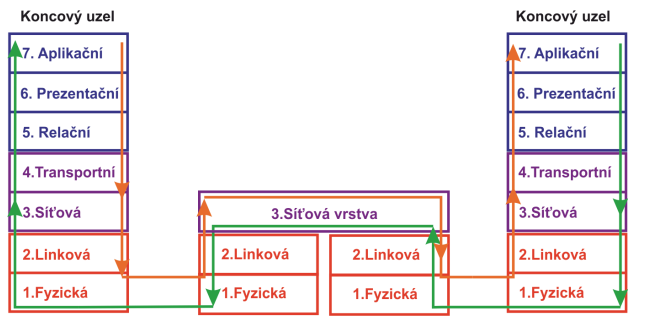
#### Faktory výběru LAN switche



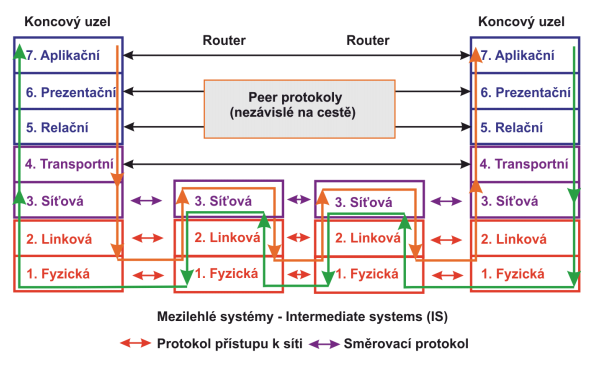
### Router

* Převádí data na 3. úrovni modelu OSI – jsou závislé na síťovém protokolu
* Směrují do druhé sítě všechna data, která do ní patří, pokud neznají cestu, generují chybové hlášení, pracují softwarově
* Přijímají jen rámce jim adresované – s cílovou MAC adresou rámce rovnající se jejich MAC adrese a MAC adrese broadcastové rámce jako PC
* Rozdělují kolizně i broadcastově síť, pro koncové uzly jsou viditelné
* Routovací tabulky
* Routovací protokoly (např. RIP, OSPF, IS-IS, BGP..)

#### Model OSI



#### Model OSI včetně horizontální komunikace



### Routing switch

* Zařízení, která fungují na 3. úrovni vrstvy (proto „router“), ale současně používají metody a techniky původně používané na úrovni 2. vrstvy (proto „switch“)
* Převedení základních směrovacích funkcí do hardwaru
* Zařízení zajišťuje volbu přepínání nebo směrování na každém portu
* Zařízení umožňuje provozování standartních směrovacích protokolů (RIP, OSPF, BGP)
* Směrování a přepínání jsou stejně rychlé

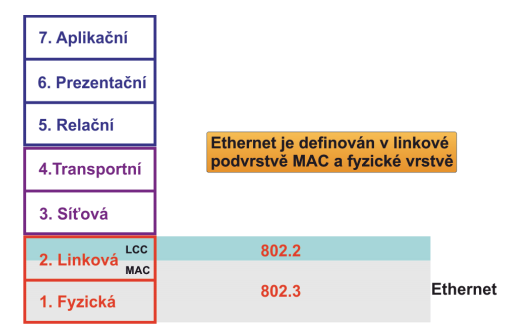
### Gateway

* Převádí data na 7. vrstvě v případě neslučitelných formátů dat síťových aplikací, např. elektronické pošty (jiný systém adres, hlavičky mailu…)
* V případě, že spojované sítě používají odlišný síťový protokol, převádí gateway data až nad 7. vrstvou

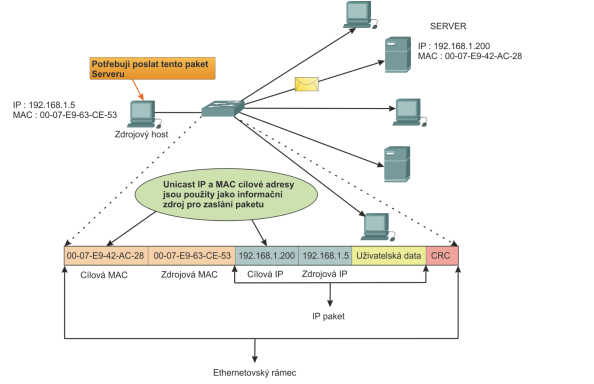
# 21. Síť Ethernet

* Dříve jen LAN, dnes MAN i WAN
* Pokrývá HW 1. a SW 2. vrstvu (podvrstvu MAC) modelu OSI
* Přenosová rychlost až 100 Gb/s
* Přenosová média TP a FO
* Fyzická topologie sběrnice, hvězda a strom
* Logická topologie sběrnice
  + Přenášená data jsou rozesílána všem uzlům, takže každý uzel obdrží data v přibližně stejném čase (platí pro fyzickou topologii sběrnice, fyz. top. Hvězda a strom s huby)
* Kódování se liší s přenosovou rychlostí a přenosovým médiem, např. 10 Mb/s TP i optická vlákna – Manchester
* Přístupová metoda CSMA/CD do 1 Gb/s v základním pásmu (baseband). Od 10 Gb/s jen dvojbodové spoje (switch-pc, switch-router…) s plným duplexem
* V přeloženém pásmu (broadband) jen několik verzí
* MAC adresa 6 B, první 3 B zleva charakterizují výrobce NIC. Obsah 3 B zprava si určuje výrobce
* Speciální vyhrazené adresy
  + Broadcast: FF-FF-FF-FF-FF-FF
  + Multicast: 01-00-5E-xx-xx-xx (broadcast šíření)

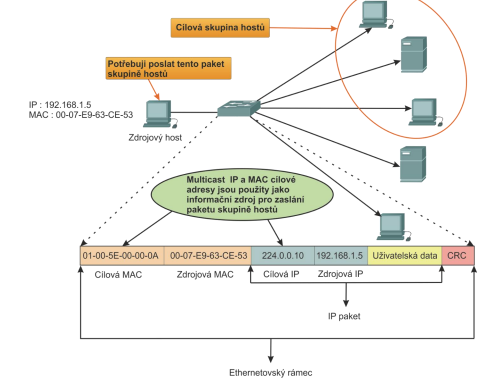
### Začlenění do modelu OSI



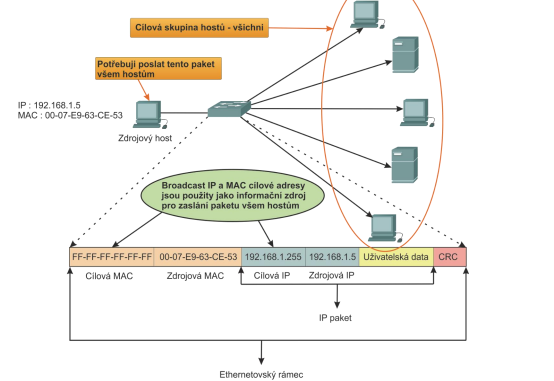
### Zasílání unicastu



#### Zasílání multicastu

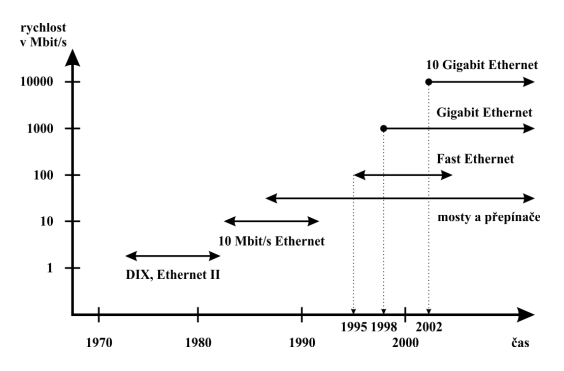


#### Zasílání broadcastu



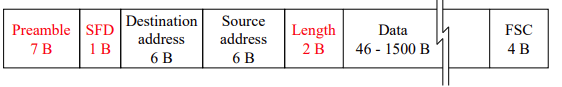
### Vývoj

* Vývoj byl zahájen v polovině 70. let ve firmě Xerox
* Dále vyvíjen společně firmami **D**EC, **I**ntel a **X**erox, v roce 1980 přijat standard **DIX** Ethernet těmito firmami
* DIX předložila svůj návrh podskupině IEEE 802.3, která po úpravách přijala Ethernet v roce 1983 jako standard IEEE 802.3 na bázi CSMA/CD
* Jedná se o nejpoužívanější síťovou architekturu pro LAN
* Později vznikl Ethernet II
* Ethernet používá 4 druhy rámců – IEEE upravený 802.3, Ethernet II, 802.3 SNAP a „raw“ 802.3

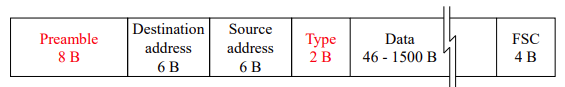


### Rámce

#### IEEE 802.3 (původní)

* Délka rámce 64 až 1518 B (nepočítá se Preamble a SFD)
* **Preamble**
  + Sekvence 56 bitů v nichž se neustále střídají hodnoty 1 a 0, slouží k synchronizaci hodin příjmače
* **SFD (Start Frame Delimiter)**
  + Sekvence obsahující 8 bitový vzorek 10101011, ukončuje začátek rámce, za kterým již následují informace
* **Destination address**
  + MAC adresa hosta, pro kterého je rámec určen
* **Source address**
  + MAC adresa hosta, který rámec odesílá
* **Length**
  + Určuje délku části Data
* **Data**
  + Obsahuje rámec 802.2, který je rámcem podvrstvy LLC linkové vrstvy
* **FSC (Frame Check Status)**
  + Obsahuje CRC (Cyclic Redundancy Check), zbytek po dělení bitů kontrolované části rámce stanoveným polynomem) – CRC se vypočítává na straně odesílatele, nezahrnuje část Preamble a SED. Vadné rámce se zahazují

#### Ethernet II

* Označený jako průmyslový standard
* Type (typ paketu)
  + Specifikuje protokol použitý na 3. vrstvě modelu OSI (např. IP, ARP, RARP…)
  + Ostatní části shodné s původním rámcem IEEE 802.3

#### IEEE upravený 802.3

* IEEE upravila původní rámec 802.3 v položce Lenght o možnost volby Lenght/Type, čímž zajistila kompatibilitu s rámcem Ethernet II
* Dnes preferovaný typ rámce

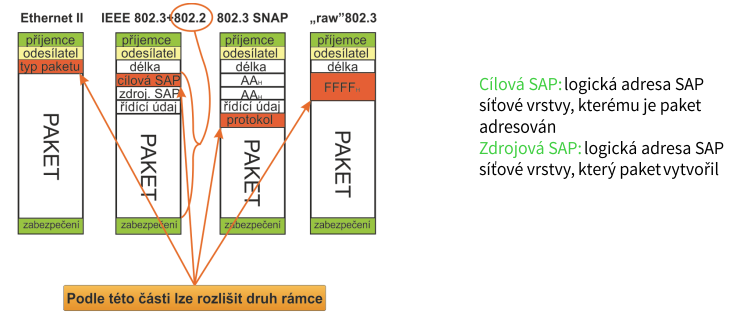
#### 802.3 SNAP

* SubNetwork Access Protocol – např. Cisco VTP (VLAN Trunking Protocol)

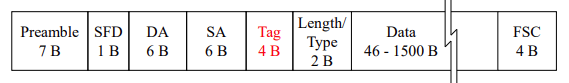
#### „raw“ 802.3

* Používala firma Novell

#### Přehled typů rámců



* Pro VLAN dle 802.1Q byly přidány 4 B – tag (taggované rámce). Maximální délka rámce tedy byla zvětšena na 1522 B. Pro přenos dat více VLAN přes jednu linku musí být nastaveny porty přepínače do trunku a u routeru definovány subinterface. Tag obsahuje identifikátor protokolu TPID – 2B. V dalších 2 B jsou umístěny priorita dle 802.1p – 3 bity, identifikátor povolení přenosu rámců Token Ring přes Ethernet síť – 1 bit a identifikátor VLAN – 12 bitů (VLAN 1 až VLAN 4096)



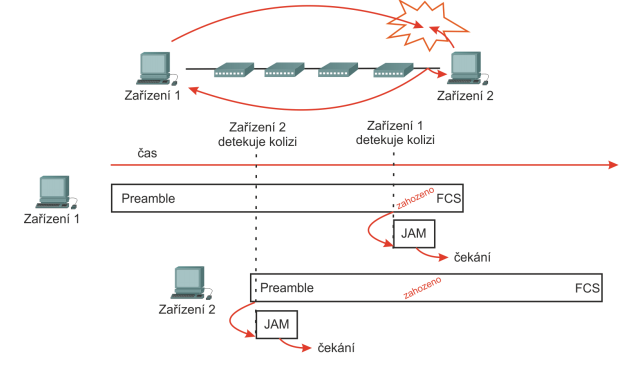
### Mezirámcová mezera

* Je nutná ke stabilizaci komunikačního média pro přenesení rámce
* Ke zpracování rámce v přijímacím řízení

### Kolize rámců

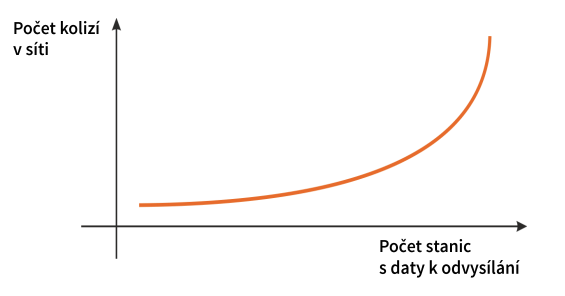
#### Řešení kolize

* Jen u verzí s CSMA/CD – do 1 Gb/s
* V případě, že stanice zjistí nesoulad mezi daty na vedení a daty, která vysílá, přeruší okamžitě vysílání a vyšle rušící signál „jam“ 32 b (101010101..)
* Po odvysílání rušícího signálu čeká stanice po dobu nutnou k odvysílání nejkratšího rámce vynásobenou náhodně vygenerovaným číslem z intervalu 0-2k, kde k je počet opakování vysílání tohoto rámce (max 10). Pokud rámec není odeslán ani po 16ti pokusech, je hlášena chyba
* Ostatní stanice (ty co nezpůsobily kolizi) čekají po přijetí rušícího signálu po dobu mezirámcové mezery



* CSMA/CD ztrácí smysl u přepínaného Ethernetu s plně duplexním provozem při i při rychlostech od 10 Mb/s
* U polo duplexního provozu 10 Mb/s až 1 Gb/s je detekována kolize při pokusu o obousměrný přenos dat

#### Závislost počtu kolizí na zatížení sítě



### Součásti sítě

#### Přenosová média

* TP
* TO

#### Konektory

* RJ-45 pro TP
* Optické konektory pro FO

#### Síťová karta

* Obsahuje HW (MAC) adresu na čipu ROM, která je pevně dána výrobcem a je pro tuto konkrétní kartu jedinečná (ethernet adresa). V některých OS je tato adresa měnitelná pomocí SW, nelze však měnit výrobní MAC adresu v ROM karty
* Je vybavena jedním (TP), nebo dvěma (TO) konektory pro připojení k přenosovému médiu

#### Repeater

* Do 100 Mb/s, u 100 Mb/s dvě verze: Class I – Translation repeater a Class II – Transparent repeater

#### Hub

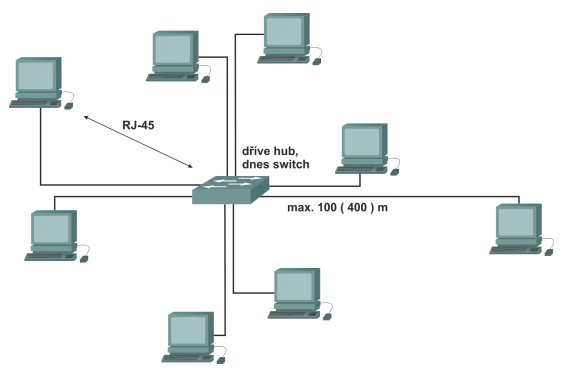
* Do 100 Mb/s

#### L2 switch (bridge)

#### Router, L3 switch

### BaseT

* Verze s TP
* Každý uzel je připojen k hubu nebo na switch, který plní roli společného přenosového média (slouží jako přenosová stanice)
* Maximální vzdálenost mezi uzlem a hubem, nebo switchem je 100 m (STP umožňuje neoficiálně až 400 m)
* Huby i switche je možné kaskádovitě řadit za sebe



* Při kaskádovitém řazení je však nutné u hubu dodržovat pravidlo 5-4 (pro switche bez omezení): max 5 segmentů propojených 4 huby



#### 100Base-TX (10Base-T)

* TP CAT 5 (3) a vyšší, 2 páry, 100 m, polo duplex – jen jedním párem v jednom směru 100 Mb/s (10 Mb/s), plná duplex – oběma páry najednou, ale párem vždy jednosměrně 100 Mb/s

#### 1GBase-T nebo 1000Base-T

* TP CAT 5E a vyšší, 4 páry, 100 m, polo duplex, jednosměrná komunikace na páru střídavě v obou směrech, plný duplex – obousměrná současná komunikace na páru

#### 10GBase-T

* TP CAT 6a a vyšší, 4 páry, 100 m, pouze plný duplex – obousměrná současná komunikace na páru (zrušena přístupová metoda CSMA/CD)

#### 40GBase-T

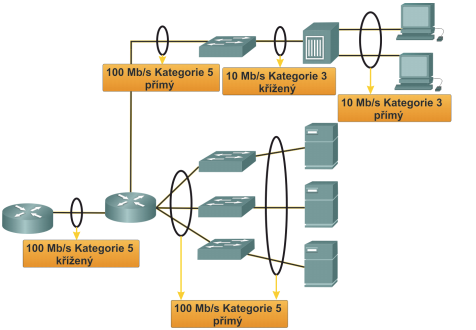
* TP CAT 8, 4 páry, 30 m, vychází z 10GBase na kroucené dvojlince

### XBaseT

#### Přímý a křížený kabel

* **Přímý kabel**
  + Oba konce T568B nebo T568A – propojení zařízení mezi skupinou PC, router a hub, bridge, switch. Např. PC- Switch
* **Křížený kabel 10 a 100 Mb/s**
  + Kříží se jen 2 páry – jeden konec T568A a druhý konec T568B – propojení zařízení ve stejné skupině
* **Křížený kabel 1 a 10 Gb/s**
  + Kříží se všechny 4 páry. Není nutné jej používat (každý vstup je zároveň i výstupem). Proto se prakticky používá jen přímý kabel

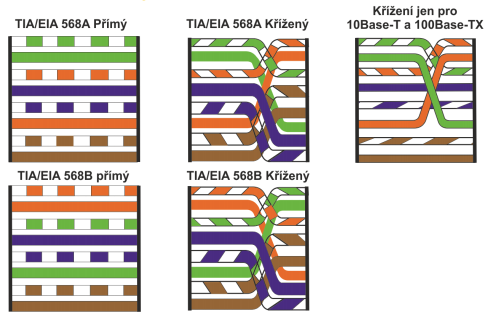
#### Určení typu kabelu pro připojení rozdílných koncových zařízení v LAN



* Pokud zařízení má křížený vstup (hub, starší switch) nebo autodetekci křížení (PC, switch), lze použít na 10 Mb/s, 100 Mb/s a 1 Gb/s místo kříženého i přímý kabel, např. PC-PC, Hub-Hub..
* U rychlosti 10 Gb/s se používá jen přímý kabel (plný duplex na každém páru)



#### Plně a částečně křížený kabel



# 22. Internet

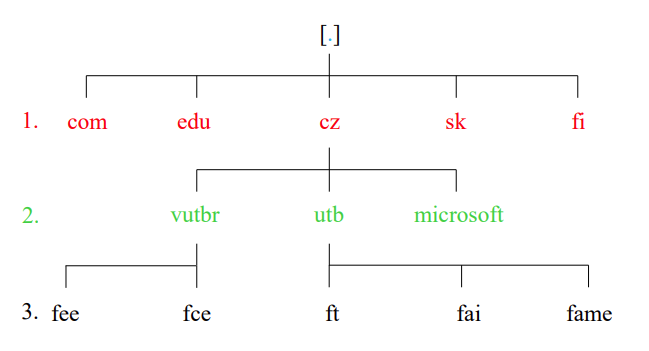
* Celosvětová počítačová síť (GAN)
* Skládá se ze vzájemně propojených menších sítí
* Síť založena na technice přepojování paketů
* Veškerá propojení mezi jednotlivými sítěmi jsou realizována přes routery, nebo gateway
* Routery směřují pakety v závislosti na cílové síti, nikoliv na cílovém počítači
* Protokoly rodiny TCP/IP zacházejí se všemi sítěmi jako s rovnocennými, nikoliv však s pakety, např. QoS

### Historie

* **1969** ARPANET – akademická sféra buduje za peníze od vojenské grantové struktury ARPA základ pozdějšího internetu (4 uzly: UCLA, Stanford Research Insitute, University of California Santa Barbara a University of Utah) s NCP protokolem (Network Control Protocol). Vojákům šlo o ověření paketového přenosu – chtěli vytvořit robustní síť. Později síť předána do plného provozu akademické sféře
* **1977–1979** – vývoj základní architektury TCP/IP
* **1983** – zaveden TCP/IP jako standard sítě místo protokolu NCP. Z ARPANETu vyčlenil MILNET (Military Network), připojení Stuttgartu a Jižní Korei
* **ARPANET** se stal zárodečnou sítí, ke které se postupně připojovaly další sítě – konkrétní soustava navzájem propojených sítí – internetwork, zkráceně internet
* **1984** - zaveden DNS
* **1986** - financování akademickou sférou NSF, páteřní síť ARPANET nahrazena sítí NSFNET
* **1989** - CERN – WWW stránky
* **Počátkem 90. let** financování na komerční bázi
* **11.10.1990** – Připojení ČSFR pevnou linkou z ČVUT do Lince k síti EARN
* **1991** – pokusné připojení ČSFR do Internetu na ČVUT
* **1993** – registrována doména CZ, 15.6 zahájení provozu CESNETu
* **1995** – doména CS nahrazena doménou CZ

### Adresace

* Kromě IP adresy je možné při komunikaci v Internetu použít i tzv. adresu v doménovém tvaru
  + Uvádí se v opačném pořadí než IP adresa
  + Jedná se o jméno hosta následované posloupností domén
  + Jako oddělovač se používá tečka
  + Počet úrovní domén není nijak omezen
* Příklad: **cas.fai.utb.cz**
  + cas – počítač cas
  + fai – Fakulta Aplikované Informatiky
  + utb – UTB ve Zlíně
  + cz – Česká republika
* domény vytvářejí stromovou strukturu
* kořenová doména (root) je označena tečkou
* domény na pozici 1. v následujícím obrázku jsou označovány jako domény nejvyšší úrovně



* Správce domény CZ je CZ.NIC – zájmové sdružení právnických osob – poskytovatelů internetu, registrace domén vycházejících z domény CZ
* Každá doména má správce, který zodpovídá za domény na nižší úrovni (směrem od kořene stromu)
* Je-li použita adresa v doménovém tvaru, je nutné ji převést před zahájením komunikace s hostem na IP adresu
* Tento převod se převádí pomocí DNS
  + Služba distribuovaného pojmenování použitá na Internetu se skládá ze dvou částí
    - DNS resolver
    - DNS server
* **DNS resolver** – proces žádající DNS server o převod doménové adresy na IP adresu nebo o obrácený převod, běží na stanicích i serverech (DNS servery mohou žádat pomocí svých resolverů jiné DNS servery o vyřešení dotazu na převod)
* DNS server – řeší požadavky od DNS resolverů
* Pro každou doménu musí být alespoň jeden DNS server (většinou bývají z bezpečnostních důvodů dva)