

Počítačové sítě

Rozdělení systémů pro sběr a přenos dat

podle aplikační oblasti

- počítačové a komunikační sítě
 - pevné
 - mobilní (terminály)
- průmyslové řídicí systémy
 - systémy řízení technologií budov
 - přístupové systémy (osob, vozidel, ...)
 - skladové a distribuční systémy (průmyslové objekty)
 - zabezpečovací systém
 - systémy pro sběr dat z měřičů médií

podle geografické rozlehlosti

- lokální (místnost, budova – řízení osvětlení, HVAC)
- rozlehlé (firma, město – přístupové a kamerové systémy)
- globální (stát – sběr dat z měřičů médií, PSTN)

podle technologie fyzické přenosové cesty

- metalické vedení
- optické vlákno
- bezdrátové
 - rádiové
 - optické

podle způsobu zpracování dat

- centralizované
- distribuované

podle stupně podpory práce v reálném čase

- real-time systémy (hard, soft)
- non real-time systémy

Referenční model ISO/OSI (Open System Interconnection)

[slidy](#)

- definován standardem ISO 7498-1

+ - první vydání je již z roku **1984**, platné z roku **1994**

- obecný rámec pro návrh protokolů distribuovaných systémů, do nějž jsou zasazována jednotlivá konkrétní řešení

- většina nových řešení byla navrhována s jeho využitím

-

(např. protokoly TCP/IP)

- hlavním cílem je umožnit snadné propojování distribuovaných systémů (heterogenní systémy)

- definuje **sedmivrstvý protokolový zásobník**

- jednotlivé vrstvy poskytují daný typ služeb

- je definován způsob interakce mezi vrstvami
- činnosti na stejném stupni abstrakce ve stejné vrstvě
- minimalizace datových toků mezi vrstvami
- aplikovatelnost na významné existující standardy (X.25)

Fyzická vrstva (Physical Layer)

- **přenos bitů** (symbolů)
- kódování, modulace, časování, synchronizace, elektrické parametry signálů, konektory, řídicí signály rozhraní, (!!!)
- přijmi bit, odešli bit
- na úrovni fyzické vrstvy se rozlišuje:
 1. paralelní a sériový přenos
 2. synchronní, asynchronní a arytmičtý přenos
 3. přenos v základním a přeloženém pásmu

Spojová vrstva (Data Link Layer)

- celé bloky dat - rámce (**frames**)
- pouze v dosahu přímého spojení - bez „přestupních stanic“
- spolehlivě či nespolehlivě, spojovaně či nespojovaně
- může využívat různé technologie fyzické vrstvy – linkové i bezdrátové
- hlavní úkoly jsou: (!!!)
 1. synchronizace na úrovni rámců - rozpoznání začátku a konce rámce, všech jeho částí
 2. řízení přístupu ke sdílenému médiu - řeší konflikty při vícenásobném přístupu ke sdílenému médiu
 3. adresace
 4. zajištění spolehlivosti - detekce chyb a náprava
 5. řízení datového toku - aby vysílající nezahltil příjemce

Síťová vrstva (Network Layer)

- přenáší bloky dat označované jako pakety (**packets**)
- zajišťuje doručení paketů až ke konečnému adresátovi
- v prostředí, kde není přímé spojení, hledá vhodnou cestu až k cíli
- zajišťuje tzv. směrování (**routing**) mezi sítěmi
- musí si uvědomovat skutečnou topologii celé sítě (obecně)
- může používat různé algoritmy směrování:
 - adaptivní, neadaptivní
 - izolované, distribuované
- je poslední vrstvou, kterou musí mít přenosová infrastruktura (až na ty velmi primitivní)
- asi nejrozšířenější implementací síťového protokolu je protokol **IP**, podporovaný protokoly pro výměnu informací o směrování mezi směrovači

Transportní vrstva (Transport Layer)

- vyšší vrstvy mohou mít jiné požadavky na charakter komunikace, než jaký nabízejí nižší vrstvy, obvykle nelze měnit vlastnosti a funkce nižších vrstev, třeba proto, že patří někomu jinému, vyšší vrstvy mohou mít různé (i protichůdné) požadavky
- úkolem transportní vrstvy zajistit potřebné přizpůsobení
- protokoly transportní vrstvy jsou implementovány pouze v koncových účastnících
- pokud by to tak nebylo, síť by poskytovala stejnou službu všem
- transportní vrstva může měnit: (!!!)
 - nespolehlivý charakter přenosu na spolehlivější
 - nespojovaný přenos na spojovaný
- napr. **TCP**

Relační vrstva (Session Layer)

- zajišťuje sestavení, řízení a zrušení relací pro spojovanou komunikaci
- dále může zajišťovat: (!!!)
 1. synchronizaci (např. více datových toků)
 2. šifrování dat
 3. kompresi dat
 4. podpora transakčního zpracování dat

Prezentační vrstva (Presentation Layer)

- nižší vrstvy se snaží doručit každý bit přesně tak, jak byl odeslán
- stejná posloupnost bitů může mít pro příjemce jiný význam než pro odesílatele, např. kvůli kódování znaků (ASCII atd.). formátu čísel (malý a velký endian), formátu struktur, polí atd.
- prezentační vrstva má na starosti potřebné konverze

Aplikační vrstva (Application Layer)

- původní představa:
 - bude obsahovat aplikace (moc aplikací, musely by být standardizovány)
- později:
 - aplikační vrstva bude obsahovat pouze „jádro“ aplikací, které má smysl standardizovat (např. přenosové mechanismy el. pošty, služby pro přístup k objektům distribuovaným v síti)
- ostatní části aplikací (typicky: uživatelská rozhraní) byly vysunuty nad aplikační vrstvu

Související definice

SAP - Service Access Point (N)

- bod, kde jsou služby N-té vrstvy poskytovány N+1 vrstvě

PCI - Protocol Control Information (N)

- řídicí informace sloužící ke koordinaci entit na vrstvě N

User data (N)

- data přenášená vrstvou N na žádost vrstvy N+1

PDU – Protocol Data Unit (N)

- datová struktura vrstvy N skládající se z řídicí informace a volitelně uživatelských dat

SDU – Service Data Unit (N-1)

- informace předávaná mezi vrstvami N a N-1

Connection (N)

- virtuální spojení mezi entitami na vrstvě N
- existuje prostřednictvím služeb poskytovaných nižšími vrstvami

Centralized connection (N)

- data odesílaná centrální entitou jsou přijímána všemi ostatními entitami vrstvy N, v opačném směru ale jen centrální entitou

Decentralized connection (N)

- data odesílaná libovolnou entitou vrstvy N jsou přijímána všemi ostatními entitami vrstvy N

Multiplexing – Demultiplexing (N)

- funkce vrstvy N, kdy jediné spojení vrstvy N-1 je použito pro více spojení vrstvy N

Splitting – Recombining (N)

- funkce vrstvy N, kdy pro jediné spojení vrstvy N je využito více spojení vrstvy N-1

Segmenting – Reassembling (N)

- funkce entity vrstvy N, kdy jediné SDU N je mapováno do více PDU n

Blocking – Deblocking (N)

- funkce entity vrstvy N, kdy více SDU je mapováno do jediného PDU

Concatenation – Separation (N)

- funkce vrstvy N, kdy více PDU vrstvy N je mapováno do jediného SDU vrstvy N-1

Přenosové cesty

[slidy](#)

Metalická přenosová cesta

- prvek bezztrátového modelu metalického vedení
- L_0 a C_0 představují indukčnost a kapacitu na jednotku délky, označujeme je jako primární parametry

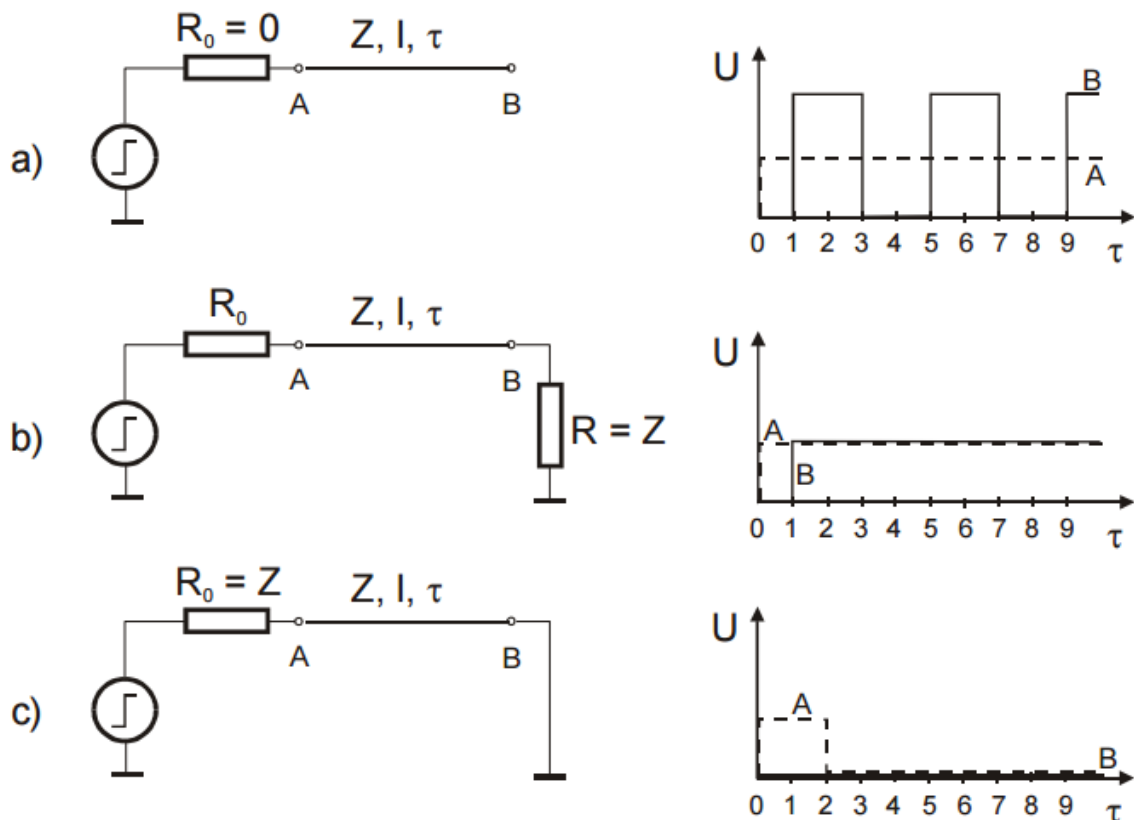
- Z_0 je charakteristická impedance vedení, $Z_0 = \sqrt{\frac{L_0}{C_0}}$, τ je zpoždění na jednotku délky

$$\tau = \sqrt{L_0 \cdot C_0}$$

- označujeme je jako sekundární parametry
- skládá se ze 3 částí: vysílač, přijímač a vedení
- kdy se musíme dívat na metalický spoj jako na vedení?
 - je-li významný vliv konečné rychlosti šíření signálu

- v různých bodech podél vedení jsou různé okamžité hodnoty napětí a proudu
- u číslicových signálů je významná hranice, kdy doba trvání hrany je kratší než dvojnásobek doby šíření signálu vedením
- odraz od konce vedení dorazí zpět až po změně úrovně

	L_0 [nH/cm]	C_0 [pF/cm]	Z [Ω]	τ [ns/m]
samostatný vodič (vzdálený od země)	20	0,06	600	~ 4
vakuum	μ_0	ε_0	370	3,3
kroucený dvoudrát	5 - 10	0,5 - 1	80 - 120	5
plochý kabel (prokládaný signál – země)	5 - 10	0,5 - 1	80 - 120	5
koaxiální kabel	2,5	1,0	50	5
signál na plošném spoji	5 - 10	0,5 – 1,5	70 - 100	~ 5
sběrníkový signál na plošném spoji	5 - 10	10 - 30	20 - 40	10 - 20



- varianty:

- koaxiální kabel
- kroucený dvoudrát
- „Nějaké“ dva dráty natažené „paralelně“ vedle sebe

Koaxiální kabel

- střední vodič, dielektrikum, vnější vodič, plášť
- vysoká šířka pásma (až jednotky GHz)
- charakteristická impedance typicky 50 nebo 75
- útlum v jednotkách až desítkách dB/100 m dle frekvence
- nesymetrické (**single-ended**) vedení
- v porovnání s kroucenou dvoulinkou:
 - nižší útlum na jednotku délky
 - vysoká odolnost vůči vnějšímu elektromagnetickému rušení
 - obtížnější konektování, dražší konektory
 - obtížnější instalace, nesnáší ostré ohyby
 - obtížnější připojování
 - vyšší cena

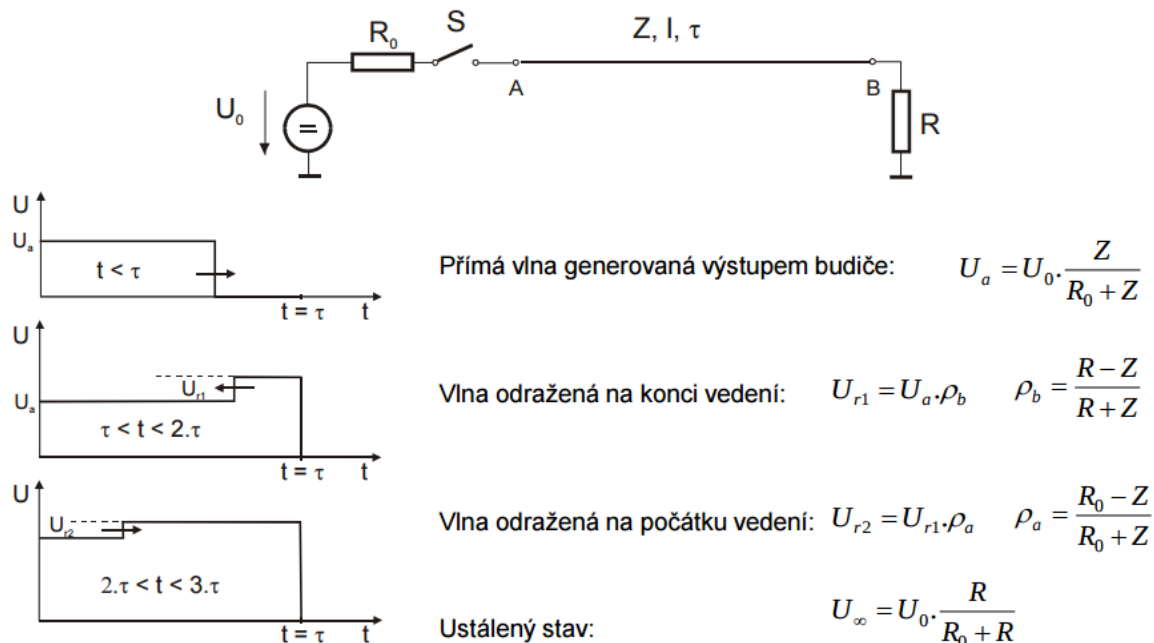
Kroucený dvoudrát (twisted pair)

- jeden nebo několik párů kroucených izolovaných vodičů
- šířka pásma stovky MHz
- stíněná (**STP**) i nestíněná (**UTP**) varianta
- charakteristická impedance okolo 100
- obvykle symetrické (differential) vedení
- flexibilní, snadné napojování, konektování

- relativně levné
- dělení do kategorií podle EIA/TIA 568B:
 - Kategorie 1**
 - dnes již není EIA/TIA specifikována
 - kabel pro klasické hlasové služby
 - „nejobyčejnější“ kroucená dvojlinka
 - s rozvojem moderních číslicových modulací se využívá i pro ISDN a xDSL technologie
 - Kategorie 2**
 - dnes již není EIA/TIA specifikována
 - původně určen pro síť token-ring 4 Mb/s
 - Kategorie 3**
 - pro datové síť s šířkou pásma do 16 MHz
 - nejrozšířenějším příkladem je IEEE802.3 - 10BaseT
 - dnes se ještě používá pro rozvod klasické telefonie v budovách
 - Kategorie 4**
 - dnes již není EIA/TIA specifikována
 - původně pro datové síť s šířkou pásma do 20 MHz
 - token-ring 16 M/s, 10BaseT, 100BaseT4
 - Kategorie 5**
 - dnes již není EIA/TIA specifikována
 - kabel pro datové síť s šířkou pásma do 100 MHz
 - existuje jak stíněné, tak nestíněné provedení
 - nejčastěji využíván pro 100BaseTX Ethernet
 - Kategorie 5e**
 - náhrada kategorie 5
 - specifikuje další požadavky (far-end cross-talk)
 - kabel pro datové síť s šířkou pásma do 100 MHz
 - vhodný pro 100BaseTX i 1000BaseT Ethernet
 - Kategorie 6**
 - pro datové síť s maximální šířkou pásma do 250 MHz
 - vyhovuje pro 1000BaseT Ethernet
 - Kategorie 6a**
 - pro datové síť s maximální šířkou pásma do 500 MHz
 - na specifikaci se pracuje
 - měla by vyhovovat pro 10Gb Ethernet
 - Kategorie 7**
 - jednotlivé páry jsou stíněny
 - využití pro 10Gb Ethernet na větší vzdálenosti
- **význam kroucení**
 - působení vnějšího elmag. pole vyvolává indukci rušivého napětí do smyčky tvořené dvojicí vodičů
 - při zkroucení se příspěvky indukované do jednotlivých elementárních smyček sčítají, mají však opačná znaménka a při shodné ploše smyček i shodnou velikost
 - analogický efekt se uplatňuje pro vyzařované elmag. pole

„Nějaká“ dvojice vodičů

- charakteristická impedance typicky 120 Ω a více
- v průběhu vedení se mění tak, jak kolísá vzdálenost vodičů



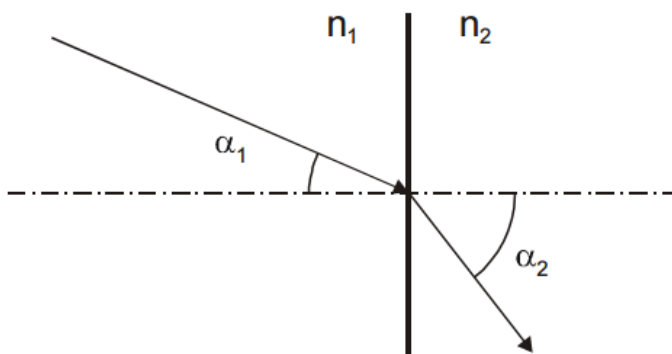
- tím dochází k útlumu vlivem odrazů
- s rostoucí vzdáleností vodičů stoupá „indukčnost“ vedení a tím i citlivost k vnějšímu rušení
- útlum takovéto dvojice vodičů s rostoucí frekvencí významně stoupá
- není vhodná pro přenosy s šířkou pásma vyšší než několik stovek kHz až jednotek MHz (v závislosti na délce vodičů)
- tento problém lze částečně obejít využitím složitých číslicových modulací (např. OFDM)

Optická přenosová cesta

- optická vlákna využívají absolutního odrazu světla na rozhraní dvou prostředí s odlišným indexem lomu
- **index lomu** (≥ 1) představuje poměr mezi rychlostí šíření světla ve vakuu a v daném prostředí

$$n = \frac{c}{v}$$

- lom světla na rozhraní dvou prostředí s různým indexem lomu popisuje **Snellův zákon lomu**:

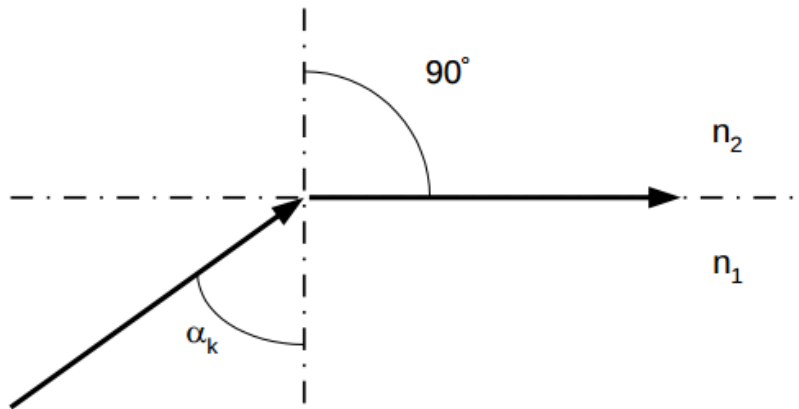


$$n_1 \cdot \sin \alpha_1 = n_2 \cdot \sin \alpha_2$$

- vstupní úhel, pro nějž je výstupní úhel roven 90° se nazývá **kritický (Brewsterův) úhel**

$$\alpha_k = \arcsin\left(\frac{n_2}{n_1}\right)$$

- pro $\alpha_1 > \alpha_2$ dochází k totálnímu odrazu světla na rozhraní



- důležitým parametrem vlákna je numerická apertura

$$NA = n_0 \cdot \sin\theta_\alpha$$

- pro vstup paprsku ze vzduchu odpovídá numerická apertura sinu maximálního vstupního úhlu

Optická vlákna

- skleněná X plastová

- standardně pouze spojení typu bod-bod
- galvanické oddělení komunikujících uzlů
- vysoká odolnost vůči elektromagnetickým vlivům
- obtížný odposlech
- extrémně vysoká přenosová kapacita
- obtížné spojování (konektorování, sváření)
- jednovidová a mnohavidová
- jednovidová vlákna jsou skleněná s velmi malým průměrem jádra (do 10 μm)
 - šíří se v nich „jediný“ paprsek
- mnohavidová vlákna jsou skleněná či plastová
 - různé paprsky se šíří různě dlouhou cestou
 - skoková či gradientní změna indexu lomu
- používají se zejména ty vlnové délky, na nichž je nejnižší útlum (absorbce)
 - skleněná vlákna - 850 nm, 1300 nm, 1500 nm
 - plastová kolem 650 nm – 680 nm
- útlum vláken je v závislosti na provedení, technologii výroby a vlnové délce světla v rozsahu jednotek až stovek dB/km
- omezení přenosové kapacity vlivem **disperze** (různé příčiny)
- vyšší cena spojů, cena samotného kabelu je již srovnatelná s metalickým spojem (zejména u plastových vláken)

Bezdrátová přenosová cesta

Optická

Infračervená komunikace

- nízký dosah (jednotky až desítky metrů, s optikou i více)
- nízká přenosová rychlost
- IrDA, různé „dálkové ovladače“
- používá se i v průmyslových aplikacích pro parametrizaci a sběr dat (např. místní odečet elektroměrů)

Laserová komunikace

- úzce směrová
- velký dosah a vysoké přenosové rychlosti
- utajení vojenské aplikace (družice)

Rádiová

- využívá velkého rozsahu frekvencí podle požadavků aplikací
- jako rádiové vlny označujeme elmag. záření s frekvencí do cca 300 GHz
- přísně regulováno státy a mezinárodními institucemi
- relativně snadný odposlech
- běžné rozsahy rádiových vln:
 - velmi dlouhé vlny (VDV, ang. **VLF** – very low frequency)
 - 3 – 30 kHz
 - dlouhé vlny (DV, ang. **LF** – low frequency)
 - 30 – 300 kHz
 - střední vlny (SV, ang. **MF** – medium frequency)
 - 300 kHz – 3 MHz
 - Nejlépe se odráží od ionosféry
 - krátké vlny (KV, ang. **HF** – high frequency)
 - 3 – 30 MHz
 - velmi krátké vlny (VKV, ang. **VHF** – very high frequency)
 - 30 – 300 MHz
 - ultra krátké vlny (UKV, ang. **UHF** – ultra high frequency)
 - 300 MHz – 3 GHz
 - super krátké vlny (SKV, ang. **SHF** – super high frequency)
 - 3 – 30 GHz

Šíření elmag. vln prostředím

- výkonová hustota elmag. pole obecně klesá se čtvercem vzdálenosti od zdroje
- vlnová délka a frekvence spolu souvisí prostřednictvím rychlosti světla (obecně elmag. vln) v daném prostředí
- parametry šíření v praxi závisí na frekvenci
- v pásmech **VLF a LF** je nízký útlum velký dosah
 - snadné pokrytí velkého území (vlnovod mezi zemí a ionosférou)

- nízký počet kanálů, vysoká úroveň rušení, velké antény
- používá se pro navigační systémy
- v pásmu **MF** dominuje šíření povrchovou vlnou
 - kolem povrchu země do výše srovnatelné s délkou vlny
 - dosah povrchové vlny klesá s rostoucí frekvencí
 - v noci se prostorová vlna odráží od ionosféry (ve dne je jí pohlcena)
 - kolísání úrovně signálu
- v pásmu **HF** se šířící se vlna odráží od země a od ionosféry
 - několikanásobné odrazy
 - lepší podmínky v noci
 - šíření závisí na frekvenci, fázi slunečního cyklu a dalších parametrech
 - na určitých frekvencích lze s dostatečným výkonem dosáhnout spojení téměř s libovolným místem na zemi
- v pásmu **VHF** se probíhá šíření přímou vlnou
 - do vzdálenosti rádiového horizontu (uplatňuje se ohyb)
 - začínají se uplatňovat odrazy a ohyby na velkých překážkách (pohoří ...)
- v pásmu **UHF** opět šíření přímou vlnou
 - do vzdálenosti rádiového horizontu (uplatňuje se ohyb)
 - i mnohanásobné odrazy od překážek rozměrově srovnatelných s délkou vlny
- v pásmu **SHF** se šíření začíná blížit šíření světla
 - ostré stíny za překážkami
 - velký vliv počasí (déšť, sníh)

Regulace rádiové komunikace

- **World Radiocommunications Conference (WRC)**
 - jednání na úrovni států
 - výsledky jsou zahrnuty v radiokomunikačním řádu
- radiokomunikační řád definuje:
 1. způsob využití frekvenčního spektra
 2. rozdělení pásem
 3. využití frekvenčních rozsahů jednotlivými službami
 4. zásady pro koexistenci rádiových zařízení na shodných nebo blízkých frekvencích
 5. koordinuje přidělování frekvenčního spektra novým zařízením a službám
- regulace rádiové komunikace v ČR
 - **ČTU - Český telekomunikační úřad**
 - odbor správy kmitočtového spektra
 - národní kmitočtová tabulka – 9 kHz – 105 GHz
- **ISM** (Industrial, Science and Medical) pásma (!!!)
 - vyhrazené frekvenční rozsahy, jejichž využití je za dodržení určitých podmínek volné (868 MHz, 2.4GHz)
 - maximální izotropně vyzářený výkon (EIRP)
 - poměr vysílání/příjem (klíčovací poměr)
 - použitá modulace a přístupová metoda
 - atd.

Přenosový kanál

přímý datový signál reprezentovaný obdélníkem pro přenos nevhodný

- SS složka (problém rozlišení sekvencí 0/1)
- problém při galvanickém oddělení trafem)
- není zaručen výskyt změn v signálu (dlouhé sekvence), problém se synchronizací
- výkonové aspekty

kódy z pohledu počtu úrovní signálu

- unipolární signály
- bipolární signály +/-
- 3-stavové
- více-stavové

zpráva - jakákoliv posloupnost rozlišitelných znaků

symboly - rozlišitelné prvky ve zprávě (grafické znázorněné znaky, elementární signály)

abeceda - množina všech symbolů (elementárních signálů)

signál - signál je fyzikální veličina, která nese informaci a slouží pro účely přenosu, záznamu a transformaci informace. Signály dělíme na spojité a diskrétní

kódování - transformace zprávy vyjádřené pomocí jedné abecedy na zprávu vyjádřenou pomocí druhé abecedy

informace - vztah mezi symboly zprávy a okolním světem

data - jakékoli vyjádření (reprezentace) skutečnosti, schopné přenosu, uchování, interpretace či zpracování

Nejčastěji používaná kódování signálu

NRZ (Not Return To Zero)

- úroveň signálu přímo odpovídá 1/0

RZ (Return To Zero)

- třístavový, polovina intervalu +1 při bitu 1, -1 při bitu 0, druhá polovina intervalu nulová.

NRZI (Not Return To Zero Inverted)

- 1-inverze signálu, 0-úroveň zůstává

PSK (Manchester)

- fázová modulace, uprostřed intervalu: 0-sestup signálu, 1-vzestup signálu
- každý bitový interval má tedy uprostřed změnu
- dvojnásobné pásmo oproti přímému kódování
- použití v Ethernetu
- **original data = clock (xor) manchester value**

DPSK (Diferenciální Manchester)

- 1-změna na začátku intervalu, 0-absence změny na začátku intervalu
- uprostřed intervalu změna vždy
- kóduje se změna/zachování úrovně posledního bitu (ne hodnota aktuálního bitu)
- použití v Token-Ring.

Základní typy chybových modelů pro reálné číslicové přenosové kanály (!!!)

„Bez paměti“:

- AWGN kanál
- BSC kanál
- BEC, BAC, ...

„S pamětí“

- Gilbert-Elliott 1960

AWGN kanál (Additive white Gaussian noise)

- (jediný) zdroj chyb v kanále je aditivní šum
 - širokopásmový (ideálně bílý)
 - normálně (Gaussovsky) rozložená amplituda
- nezohledňuje řadu typů chyb (únik, vícecestné šíření, interference, ...)
- použití
 - modely satelitních komunikací
 - šum pozadí v pozemských komunikacích (jako jeden ze vstupů do komplexnějšího modelu)

BSC kanál (Binary Symmetric Channel)

- binary symmetric channel with crossover probability p denoted by BSC_p
- channel with binary input and binary output and probability of error p
- \mathbf{X} is the transmitted random variable and \mathbf{Y} the received variable
- then the channel is characterized by the conditional probabilities:

$$P(Y = 0 | X = 0) = 1 - p$$

$$P(Y = 0 | X = 1) = p$$

$$P(Y = 1 | X = 0) = p$$

$$P(Y = 1 | X = 1) = 1 - p$$

BEC (Binary Erasure Channel)

- binary erasure channel with erasure probability P_e
- channel with binary input, ternary output, and probability of erasure P_e
- let \mathbf{X} be the transmitted random variable with alphabet $\{0, 1\}$
- let \mathbf{Y} be the received variable with alphabet $\{0, 1, e\}$, where e is the erasure symbol
- the channel is characterized by the conditional probabilities

$$P(Y = 0 | X = 0) = 1 - p$$

$$P(Y = e | X = 0) = p$$

$$P(Y = 1 | X = 0) = 0$$

$$P(Y = 0 | X = 1) = 0$$

$$P(Y = e | X = 1) = p$$

$$P(Y = 1 | X = 1) = 1 - p$$

BAC (Binary Assymmetric Channel, též Z-kanál)

- Z-channel (or a binary asymmetric channel) is a channel with binary input and binary output
- crossover $1 \rightarrow 0$ occurs with nonnegative probability p , whereas the crossover $0 \rightarrow 1$ never occurs
- př. datová media
- in other words, if \mathbf{X} and \mathbf{Y} are the random variables describing the probability distributions of the input and the output of the channel, respectively, then the crossovers of the channel are characterized by the conditional probabilities:

$$P(Y = 0 | X = 0) = 1$$

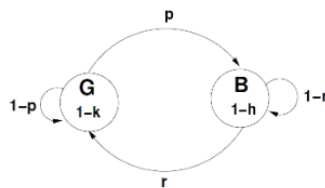
$$P(Y = 0 | X = 1) = p$$

$$P(Y = 1 | X = 0) = 0$$

$$P(Y = 1 | X = 1) = 1-p$$

Gilbert-Elliott 1960

- used for describing burst error patterns in transmission channels, that enables simulations of the digital error performance of communications links
- it is based on a Markov chain with two states G (for good or gap) and B (for bad or burst)
- pravděpodobnost chybného přenosu bitu závisí na výsledku přenosu bitu předchozího („závislé ztráty“)
- modelujeme pomocí dvoustavového Markovova řetězce



- **p** pravděpodobnost přechodu ze stavu Good do stavu Bad
- **r** pravděpodobnost přechodu ze stavu Bad do stavu Good
- **1-k** pravděpodobnost chybného přenosu bitu v Good stavu (obvykle =0)
- **1-h** pravděpodobnost chybného přenosu bitu v Bad stavu (např. 0.5)

Modulace

z hlediska modulované veličiny

- amplitudová, frekvenční, fázová, šířková

z hlediska nosného signálu

- s harmonickým n.s., s impulsním n.s.

dle modulačního signálu

- analogový, číslicový (binární, vícestavový)

Modulace pro přenos dat -> pro sériový přenos binární posloupnosti

- amplitudová modulace **ASK** (Amplitude-shift keying)
- kmitočtová modulace **FSK** (Frequency-shift keying)
- fázové modulace **PSK** (Phase-shift keying)
 - (**BPSK** – Binary phase-shift keying)
 - kvadrSaturní fázová modulace **QPK** (Quadrature phase-shift keying); 4 logické stavy
 - 8 -PSK; osmistavová modulace
- kvadraturní amplitudová modulace **QAM** (Quadrature amplitude modulation)

Bezpečnost dat

Kódové zabezpečení přenosu dat

- popis přiřazení kódových slov jednotlivým zprávám (kódová kniha).
- kódové slovo je posloupnost znaků použité abecedy
- abeceda je množina znaků (např. binární abeceda $Z_2 = \{0, 1\}$)
- minimální délka kódového slova: $N^*(x) = -\log_2(P(x))$ [bit]
- vlastnosti kódu:
 - prosté kódování: různým zprávám odpovídají různá kódová slova
 - jednoznačná dekódovatelnost: ze znalosti zakódované zprávy lze jednoznačně určit zprávu zdrojovou
 - kód $K : A \rightarrow B$ musí být prostým zobrazením
- detekce chyb:
 - množinu všech slov rozdělíme na slova kódová a slova nekódová
 - t-násobná chyba změní kódové slovo na nekódové, pokud se dvě kódová slova liší ve více než t znacích
 - Hammingova vzdálenost je počet znaků ve kterých se dvě kódová slova liší
 - Hammingova vzdálenost kódu d je nejmenší z nich
- kód odhaluje t-násobné chyby, pokud je Hammingova vzdálenost kódu $d > t$
- kód opravuje t-násobné chyby, pokud je Hammingova vzdálenost kódu $d > 2t$

Prefixový kód

- žádný symbol jeho kódové abecedy není předponou (začátkem) jiného symbolu abecedy

Př.:

$\{1, 21, 22, 231, 232, 24, 35, 535, 7\}$ je prefixový kód

$\{1, 21, 22, 221, 222, 24, 35, 355, 7\}$ není prefixový kód

Kraftova nerovnost

- z n znaků lze sestavit prefixový kód s délkami kódovaných slov d_1, d_2, \dots, d_r právě když

platí Kraftova nerovnost: $n^{-d_1} + n^{-d_2} + \dots + n^{-d_r} \leq 1$

Př.: 0: 00, 1: 01, 2: 1xx, 3: 1xx, 4: 1xx, 5: 1xx, 6: 1xx, 7: 1xx, 8: xxxx, 9: xxxx

$2 \cdot 2^{-2} + 6 \cdot 2^{-3} + 2 \cdot 2^{-4} = \frac{22}{16} > 1$ - prefixový kód nelze sestavit

0: 00, 1: 01, 2: 100, 3: 1010, 4: 1011, 5: 1100, 6: 1101, 7: 1110, 8: 11110, 9: 11111

$2 \cdot 2^{-2} + 1 \cdot 2^{-3} + 5 \cdot 2^{-4} + 2 \cdot 2^{-5} = \frac{32}{32} = 1$ - prefixový kód lze sestavit

Zabezpečující lineární kódy

Lineární paritní kód

- sudý, lichý
- např. pro sudou paritu platí, že součet mod2 všech prvků slova včetně paritního je 0 (= „doplnění paritního znaku na sudý počet jedniček“)
- lze detekovat lichý počet chyb

- příčná a podélná parita - při přenosu bloku dat

Lineární cyklické kódy

- přenáší se kódové slovo a zbytek po dělení tohoto slova generujícím polynomem (musí být primitivní a neredukovatelný)
- na přijímací straně se celá přijatá sekvence opět dělí generujícím polynomem
- při bezchybném přenosu je zbytek 0
- př.: Cyclic Redundancy Codes (CRC):

Kód	generující polynom $g(x)$	stupeň $g(x)$
CRC – 12	$x^{12}+x^{11}+x^3+x^2+x+1$	12
CRC – 16	$x^{16}+x^{15}+x^3+x^2+1$	16
CRC – CCITT	$x^{16}+x^{12}+x^5+1$	16
CRC - 32	$x^{32}+x^{26}+x^{23}+x^{22}+x^{16}+x^{11}+x^{10}+x^8+x^7+x^5+x^4+x^2+x^1+1$	32

Cyclic Redundancy Code (CRC)

- cíl - maximalizovat zabezpečení, minimalizovat bity navíc
- princip - přidat k bitů redundantních dat k n -bitové zprávě
- n -bitová zpráva je reprezentována jako polynom n -tého stupně, kde každý bit odpovídá příslušnému koeficientu v polynomu
- chyba je detekována pokud $C(x)$ nedělí $E(x)$ (chybový polynom)
- (neboli: je-li $E(x)$ násobek $C(x)$, chyba není detekována)
- jaké chyby lze detekovat?
 - všechny jednonásobné chyby, pokud x^k a x^0 nemají nulové koeficienty
 - všechny dvojnásobné chyby, pokud má generující polynom alespoň 3 členy
 - všechny chyby liché násobnosti, pokud generující polynom obsahuje $(x + 1)$
 - všechny souvislé chybové sekvence délky $< k$, pokud $C(x)$ obsahuje nenulový konstantní člen
 - většinu souvislých chybových úseků délky k

Oprava (korekce) chyb

- příklad:
 - opakovací kód délky 3 – 000, 111 - jsou kódová slova
 - 001, 010, 100, 110, 101, 011 - nejsou kódová slova
 - Hammingova vzdálenost kódu = 3 kód opravuje jednonásobné chyby
- triviální implementace – většinová logika
 - 001, 010, 100 opraveno na 000
 - 110, 101, 011 opraveno na 111
- při výskytu 2 chyb
 - detekce je možná
 - oprava bude chybná
- lze využít
 - buď vyšší redundanci (např. opakovací kód délky 5, opraví dvě chyby)
 - nebo lépe jiné třídy kódů (Hammingovy, BCH, konvoluční, ...)
 - poskytují lepší infomační poměr pro daný počet oprav

Úvod do kryptografie (šifrování)

Kryptologie

- kryptografie: věda zabývající se šifrováním informace
- kryptoanalýza: věda, zabývající se dešifrováním informace

Šifrovací algoritmus

- funkce sestavená na matematickém (dříve příp. mechanickém) základě
- provádí samotné šifrování a dešifrování dat

Šifrovací klíč

- vstupní parametr (de)šifrovacího algoritmu
- vždy dostaneme nějaký výsledek - jeho správnost závisí na zadaném klíči
- délka klíče ovlivňuje časovou náročnost při útoku hrubou silou

Šifry z hlediska cíle procesu

- obousměrné - při znalosti správného klíče lze dešifrovat výsledek a získat tak opět originál
- jednosměrné - ukládání hesel, výtahy zpráv, digitální podpisy

Šifry z hlediska směrovosti

- šifrování s privátním klíčem (symetrické či se symetrickým klíčem)
 - stejný klíč pro zašifrování i dešifrování zprávy
 - použití je omezeno na případy, kdy účastníci znají daný klíč předem
 - př.: DES, IDEA, Skipjack, Blowfish, Twofish, CAST5
- šifrování s veřejným klíčem (asymetrické či s asymetrickým klíčem)
 - dva klíče: privátní a veřejný
 - cokoli zašifrováno jedním klíčem, lze dešifrovat pouze druhým klíčem a naopak
 - kdokoli zprávu zašifruje veřejným klíčem
 - lze dešifrovat pouze pomocí privátního klíče
 - př.: RSA, ElGamal, DSA, Diffie-Hellman
- hybridní šifrování
 - kombinace obou výše zmíněných, př. dočasná komunikaci aplikací typu klient/server

Výtahy zpráv (message digest, kryptografický kontrolní součet)

- jednosměrné algoritmy (hash)
- z výsledku nejsme schopni obnovit originál
- konstantní a poměrně krátká délka výsledného kódu (typ. 128 bitů)
- vlastnosti ideální kryptologické hashovací funkce
 - ze vstupu proměnné délky vytváří malou hodnotu
 - ze stejného vstupu vytváří vždy stejný výstup
 - každé výsledné hodnotě by mělo odpovídat více vstupních kombinací
 - algoritmus by neměl být snadno odvoditelný či invertovatelný
 - malá změna na vstupu má za následek velké změny ve výstupu
- aplikace: zabezpečení dokumentů (ftp), dig. podpis
- příklady: MD2, MD5, SHA, HAVAL, SNEFRU, RIPEMD160

Digitální podpis

- výtah zprávy zašifrovaný privátním klíčem autora dokumentu

- klíč distribuován spolu s dokumentem
- držitel příslušného veřejného klíče je schopen dešifrovat zakódovaný výtah zprávy a porovnat ho s výtahem, který vytvoří z obdrženého dokumentu
- digitální podpis zajišťuje tři funkce
 - integritu
 - autentifikaci (kdo zprávu podepsal)
 - nepopíratelnost (autor nemůže v budoucnu zapřít, že zprávu podepsal)
- zpráva (soubor) bude čitelná (použitelná) i v případě, že nemáme příslušné nástroje pro ověření její pravosti

Základní princip komunikací

Základní typy datových přenosů

Podle směru přenosu

- jednosměrný (**simplex**)
- obousměrný střídavý (poloviční duplex/**half-duplex**)
- obousměrný současný (plný duplex/**full-duplex**)

Podle počtu současně využitých kanálů

- **sériový**
 - bity (symboly) jsou přenášeny v čase postupně
- **paralelní**
 - bity (symboly) jsou přenášeny v čase po skupinách

Podle způsobu synchronizace (v základním pásmu)

- paralelní synchronní přenos
- paralelní asynchronní přenos
- sériový asynchronní (arytmický) přenos
- sériový synchronní přenos
 - buď vyhrazený kanál pro přenos hodin
 - častěji je synchronizační signál zakódován přímo do datové posloupnosti (kanálová kódování – např. Manchester)
 - stačí jediný kanál
 - je třeba vyšší šířka pásma
 - technicky složitější synchronizace přijímače

Podle využitého frekvenčního pásma

- přeložené pásmo se používá, protože:
 - umožňuje efektivní využití kapacity kanálu
 - automaticky v sobě zahrnuje frekvenční multiplex
 - je typické pro rádiové přenosy, ale využívá se i jinde
 - PLC komunikace, xDSL
 - digitální kabelové rozvody

Sdílení kapacity kanálu

- metody umožňující rozdělit jeden fyzický kanál na více kanálů logických (multiplexování)
- frekvenční multiplex (**FDM**)

- šířka pásma fyzického kanálu je rozdělena na požadovaný počet subkanálů
- využití subkanálu lze dosáhnout vhodnou modulační technologií
- může být jiná pro jednotlivé subkanály
- překrývání spekter sousedních subkanálů komplikuje demodulaci
- mezery mezi nimi snižují přenosovou kapacitu
- rozhlasové vysílání – PSTN + ISDN + ADSL
- frekvenční multiplex (**FDM**) v optických přenosech
 - elektrické multiplexování
 - vše se realizuje elektricky a výsledným součtovým signálem se moduluje zdroj záření
 - vyžaduje vysokou linearitu zdroje
 - optické multiplexování (vlnový multiplex - WDM)
- časový multiplex (**TDM**)
 - kapacita kanálu je postupně využívána pro přenos dat jednotlivých subkanálů
 - obvykle statické přiřazení časových slotů
 - typické pro telekomunikační sítě
 - např. rozhraní typu E1 – 2 Mbit/s, 32 subkanálů po 64 kbit/s
- statistický časový multiplex (**STDM**)
 - v případě, kdy je konstantní přiřazení časových slotů neefektivní
 - např. multiplexování programových toků v DVB
 - podobnou funkci implementují MAC algoritmy
 - má dodatečnou režii spojenou s identifikací a přiřazením časových slotů jednotlivým subkanálům
- kombinovaný časový a frekvenční multiplex
 - spojuje obě metody
 - typickým příkladem jsou sítě GSM
 - 8 časových slotů na jeden FDM subkanál
- kódový multiplex
 - modifikace vybraného parametru signálu podle předem daného (obvykle pseudonáhodného kódu)
 - komunikace v rozprostřeném spektru
 - DSSS, FHSS
 - jednotlivé kanály tak v totéž čase sdílejí frekvenční pásmo
 - dekódování je založeno na ortogonalitě pseudonáhodných sekvencí
 - WiFi, Bluetooth
- prostorový multiplex (**SDM**)
 - tento pojem se používá poměrně zřídka
 - je založen na omezeném fyzickém dosahu
 - tzn. umožňuje současné využití téhož frekvenčního pásma a kódu v jiné lokalitě
 - typický především v rádiových systémech
 - v principu i metalické vedení či optické vlákno
 - přeslech při špatném multiplexování

Topologie fyzické vrstvy

- sběrnice, hvězda, kruh, strom existují i další topologie (strom-hvězda, mříž ...)
- některé jsou využívány pouze ve speciálních aplikacích

Adresace na linkové vrstvě

1. adresace uzlů (node oriented addressing)

- **MAC** adresa
- specifikuje, komu je linkový rámec určen a kdo je odesilatelem
- v některých systémech stačí pouze adresa příjemce (řízení Master – Slave)
- některé adresy či jejich rozsahy mohou být vyhrazeny pro zvláštní účely (broadcast, multicast, adresace v síťové vrstvě ...)

2. adresace zpráv (message oriented addressing)

- typická pro systémy, kde jsou rámce vysílány do sítě (**broadcast**)
- identifikuje obsah rámce (často se proto nazývá identifikátor)
- neříká nic o příjemci
 - tím jsou obvykle všechny uzly sítě, které mají o data v rámci zájem
 - všechny uzly tedy přijímají současně

3. adresace polohou

Řízení přístupu k médiu

- jedná se vlastně o řízení sdílení komunikačního kanálu
 - obvykle časové
 - časové sloty však nejsou obvykle přiřazeny konstantně
- současný přístup více uzlů vede ke kolizi
 - důsledkem je ztráta přenášené informace
- obecně existují dva základní přístupy (!!!)
 - **deterministické**
 - zde kolize vůbec nenastávají
 - **stochastické** (náhodným přístupem)
 - kolize nastat může a protokol s ní počítá
 - někdy se přidává další kategorie, a to pro systémy využívající CDMA
 - do určitého bodu (počtu současně vysílajících uzlů) pracují deterministicky
 - při jeho překročení (vyšší úroveň šumu) již vznikají kolize (nežádoucí režim)

Deterministické metody (!!!)

- Master-Slave

- vyhrazený uzel (**Master**) se dotazuje uzlů typu **Slave**
 - ty nesmí samostatně vysílat
 - komunikace probíhá pouze mezi uzlem Master a jednotlivými uzly (Slave)
- nevýhodami jsou
 - závislost komunikačního cyklu na počtu uzlů
 - závislost na výpadku uzlu Master
- výhodou je velmi jednoduchá implementace
- často využívá především u systémů s nižší datovou propustností a tam, kde daný typ komunikace odpovídá požadavkům aplikace
- průmyslové distribuované systémy

- Token Passing

- jednotlivé uzly jsou rovnocenné

- oprávnění k vysílání má pouze držitel pověření (**token**)
- to si uzly předávají v kruhu mezi sebou
- vlastnictví pověření je obvykle časově omezeno
- nevýhodami jsou
 - obvykle dlouhý čas na zformování kruhu při ztrátě pověření nebo při spuštění sítě
- výhodou je nezávislost na jediném uzlu
- **TDMA**
 - přesně určené časové sloty
 - využívá se v aplikacích s vysokými nároky na bezpečnost – X by wire
- **Delegated Token**
 - opět existuje vyhrazený uzel
 - někdy se nazývá **arbitr** (bus arbiter)
 - vysílání speciální výzvy, umožňující ostatním uzlům vyslat rámeček nebo rámce
 - obvykle mohou přijímat současně všechny uzly sítě (využívá se adresace zpráv)
 - nevýhodami jsou – závislost na uzlu arbitra

Stochastické metody

- jedním z nejstarších byl protokol **ALOHA** (universita Hawaii)
- dnes se využívají varianty **CSMA (Carrier Sense Multiple Access)**
- uzly jsou obvykle rovnocenné
- chtějí-li začít vysílat, čekají na volný kanál (**Carrier Sense**), poté mohou začít vysílat
- může dojít ke kolizi (**CS** vede k synchronizaci)
- ta se může rozpoznat nebo nikoliv (pak jsou data ztracena)
- **CSMA/CD (... with Collision Detection)**
 - kolize jsou detekovány
 - po kolizi zúčastněné uzly čekají náhodnou dobu
 - tato doba je $T_a \cdot d$, kde
 - » T_a je konstanta závislá na technologii
 - » d je náhodně zvolené číslo s exponenciálně rostoucí horní mezí
- **CSMA/CR (... with Collision Resolution)**
 - kolize nejsou destruktivní a slouží k arbitráži mezi současně vysílanými rámci
 - rámeček s nejvyšší prioritou je odvyslán, ostatní pokus opakují
 - typické pro sběrnici CAN
- **CSMA/CA (... with Collision Avoidance)**
 - převážně v bezdrátových sítích
 - zde nemusí být kolize rozpoznána
 - po detekci volného kanálu se čeká po náhodnou dobu a pokud je kanál ještě volný, uzel smí vysílat
 - často se kombinuje s tzv. rezervací kanálu
 - uzel si rezervuje určitou dobu pro své vysílání, ostatní předpokládají, že je po tuto dobu obsazen (např. WiFi)

Spolehlivá a nespolehlivá služba

Nespolehlivá služba

- doručení všech rámců či paketů není zaručeno

- může provádět kontrolu správnosti obsahu
- při zjištění chyb se data zahodí
- přenos se neopakuje
- příkladem je Ethernet

Spolehlivá služba

- zabezpečuje kompletní doručení všech rámců či paketů bez chyb
- provádí kontrolu správnosti obsahu
- s využitím redundantních informací přidanych k datům
- při zjištění chyb se přenos opakuje (nebo se chyby opraví)
- počet opakování je obvykle omezen
- příkladem je USB (všechny typy přenosů mimo isochronního)

Dopředná korekce (**FEC** – Forward Error Correction)

- různé kódy podle charakteru dat
 - blokové (Reed-Solomonovy, BCH, ..)
 - proudové (především konvoluční)
- často kombinováno s prokládáním
 - vyšší odolnost vůči skupinovým chybám
- využívá se pro:
 - simplexní kanály - např. DVB, není možné žádat o opakování dat
 - kanály s vysokou chybovostí - např. PLC
 - isochronní datové toky - streamování multimédi

Automatic Repeat reQuest (**ARQ**)

- algoritmy detekce chyb
- v případě chyby je zdroj požádán o opakování přenosu

Stop and Wait ARQ

- po odeslání dat je očekáváno potvrzení (**ACK**)
- pokud není přijato do určité doby, přenos se opakuje
 - neefektivní pro kanály s vysokým zpožděním
 - potvrzení se může ztratit - tatáž data vyslána 2x
- v případě dočasného zvýšení zpoždění může být potvrzení přiřazeno špatnému rámcu
- lze řešit číslováním rámců a potvrzení

Go-Back-N ARQ

- **datové rámce (pakety) obsahují pořadové číslo**
- vysílající uzel smí odeslat až N rámců (paketů), aniž by obdržel potvrzení
 - N je velikost vysílacího okénka
- potvrzení obsahuje pořadové číslo posledního správně přijatého rámce (paketu)
 - chybné (či chybějící) a následující jsou ignorovány
- po odeslání N rámců (paketů) vysílač vyhodnotí pořadové číslo posledního přijatého potvrzení a pokračuje ve vysílání následujícího rámce (paketu)
 - rozsah pořadového čísla musí být $> N$
- **všechny rámce (pakety) odeslané po chybě jsou opakovány**

Selective Repeat ARQ

- datové rámce (pakety) obsahují pořadové číslo
- vysílající uzel smí odeslat až N rámců (paketů), aniž by obdržel potvrzení
 - N je velikost vysílacího okénka
- přijímač přijímá všechny bezchybně doručené rámce i po výskytu chyby až do počtu M
 - M je velikost přijímacího okénka
- potvrzení obsahuje pořadové číslo prvního chybného rámce (paketu) nebo dalšího v pořadí (nenastala-li chyba)
- vysílač vyhodnotí pořadové číslo v posledním přijatém potvrzení a pokračuje vysíláním rámce (paketu) s tímto číslem a následujících (max. N, **bezchybné se neopakují**)
 - rozsah pořadového čísla musí být $N + M$

Přepínání okruhů X přepínání paketů

Přepínání okruhů (circuit switching)

- příklad: klasická telefonie, ale i např. klasický rozhlas, TV
- mezi příjemcem a odesílatelem vzniká (fyzicky) přímá, souvislá cesta, komunikace probíhá v reálném čase
 - představa: od odesílatele vede až k příjemci vyhrazená „roura“
- přenášená data se nikde nehromadí
- výhodné pro kontinuální přenosy (konstantní datový tok)
- vhodné pro multimediální formáty (živý zvuk a obraz)
- data nemusí být příjemci explicitně adresována
 - příjemce je jednoznačně určen: ten, kdo je na druhém konci „roury“
- typické pro telekomunikační sítě (technologie PSTN – PDH, SDH ...)
 - dnes jsou i zde stále častěji využívány paketové sítě a virtuální okruhy (VoIP ...)

Přepínání paketů (packet switching)

- příklad: odeslání dopisu
- mezi příjemcem a odesílatelem nevzniká žádná souvislá vyhrazená cesta
 - na cestě od příjemce k odesílateli existují přestupní body, které si zásilku postupně předávají, a jsou schopny ji nakonec dopravit až k příjemci
 - přenášená data cestují podle principu „**store & forward**“
 - jednotlivé přestupní uzly nejprve přijmou celý přenášený blok dat (paket), a teprve pak jej předají dál
- není to v reálném čase
- přenášená data musí být explicitně adresována
 - musí nějak identifikovat příjemce
- výhodné pro přenosy s náhodnými požadavky, např. přenosy souborů
- nevhodné pro izochronní přenosy (QoS)
- typické pro počítačové sítě
 - často se však v některé z vyšších vrstev (obvykle transportní) emuluje spojení – vytváří se virtuální okruh

Spojovaná a nespojovaná služba

Nespojovaná služba

- před vysláním dat není třeba budovat „spojení“ s druhou stranou
- jednotlivé pakety jsou odesílány a zpracovávány sítí nezávisle
- mohou k cíli dorazit různými cestami
 - může dojít k prohození pořadí při příjmu

Spojovaná služba

- nejprve je třeba otevřít „spojení“ s druhou stranou
- poté lze odesílat data
- často existuje mechanismus na řízení datového toku
- v případě prohození pořadí paketů v nižších protokolových vrstvách je zajištěno jeho obnovení

Internetworking

propojování distribuovaných systémů - lze si pod ním představit propojování jednotlivých síťových segmentů, podsítí i celých sítí

Důvody pro propojování/segmentování sítí (!!!)

- potřeba přenosu dat mezi technologiemi různých parametrů
 - počítačové sítě
 - telekomunikační sítě
 - průmyslové distribuované systémy
- překonání technických omezení/překážek
 - např. dosah kabelových segmentů je omezený (10Base2: 185 metrů)
 - omezený je i počet uzlů, které lze připojit ke kabelovému segmentu
 - rozbočování některých typů fyzických médií je obtížné či nemožné, realizuje se elektronicky prostřednictvím rozbočovacích prvků
 - týká se zejména kroucené dvoulinky a optických vláken
 - lze je použít jako dvoubodové spoje, mnohdy pouze jednosměrné
- zpřístupnění vzdálených zdrojů
 - např. přístup ke vzdáleným FTP archivům, WWW serverům
 - využití výpočetní kapacity vzdálených počítačů
- zvýšení fyzického dosahu poskytovaných služeb
 - užitná hodnota některých služeb je tím větší, čím větší je její pokrytí (např. elektronická pošta, Internetová telefonie, vyhledávací služby, sociální sítě, ...)
- optimalizace fungování sítí (na různých vrstvách OSI)
 - snaha omezit tok dat pouze tam, kde je třeba
 - zvýšení spolehlivosti prostřednictvím redundance spojů
 - optimalizace směrovacích strategií
 - multicastové vysílání
 - zajištění kvality služby

Propojovací prvky

Pojmenování propojovacích zařízení

- podstatné je, jakým způsobem pracuje propojovací prvek:
 - může pracovat na úrovni fyzické až aplikační vrstvy
 - podle toho se také pojmenovává
- podle vrstvy OSI modelu, ve které pracují:
 1. fyzická vrstva: opakovací (repeater), rozbočovač, u ethernetu se mu říká **hub**
 2. linková vrstva: most (**bridge**), přepínač, (**switch**)
 3. síťová vrstva: směrovač (**router**)
 4. aplikační vrstva: brána (**gateway**)
- propojovací prvek musí rozumět protokolům vrstvy v níž pracuje a všech vrstev nižších
- pro vyšší protokolové vrstvy je jeho funkce transparentní a má na ně pouze nepřímý vliv (zpoždění) - jinak je „neviditelný“
- někdy (u některých technologií téměř vždy) je propojovací prvek viditelný i na vyšších vrstvách
 - typické využití je pro konfiguraci jeho chování jako propojovacího prvku
 - např. prostřednictvím webového rozhraní nebo ssh
 - domácí ADSL směrovač lze téměř vždy konfigurovat prostřednictvím webového rozhraní

Opakovač (Repeater)

- pracuje ve fyzické vrstvě
- je to pouze digitální zesilovač, který zesiluje a znovu tvaruje přenášený signál
 - kompenzuje zkreslení, útlum a další vlivy komunikačního kanálu
- pracuje s jednotlivými bity či symboly
 - tedy s elementy přenášenými na úrovni fyzické vrstvy
- opakovací „nevnímá“, že určité skupiny bitů patří k sobě a tvoří rámec nebo určité pole rámce (např. adresu či kontrolní součet)
 - nedokáže rozpoznat adresu odesílatele ani příjemce dat (rámce)
 - nemá k dispozici informace, které by mu umožnily měnit jeho chování podle toho, jaká data skrz něj prochází
- ke všem bitům se musí chovat stejně
- chování opakovacího
 - všechny datové bity (symboly) přijaté z daného fyzického segmentu sítě rozesílá („opakuje“) do všech stran (do všech ostatních segmentů, ke kterým je připojen)
 - nemá informace pro rozhodnutí, co je a co není třeba opakovat
 - funguje v reálném čase
 - až na malé zpoždění ve vnitřních obvodech
 - nemá žádnou vnitřní paměť pro uložení dat
 - může propojovat jen segmenty se stejnou přenosovou rychlostí
 - ale s jinak různými vlastnostmi
 - metalické vedení X optika
 - je nezávislý na protokolech linkové vrstvy
 - hodnoty některých parametrů ale mohou být ovlivněny funkčními principy protokolů spojové vrstvy

- např. doba přepnutí vysílání-přijem
- existují tedy opakovače pro konkrétní síťové technologie, např. pro Ethernet (zde se také nazývají huby)
- počet segmentů, které opakovač propojuje, není apriorně omezen
- nevýhody opakovače
 - jsou to „hloupá“ zařízení, šíří do ostatních segmentů i komunikaci, která by mohla zůstat lokální
 - neví, co by mohl zastavit a nemusel šířit dál
 - plýtvají dostupnou přenosovou kapacitou

Most (Bridge) a přepínač (Switch)

- snaží se propojit komunikaci v jednotlivých propojovaných segmentech
- mosty typicky spojují 2 segmenty, přepínače více
- aby se mohly takto chovat, musí alespoň trochu rozumět přenášeným datům
 - potřebuje znát adresu příjemce a adresu odesílatele
- tu může poznat z hlavičky rámce
- pracují ve spojové vrstvě
 - musí znát její protokoly
 - musí respektovat algoritmus **MAC**
- rámce mohou být dočasně uloženy v propojovacím prvku, dokud neobdrží oprávnění k vysílání do cílového segmentu sítě
- implementují filtrování (**filtering**) a cílené předávání (**forwarding**)
 - filtrování
 - propojovací uzel dokáže poznat, které rámce jsou lokální ve zdrojovém segmentu a nešíří je dále
 - cílené předávání
 - rámce, které je třeba předat dále, jsou šířeny pouze do cílového segmentu a nikam jinam
 - díky těmto schopnostem lze významně „lokalizovat“ provoz
- aby dokázaly reagovat na adresy příjemce a odesílatele, nemohou již pracovat v reálném čase!!!
- musí nějakým způsobem ukládat data
 - celé rámce nebo alespoň jejich části (ty, z nichž lze poznat adresy)
- díky tomu mohou propojovat segmenty s různými přenosovými rychlostmi
 - např. přepínač na Ethernetu: 1 Gbit/s, 100 Mbit/s a 10 Mbit/s
- obecně s různými implementacemi fyzických vrstev
- vzniká dopravní zpoždění
 - jeho velikost může záviset na zátěži propojovacího prvku
 - v určitých situacích může dojít i ke ztrátě dat

Směrovač (Router)

- pracuje v síťové vrstvě
- analyzuje obsah paketu síťové vrstvy a podle cílové (výjimečně i zdrojové) adresy paket směřuje k cíli
- musí mít „povědomí“ o topologii celé sítě
 - to však nemusí být zase příliš vysoká, detailní znalost je třeba pouze o nejbližším okolí
- údaje jsou uloženy v tzv. směrovací tabulce

- statická nebo s dynamickou aktualizací (informace pro směrování mohou být předávány speciálními protokoly mezi směrovači)
- paket zaslaný směrovači je na linkové vrstvě odeslán na jeho MAC adresu kolik
- musí existovat cesta jak získat MAC adresu ze známé síťové adresy
- může spojovat podsítě se zcela odlišnými fyzickými a linkovými technologiemi
 - typické např. pro IP sítě
- nepracuje v reálném čase
- proměnné zpoždění, možné ztráty paketů

Brána (Gateway)

- pracuje ve vyšší než síťové vrstvě
 - často v aplikační, pak hovoříme o aplikační bráně
- „rozumí“ (alespoň částečně) všem přenášeným datům
- v systémech, kde je aplikační vrstva definována, mohou pracovat jako obecné propojovací prvky
 - např. jednosměrný přístup v reálném čase k datům z výrobního procesu pro management
- nejsou-li definovány obecné aplikační protokoly
 - brána podporuje jednu nebo několik aplikací
 - nebo jistou třídu aplikací - **http gateway**
- může propojovat systémy postavené na zcela jiných technologiích
 - např. mimo OSI model

Základní modely přenosu dat

Klient - Server

- komunikace mezi dvěma uzly distribuovaného systému
- role se mohou měnit
 - ve vztahu k jinému i k témuž uzlu
- uzel v roli Serveru poskytuje službu uzlu v roli Klienta
 - služební primitiva
- služba může být potvrzovaná i nepotvrzovaná

Producent - Konzument

- komunikace mezi dvěma a více uzly distribuovaného systému
 - informace je vysílána do sítě
 - konzumenti ji přijímají současně
- role se mohou měnit
 - ve vztahu k jinému i k témuž uzlu
- služba je obvykle nepotvrzovaná

Protokolový zásobník

TCP/IP a ISO/OSI Model

- TCP/IP je starší – neodpovídá plně ISO/OSI

- vývoj v 70. letech minulého století
- 1971 - ARPANET working group – financováno DARPA – spolupráce ITU, ISO
- 1978 – dokončeno
- 1980 – ARPANET přechází na **TCP/IP**
- 1983 – otevřená TCP/IP implementace v BSD Unixu
- další vývoj:

- **NSFNET (National Science Foundation)**

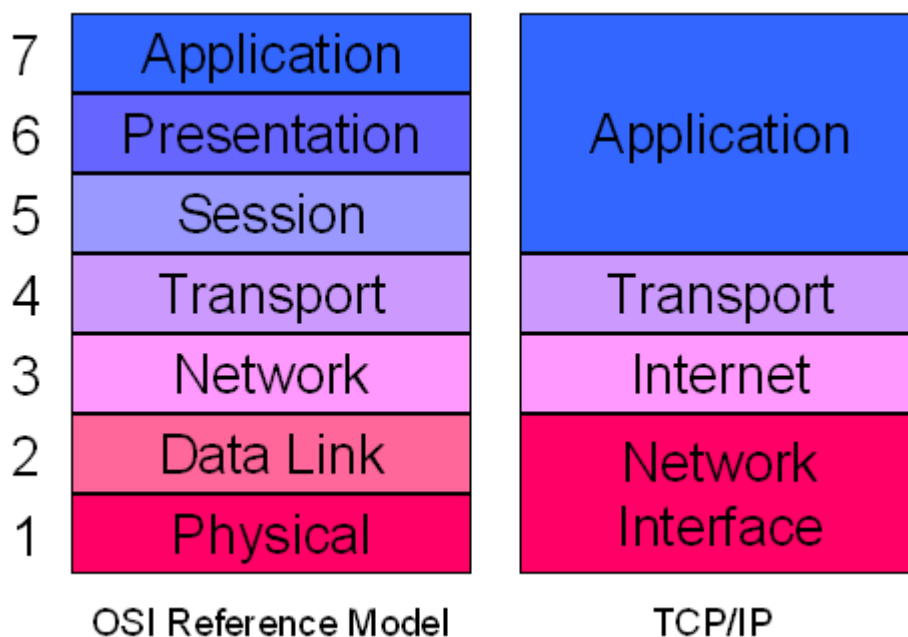
- univerzitní a výzkumná síť
- propojení s ARPANETem na Carnegie Mellon University
- uzly sítě propojeny prostřednictvím pronajatých linek
 - 1. generace – 56 kbit/s
 - 2. generace – 448 kbit/s
 - 3. generace (1989) – 1.544 Mbit/s (T1)
 - 1992 – migrace na T3 – 45 Mbit/s
- 1995 – skončila podpora vlády USA

Projekt Internet2

- <http://www.internet2.edu>

Komerční páteřní síť

- nebyl navržen dle OSI modelu, ale
 - Network interface and hardware ~ fyzická a spojová vrstva
 - Internetwork ~ síťová vrstva
 - Transport ~ transportní vrstva
 - Applications ~ relační až aplikační vrstva



Příklady protokolů jednotlivých vrstev

- nejedná se o kompletní sady protokolů TCP/IP
 1. Applications - **SMTP, Telnet, FTP, Gopher, ...**
 2. Transport - **TCP, UDP**
 3. Internetwork - **IP, ICMP, ARP, RARP**
 4. Network interface and Hardware - **Ethernet, Token-ring, FDDI, Wireless, ...**

Doručování

Unicast

- právě jeden příjemce
- jediná možnost pro spojově-orientované technologie

Broadcast

- limited broadcast: 255.255.255.255, ff0x::1
 - dosah je omezen směrovači
- directed broadcast: např. 169.47.255.255
 - směrován do cílové sítě

Multicast

- doručení vybrané skupině hostitelů
- adresy třídy D nebo multicastový prefix ff00::/8

Anycast

- nejbližší příjemce ze skupiny možných poskytovatelů služby (IPv6)

IP Adresy

IPv4 ... IPv6 adresy

- 4 resp. 16 bajtů
- správa IP adres je **regionální**
 - American Registry for Internet Numbers (**ARIN**, Ameriky + Afrika)
 - Reseaux IP Europeans (**RIPE**, Evropa, střední východ, Afrika)
 - Asia Pacific Network Information Centre (**APNIC**, Asie, Austrálie ...)

IPv4 adresa 10.0.0.15 (4 dekadická čísla v rozsahu 0 .. 255)

- IP address = <network number><host number>
- původně se používaly tzv. třídy adres
 - A – 2^7-2 (126) sítí, $2^{24}-2$ (16777214) hostitelů
 - B – $2^{14}-2$ (16382) sítí, $2^{16}-2$ (65534) hostitelů
 - C – $2^{21}-2$ (2097150) sítí, 2^8-2 (254) hostitelů

Původně 3 třídy adres

- nízká granularita
- plýtvání adresovým prostorem

Třída adres D – 1110...

- pro multicastovou komunikaci

Třída adres E – 11110...

- pro budoucí definice a experimenty

vylepšená správa IPv4 adres

- hranice položky <host number> definována 32bitovou maskou podsítě
- např. 255.255.252.0 ... $2^{10}-2$ uzlů v síti

Classless InterDomain Routing - CIDR

- IP adresa = <network number><subnetwork number><host number>
- **maska podsítě** v síti třídy B je např. 255.255.255.240
 - prvních 12 bitů definuje číslo podsítě, zbývajících 4 adresu hostitele

- $2^{12}-2$ (4094) možných podsítí, pouze 2^4-2 (14) hostitelů v podsíti
- statická definice (všechny podsítě mají shodnou velikost)
- definice s proměnnou délkou (různé velikosti podsítí)
- neviditelné pro uzly vně místní sítě, využívané jen uzly v rámci sítě
- lokální management

Vyhrazené IPv4 adresy

- netid, hostid=0: adresa sítě (147.229.0.0)
- netid=0, hostid: adresa uzlu (0.0.0.5)
- **255.255.255.255 limited broadcast** (omezená všeobecná adresa), neprochází přes router
- netid, hostid=11..1 directed broadcast (147.229.255.255), řízená všeobecná adresa
- **127.x.x.x loopback**, softwarová zpětnovazební adresa (komunikace mezi procesy počítače bez vysílání na síť)

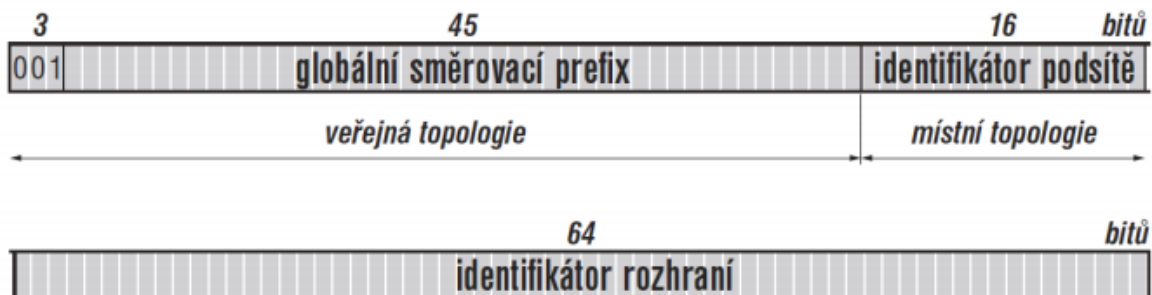
Privátní (neveřejné) IPv4 adresy

- 10.0.0.0: síť třídy A
- 172.16.0.0 až 172.31.0.0 - 16 sítí třídy B
- 192.168.0.0 až 192.168.255.0: 256 sítí třídy C
- nejsou směrovány ve veřejném Internetu

IPv6 adresy (16 bajtů)

- individuální (**unicast**)
- skupinová (**multicast**)
- výběrová (**anycast**)
- jedno rozhraní uzlu může (musí) mít několik adres
- zápis IPv6 adresy
 - 8 skupin po 4 šestnáctkových číslicích
 - např. fedc:ba98:7654:3210:fedc:ba98:7654:3210 linková ad
 - lze vynechat počáteční nuly
 - místo 0123:0000:0000:0000:fedc:ba98:7654:3210 lze psát 123:0:0:0:fedc:ba98:7654:3210
 - lze nahradit skupinu nul
 - místo 123:0:0:0:fedc:ba98:7654:3210 lze psát 123::fedc:ba98:7654:3210
 - dvojici „::“ lze použít jen jednou
- zápis IPv6 adresy v tzv. kanonickém tvaru
 - šestnáctková čísla malými písmeny
 - vynechání počátečních nul je povinné
 - konstrukce „::“ musí mít maximální efekt
 - dvojici „::“ se musí použít na nejdelší (případně první) sekvenci nul
- při použití v URL se IPv6 adresa uzavírá do hranatých závorek
 - http://[2002:d91f:cd32::1]/
- určení příslušnosti k síti nebo podsíti vyjadřuje tzv. prefix
 - IP adresa/délka prefixu
 - 12ab:0:0:cd30:0:0:0:0/60
 - prefix lze zapsat v kanonickém tvaru
 - 12ab:0:0:cd30::/60

- typy IPv6 adres
 - `::/128` - nedefinovaná adresa
 - `::1/128` - loopback (localhost)
 - `fc00::/7` - unikátní individuální lokální adresa
 - `fe80::/10` - individuální lokální linková adresa
 - `ff00::/8` - skupinová adresa
 - ostatní - individuální globální adresy
 - využívá se prefix `2000::/3`

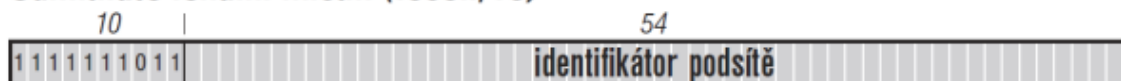


- známé prefixy
 - `64:ff9b::/96` - adresy s vloženou IPv4
 - `2002::/16` - přenos IPv6 přes IPv4 sítě

Lokální linkové (`fe80::/10`)



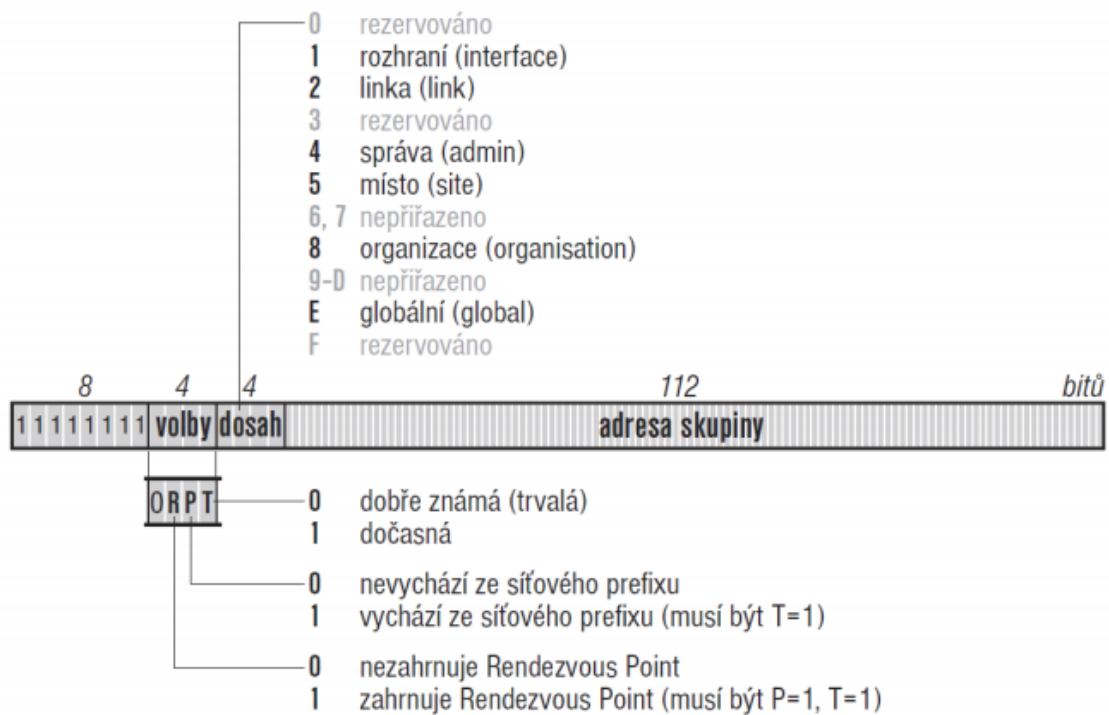
Odmítnuté lokální místní (`fec0::/10`)



Unikátní lokální (`fc::/7`)



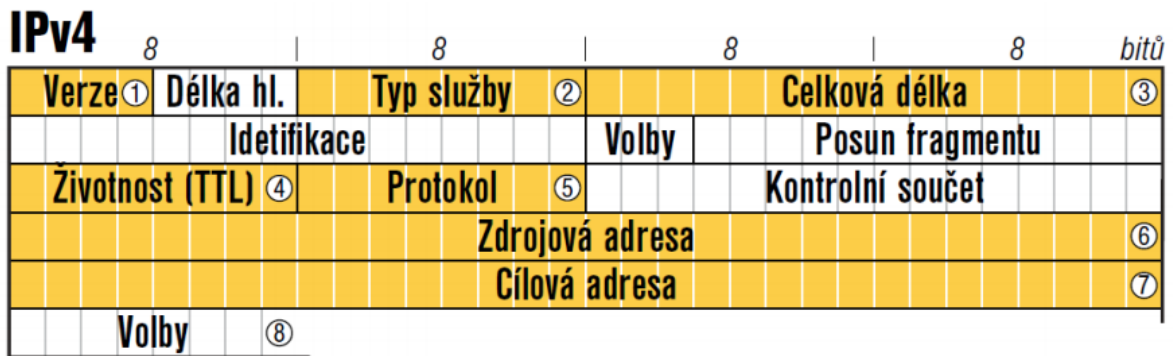
- 1 lokálně generovaný
- 0 jinak generovaný



Skupinové IPv6 adresy

- dobře známé adresy jsou přidělovány centrálně (IANA)
 - dočasné si volí aplikace
- dosah (ff0x::101 je skupinová adresa pro **NTP** servery)
 - - ff02::101 NTP servery na stejné lince (např. Ethernetu)
 - ff05::101 NTP servery v daném místě (lokálně)
 - ff0e::101 NTP servery v celém Internetu
- přidělování skupinových adres
 - 0–3fff:ffff skupiny přidělené IANA (definice celé adresy, RFC 2375)
 - 4000:0000–7fff:ffff identifikátory přidělené IANA
 - 8000:0000–ffff:ffff dynamické, volně k použití
- existuje několik způsobů tvorby skupinových adres
 - odvozeno z individuálního prefixu sítě
 - část z nich pro tzv. Source Specific Multicast (IP rádio či televize, prefix ff3x::/96)
 - odvozeno od identifikátoru rozhraní
 - odvozeno od tzv. rendezvous pointu (prefix ff70::/12)
- předdefinované adresy
 - ff01::1 resp. ff02::1 – broadcast v daném dosahu
 - ff01::2 až ff05::2 – broadcast na všechny směrovače v daném dosahu

Packety



IPv4 paket

- verze – 4 pro IP v4
- délka hlavičky – délka hlavičky v 32 bitových slovech, obvykle 5
- typ služby – často ignorováno, obsahuje požadavky na prioritu atp.
- celková délka – celková délka IP paketu včetně hlavičky (až 64 kB)
- Identifikce – použit pro identifikaci fragmentů téhož IP paketu
- volby – tříbitové pole
 - první bit vždy 0
 - druhý označuje možnost fragmentace (0 – ano, 1 – ne)
 - třetí označuje, zda se jedná o poslední fragment paketu (0 – ano, 1 – ne)
- posun fragmentu – offset dat od počátku původního paketu v násobcích 8 bajtů
- životnost (Time To Live) – omezuje počet průchodů paketu směrovači a zamezuje jeho nekonečnému kroužení v síti. Každý směrovač snižuje hodnotu o 1, je-li nulová, je paket zahozen.
- protokol – udává protokol nesený v IP paketu (hodnota 1 pro ICMP, 6 pro TCP ...)
- kontrolní součet – kontrolní součet hlavičky
- zdrojová adresa – IP adresa odesílatele
- cílová adresa – IP adresa příjemce
- volby – rozšíření o další funkce, běžně se nepoužívá
- padding – zarovnání pole Volby na 32 bitů

IPv6 paket

Verze ①	Třída provozu ②	Značka toku ②														
Délka dat ③		Další hlavička ⑤ ⑧					Max. skoků ④									
Zdrojová adresa																
Cílová adresa																

- verze – 6 pro IPv6
- třída provozu – možnost různého zacházení s IP pakety sítí (diffserv)
- značka toku – možnost označit sekvenci IP paketů
- délka dat – celková délka IP paketu bez standardní hlavičky (až 64 kB)
- další hlavička – typ následující rozšiřující hlavičky
- max. skoků – maximální počet průchodů paketu směrovači (TTL)
- rozšiřující hlavičky – položka Další hlavička (Next header)
 - 0 – volby pro všechny (hop by hop options)
 - 43 – směrování
 - 44 – fragmentace
 - 50 – šifrování
 - 51 – autentizace
 - 59 – poslední hlavička
 - 60 – volby pro cíl (destination options)
- nahrazuje položku Protokol (IPv4)
 - 6 – TCP
 - 8 – EGP
 - 9 – IGP
 - 17 – UDP
 - 46 – RSVP
 - 47 – GRE
 - 58 – ICMP

hlavička IPv6 další=6(TCP)	TCP segment
---	--------------------

a) bez rozšiřujících hlaviček

hlavička IPv6 další=43(směrování)	hlavička směrování další=6(TCP)	TCP segment
--	--	--------------------

b) s hlavičkou *Směrování*

hlavička IPv6 další=43(směrování)	hlavička směrování další=44(fragment.)	hlavička fragmentace další=6(TCP)	TCP segment
--	---	--	--------------------

c) s hlavičkami *Směrování* a *Fragmentace*

Protokoly

NAT

- Network Address Translation

- předpokladem je, že pouze nízký počet uživatelů z privátní sítě potřebuje současně přístup do veřejného Internetu - jejich privátní adresa je při přechodu do veřejné části sítě nahrazena adresou veřejnou (přeložena) a naopak
- by měl být transparentní pro komunikující uzly
 - vyžaduje nový výpočet CRC v hlavičkách vyšších vrstev
 - problém např. s FTP - IP adresa je i v datovém poli aplikačního paketu, musí být také správně přeložena
 - i další aplikace mohou mít obdobné problémy
- otázka - kdy vracet veřejnou adresu d
 - IP protokol je bezstavový - nejsme schopni zjistit, zda bude komunikace pokračovat
 - TCP poskytuje informaci spojení, UDP ne
 - vrací se, pokud není nějakou dobu využita - timeout (obvykle desítky sekund až jednotky minut)
- NAT musí být přednastaven pro komunikaci iniciovanou z veřejné sítě
 - např. interní mail server

Varianta překladu NAPT

- Network Address Port Translation (NAPT)

- kromě IP adresy se překládá i číslo portu (buď TCP nebo UDP) nebo číslo dotazu (query ID u ICMP)
- celá privátní síť je tak z pohledu veřejné sítě vnímána jako jeden uzel s mnoha současně komunikujícími procesy

- NAPT není schopen správně překládat fragmentované pakety v případě komunikace více uzlů z privátní sítě s jedním uzlem sítě veřejné
 - číslo portu je nahrazeno „fragmentation ID“ ve fragmentech
 - uzel ve veřejné síti pak není schopen rozlišit pakety s tímto „fragmentation ID“ od dvou různých privátních uzlů
 - nepravděpodobné, leč možné

ARP Protokol

Address Resolution Protocol - poskytuje konverzi IP adresy na MAC adresu

- spojová vrstva neumí s **IP** adresou pracovat
- spojová vrstva posílá rámce na **MAC** (linkovou) adresu
- uzel sítě si udržuje tabulku s relacemi **IPMAC**
- ARP cache – pokud MAC pro požadovanou IP není nalezena, **ARP** ji vyžádá
 - pošle dotaz broadcastem na spojové vrstvě (**MAC broadcast**)
 - příjemci vyhodnotí, zda je dotazovaná IP adresa jejich
 - ARP odpověď obsahuje požadovanou MAC adresu
 - nový záznam (aktualizace) ARP cache
 - ARP odpověď je adresovaná odesílateli ARP dotazu
- ARP cache lze aktualizovat při příjmu ARP žádostí
 - možná jen aktualizace, nikoliv vytvoření nového záznamu
- struktura packet ARP
 - HW Addr. Space – 1 pro Ethernet
 - Prot. Addr. Space – 0x0800 pro IP
 - HW Addr. Len. – 6 pro Eth. MAC
 - Prot. Addr. Len. – 4 pro IPv4
 - Operational Code
 - 1 – žádost, 2 – odpověď
 - HW Address of Sender
 - MAC adresa odesílatele
 - Protocol Address of Sender
 - IP adresa odesílatele
 - HW Address of Target
 - cílová MAC adresa
 - Protocol Address of Target
 - cílová IP adresa

0	15
HW Address Space	
Protocol Address Space	
HW Address Len.	Prot. Address Len.
Operation Code	
HW Address of Sender	
Protocol Address of Sender	
HW Address of Target	
Protocol Address of Target	

ICMP Protocol

- Internet control message protocol
- slouží k hlášení problémů při zpracování IP paketů směrovači
- **ICMP** zpráva je v datovém poli IP paketu (protocol = 1, další hlavička = 58)
- povinná část implementace IP
- posílá se jen pro první fragment (v případě fragmentace)
- není určen k zajištění spolehlivosti komunikace !!!
- nepoužívá se pro broadcast nebo multicast
- nepoužívá se, pokud zdrojová IP adresa není unikátní adresa hostitele (např. samé 0, samé 1, loopback ...)
- generování ICMP zpráv je volitelné
 - téměř vždy směrovači
 - u hostitelů záleží na implementaci – některé ICMP pakety mohou být zahozeny směrovači
 - např. kvůli bezpečnosti
- **ICMP v4 zpráva**
 - type definuje typ ICMP zprávy
 - 0 – echo reply
 - 3 – destination unreachable
 - 4 – source quench
 - 5 – redirect
 - 8 – echo
 - 9 – router advertisement, 10 – router solicitation
 - 17 – address mask request, 18 – address mask reply
 - ...
 - code definuje specifický kód chyby
- **Echo a Echo reply**
 - používá např. aplikace **ping**

- odesílatel vyšle zprávu echo (8) k cíli
- cíl odpoví zprávou echo reply (0) odesílateli
- lze např. testovat, zda jsou hostitel či router aktivní
- zpracování zprávy echo může být administrátorem z důvodu bezpečnosti zakázáno
 - na hostiteli
 - na routeru
- využito také aplikací **tracert** jako testovací paket
- **Time Exceeded**
 - pole code poskytuje podrobnou informaci
 - 0 – transit TTL exceeded
 - 1 – reassembly TTL exceeded
 - využito v programu **tracert** (Win) nebo **tracertoute** (Unix)
- **Destination Unreachable**
 - pole code poskytuje podrobnou informaci
 - 0 – network unreachable
 - 1 – host unreachable
 - 2 – protocol unreachable
 - 3 – port unreachable
 - 4 – fragmentation needed but disabled
- **ICMP v6 zpráva**
 - type definuje typ ICMP zprávy
 - 1 – cíl nedosažitelný
 - 2 – příliš velký paket
 - 3 – vypršela životnost paketu
 - 4 – problém s parametry (chybné kódy v hlavičce)
 - 128 – echo request
 - 129 – echo reply
 - ...
 - kód definuje specifický kód chyby

NDP Protokol

- **Neighbor Discovery Protocol**
- umožňuje
 - zjistit linkovou adresu z IP adresy
 - detekovat změny v linkových adresách
 - hledat směrovače
 - přesměrování
 - zjišťování parametrů sítě (např. prefixů) pro automatickou konfiguraci
 - ověření dosažitelnosti sousedů
 - detekci duplicitních adres
- využívá ICMP v6
 - router solicitation (výzva směrovači)
 - router advertisement (ohlášení směrovače)
 - neighbor solicitation (výzva sousedovi)
 - neighbor advertisement (ohlášení souseda)
 - redirect (přesměrování)
- hledání souseda
- skupinové adresy s prefixem ff02::1:3

- posledních 24 bitů hledané adresy se připojí za tento prefix
- příklad (hledáme linkovou adresu pro 2001:db8:1:1:022a:fff:fe32:5ed1)
 - skupinová adresa pro zaslání dotazu je ff02::1:ff32:5ed1
- ve volitelných položkách může poslat vlastní linkovou adresu
 - kvůli odeslání odpovědi

Porty a Sokety

- port se využívá jako lokální multiplexor pro současně běžící aplikace (procesy)
- data (pakety) jsou doručeny aplikaci dle trojice:
 - protokol (tedy UDP/IP, TCP/IP ...)
 - síťová adresa (tedy IP adresa)
 - multiplexor na transportní vrstvě (tedy číslo portu)
- port v IP síti je šestnáctibitové číslo
 - různé instance pro TCP a UDP protokoly
- čísla portů < 1024
 - dobře známé porty
 - definované aplikace (např. 23 pro Telnet, 20 a 21 pro FTP ...)
 - definovány organizací IANA
- soket (socket)
 - struktura definující komunikační kanál pro aplikaci (výše popsaná trojice)
 - první implementace v BSD soketech (BSD Unix)

UDP Protokol

- User Datagram Protocol
- povinná implementace
- poskytuje aplikační rozhraní k IP
 - jediná přidaná hodnota je multiplexování podle čísla portu
 - neposkytuje spolehlivost, emulaci spojení, řízení datového toku

TCP Protokol

- Transmission Control Protocol
- povinná implementace
- multiplexování dle čísla portu
- spolehlivá komunikace
 - sekvenční čísla
 - generování potvrzení (ACK), opakování při chybě
- emulace spojení
 - aplikační rozhraní jako proud bajtů
 - garantuje pořadí přenášených dat
 - emulace plně duplexní komunikace

Взяв.- řízení datového toku

- mechanismus okének
 - - segmentace dat do paketů

DHCP Protocol

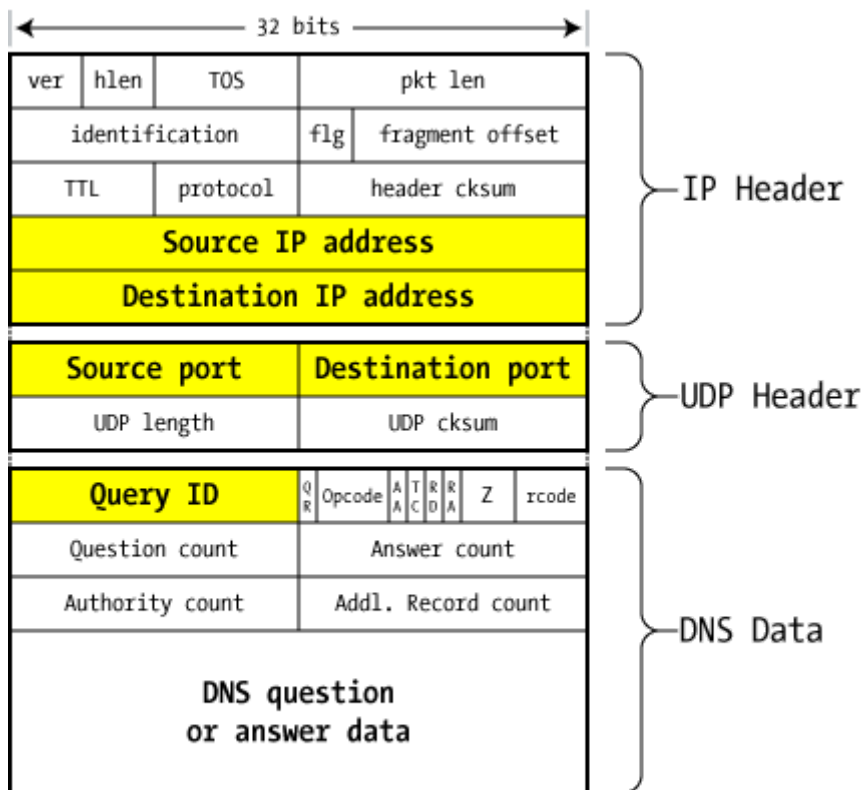
- Dynamic Host Configuration Protocol

- distribuce konfigurace TCP/IP
 - - umožňuje bootování bezdů hostitel
 -
 - Φ
- vychází ze staršího protokolu BOOTP
 - BOOTP klienti mohou být obslouženi DHCP serverem
- DHCP zprávy se přenášejí v UDP paketech
 - nezabezpečené
 - možné útoky prostřednictvím neautorizovaného DHCP serveru
- klasické DHCP využívá broadcast
- DHCPv6 skupinové adresy
 - všichni DHCP agenti a servery ff02::1:2
 - všechny DHCP servery ff05::1:3

DNS (Domain Name System)

- proč jmenný systém?
- je jednodušší používat jména počítačů než jejich IP adresy
 - pro lidi, nikoliv pro stroje
- pokud je uzel přesunut do jiné sítě
 - IP adresa se změní
 - jmenný název zůstává
- původně plochý jmenný prostor
 - jednoduchá jména uzlů, např. "Jupiter"
 - lokální soubor "hosts.txt", obsahuje databázi jmen a příslušných adres, později stahovaný z FTP
 - složitá (nemožná) metoda pro velké sítě s distribuovanou správou
- hierarchický jmenný systém
- distribuovaný systém s distribuovanou správou
- obvykle kopíruje organizační struktury
- název uzlu definuje pozici v hierarchii
 - "hostname.subdomainN....subdomain1.toplevel domain"
 - např. measure.feld.cvut.cz
- Top-level domény
 - generické - např. com, biz, org, net ...
 - států – např. cz, sk ...
- rozděleno na zóny
- pravomoc (authority) k zóně má odpovídající jmenný server
- jediný server může být zodpovědný za více zón
- pravomoc k dílčímu podstromu v hierarchii může být delegována
 - a to rekurzivně
- pro TLD zóny jsou k dispozici kořenové jmenné servery, koordinované ICANN
 - podpora anycastu v IPv6
 - podpora „load sharing“
- DNS poskytuje více než jen překlad jmen IP



- překlad IP -> jméno
- získání dalších informací o hostiteli (např. typ OS ...)
- informaci o konfiguraci mailu pro konkrétní doménu
- ...















DNS packet on the wire

- typy DNS Serverů
 - primární
 - má autoritu nad zónou
 - probíhá na něm editace záznamů
 - sekundární
 - má autoritu nad zónou
 - přebírá data od primárního serveru
 - tzv. přenos zóny v pravidelných časových intervalech (typicky jednotky hodin)
 - „Caching only“
 - poskytují neautorizované odpovědi
 - získávají informace z primárních nebo sekundárních serverů
 - slouží k omezení zátěže těchto serverů (a také k redukci síťového provozu)
- tentýž fyzický server může pracovat jako DNS server různého typu pro různé zóny

DNS configuration

Zone: `unixtest.test200.psoft`  

Name	TTL	Class	Type	Data
Built in A records				
unixtest.test200.psoft	86400	IN	A	192.168.114.200
*.unixtest.test200.psoft	86400	IN	A	192.168.114.200
Custom A records				
Add DNS A Record				
Built in MX records				
unixtest.test200.psoft	86400	IN	MX	10 mail.test200.psoft
Custom MX records				
Add DNS MX Record				
Built in CNAME records				
mail.unixtest.test200.psoft	86400	IN	CNAME	mail.test200.psoft
Custom CNAME records				
Add DNS CNAME Record				

Type ↕	Value (decimal) ↕	Defining RFC ↕	Description ↕	Function ↕
A	1	RFC 1035  ^[1]	Address record	Returns a 32-bit IPv4 address, most commonly used to map hostnames to an IP address of the host, but also used for DNSBLs , storing subnet masks in RFC 1101  , etc.
AAAA	28	RFC 3596  ^[2]	IPv6 address record	Returns a 128-bit IPv6 address, most commonly used to map hostnames to an IP address of the host.
AFSDB	18	RFC 1183 	AFS database record	Location of database servers of an AFS cell. This record is commonly used by AFS clients to contact AFS cells outside their local domain. A subtype of this record is used by the obsolete DCE/DFS file system.
APL	42	RFC 3123 	Address Prefix List	Specify lists of address ranges, e.g. in CIDR format, for various address families. Experimental.
CAA	257	RFC 6844 	Certification Authority Authorization	CA pinning, constraining acceptable CAs for a host/domain
CERT	37	RFC 4398 	Certificate record	Stores PKIX , SPKI , PGP , etc.
CNAME	5	RFC 1035  ^[1]	Canonical name record	Alias of one name to another: the DNS lookup will continue by retrying the lookup with the new name.
DHCID	49	RFC 4701 	DHCP identifier	Used in conjunction with the FQDN option to DHCP
DLV	32769	RFC 4431 	DNSSEC Lookaside Validation record	For publishing DNSSEC trust anchors outside of the DNS delegation chain. Uses the same format as the DS record. RFC 5074  describes a way of using these records.
DNAME	39	RFC 2672 	Delegation Name	DNAME creates an alias for a name and all its subnames, unlike CNAME, which aliases only the exact name in its label. Like the CNAME record, the DNS lookup will continue by retrying the lookup with the new name.
DNSKEY	48	RFC 4034 	DNS Key record	The key record used in DNSSEC . Uses the same format as the KEY record.
DS	43	RFC 4034 	Delegation signer	The record used to identify the DNSSEC signing key of a delegated zone

- záznamy (Resource records)

- class

- aktuálně pouze hodnota IN (Internet system), ostatní jsou zastaralé

- TTL

- specifikuje čas v sekundách, po který je záznam platný v DNS cache
- typická hodnota pro záznam A je 86400 (1 den)
- RDLlength
 - délka pole RData
- RData
 - řetězec popisující daný záznam
 - formát závisí na typu (a třídě) záznamu
- přístup do DNS - program NSLOOKUP
- dynamické DNS záznamy – spolupráce DHCP DNS

Ethernet

- vznikl počátkem 70. let u firmy Xerox (3 Mbit/s)
- varianta 10 Mbit/s vznikla ve spolupráci s DEC a Intel (DIX)
- později standardizován v rámci standardu IEEE 802, konkrétně 802.2 (podvrstva LLC – Logical Link Control) a 802.3 (podvrstva MAC – Medium Access Control a fyzická vrstva) - existuje mnoho variant - různé fyzické topologie a přenosové rychlosti
- shodná metoda řízení přístupu k médiu a formát rámce
- mimo standard IEEE802 existují další formáty rámců
- jednotlivé varianty standardizovány jako IEEE802.3xx, kde xx je jedno či dvou písmenné označení
- např. klasický 10Base2 je značen 802.3a
- gigabitový Ethernet 1000Base-T je značen 802.3ab

Virtual LAN (VLAN)

- realizace „samostatných“ virtuálních LAN se sdílenou fyzickou infrastrukturou
- oddělení komunikace v jednotlivých sítích
 - včetně specifického broadcastu v rámci **VLAN**
- implementace prostřednictvím aktivních prvků infrastruktury
 - přepínače (mosty) - uživatelské MAC rámce obsahují tzv. tagy součástí tagu může být i informace o prioritě MAC rámce
- definováno standardem IEEE802.1Q
- částečně vychází z IEEE802.1D (specifikace standardních přepínačů)
- uživatelské MAC rámce jsou vždy přiřazeny do právě jedné VLAN
- přímo - rámec obsahuje daný tag
- nepřímý - tag je doplněn přepínačem dle portu, z něhož dorazil

Spanning Tree

- algoritmus je implementován pro každou VLAN
- **MSTP (Multiple Spanning Tree Protocol)**
- volba kořenového „root“ prvku pro VLAN — nalezení kořenového portu (s nejnižší „cenou“) — volba aktivního a případného záložního portu — specifické protokoly pro komunikaci mezi mosty
- typ 0x8100 – indikace VLAN VID (VLAN ID) — 0, pouze info o prioritě — 1, standardní hodnota pro ingress, lze změnit — 0xffff, rezervováno jako „wildcard“ PCP – priorita CFI (canonical format identification) — 0 – little endian, 1 big endian

Bezdrátové systémy

využívají rádiový komunikační kanál

- jeho základní vlastnosti jsou uvedeny ve 2. přednášce

výhodou je vysoká flexibilita

- žádná nezbytná infrastruktura
 - kromě napájení
- jednoduché změny topologie
 - přemístění uzlů, rozšiřování

nevýhodou je potřeba frekvenčního pásma

- v SPD aplikacích nejčastěji využívána pásma ISM
 - při dodržení podmínek není třeba povolení
 - je třeba počítat s případnou koexistencí s dalšími uživateli
 - možnost dočasné (trvalé) nedostupnosti uzlů – vzhledem k rušení nebo omezenému výkonu vysílání (S/N ratio)

IEEE 802.x

- tento standard již byl zmíněn v předchozí přednášce
- definuje např. varianty CSMA/CD sítí
- jeho další části definují technologie pro bezdrátové sítě

802.11

- původní specifikace
- ISM pásmo 2.4 GHz, 1 (2) Mbit/s
- komunikace v rozprostřeném spektru
 - FHSS – 75 kanálů s šířkou 1 MHz
 - DSSS – 14 (překrývajících se) kanálů s šířkou 22 MHz
- přístupová metoda CSMA/CA
- dosah 30/90 m (uvnitř budov/volné prostranství)

802.11a

- pásmo 5 GHz, maximálně 54 Mbit/s
 - výhodou je nižší využití pásma (nižší úroveň rušení)
- OFDM modulace, 52 nosných, BPSK, QPSK, 16(64)QAM
 - se zhoršující se kvalitou kanálu se volí robustnější modulace
- 12 (někde 24) kanálů po 20 MHz
- v Evropě nejsou (nebyly) k dispozici frekvence
- nesplňuje zcela požadavky evropských regulátorů

802.11b

- první inovace původního standardu
- ISM pásmo 2.4 GHz, maximálně 11 Mbit/s
- pouze DSSS (FHSS je kvůli zpětné kompatibilitě)
- s anténami s vyšším ziskem lze komunikovat až na několik km

802.11g

- druhá inovace původního standardu
- ISM pásmo 2.4 GHz, maximálně 54 Mbit/s
- výhradně OFDM, DSSS pouze kvůli zpětné kompatibilitě
 - opět 16/64QAM, pro nižší rychlosti BPSK a QPSK (při nižší kvalitě kanálu)
- zařízení jsou obvykle kompatibilní i s variantou b (značí se b/g)

802.11h – varianta 802.11a pro Evropu – pásmo 5GHz – zahrnuje dynamický výběr kanálu a řízení výkonu • robustnější • odolnější vůči rušení

802.11n – ISM pásma 2.4 GHz nebo 5 GHz, 40 MHz kanály – modulace až 64QAM (OFDM) – využívá prostorové multiplexování • MIMO (Multiple In/Multiple Out) technologie – více vysílacích/ přijímacích antén • konfigurace TxR:S – např. 3x3:2 – 3 vysílací antény – 3 přijímací antény – 2 současné datové toky – dostupné fyzické rychlosti jsou až 600 Mbit/s pro 4 datové toky – obvyklé je využití 2 datových toků – 2x2:2

802.11ac – ISM pásmo 5 GHz, 80 – 160 MHz kanály – modulace až 256QAM (OFDM) – využívá prostorové multiplexování • MIMO (Multiple In/Multiple Out) technologie – až 8 prostorových datových toků – dostupné fyzické rychlosti jsou až >800 Mbit/s na datový tok – možnost MU-MIMO – jednotlivé datové toky přijímány více uživateli současně

Pásmo 2.4 GHz je dnes využito následovně – 14 částečně se překrývajících kanálů (odstup 5 MHz, sirka 22 MHz) • 11 USA, 13 Evropa, 14 Japonsko – povolen EIRP 100 mW (20 dBm) – při použití směrových antén je třeba snížit výkon!! Poslední verze standardu 802.11-2012 zahrnuje většinu dodatečných specifikací

Struktura sítě IEEE802.11

Ad-hoc sítě

- přímá komunikace mezi uzly bez síťové infrastruktury – označovány jako IBSS (Individual Basic Service Set)

Stacionární sítě

- infrastruktura (DS, Distribution System) využívající (obvykle) stacionární přístupové body (AP, Access Point) • součástí AP může být i most do pevné sítě (typicky Ethernet) – každý AP obsluhuje oblast označovanou jako BSA (Basic Service Area) • skupina uzlů řízených jedním AP se označuje BSS (Basic Service Set) – oblast pokrytá více AP propojenými DS se nazývá ESA (Extended Service Area) • kompletní bezdrátová síť (bez DS) pak ESS (Extended Service Set) – síť je identifikována prostřednictvím SSID (Service Set ID v Beacon rámcích)

Přístupová metoda CSMA/CA

- CSMA/CA (.../Collision Avoidance) – ne všechny uzly sdílející fyzický kanál se slyší navzájem • nejsou schopny detekovat kolize – před vysláním rámce uzel čeká po dobu mezirámcové mezery a teprve pokud je kanál stále volný: • zvolí náhodný časový interval (back-off) • pokud po je celou tuto dobu kanál volný, vysílá

Virtuální odposlech kanálu (CS)

předpoklad: všechny uzly slyší AP – uzel nejprve vyšle žádost o přidělení kanálu (RTS – Request To Send) - neplést se signálem EIA/TIA 232 ! – s využitím CSMA/CA – AP odpoví přidělením vysílacího času (CTS – Clear To Send) • ostatní slyší a pokládají kanál za obsazený, i když nedetekují obsazený kanál • aktualizují svůj NAV (Network Allocation Vector) – výrazně se snižuje pravděpodobnost vzniku kolize • teoreticky by neměla vzniknout vůbec – pokud všechny uzly slyší rámec CTS

Pouze pro rámce delší než předdefinovaný limit – případně lze RTS/CTS zcela vypnout – jen pro unicast

Potvrzovací mechanismus - ACK

Pouze pro unicast rámce – vysílá se s krátkou IFS – vyšší priorita – případně lze zcela vypnout • má význam u přenosu na vyšší vzdálenost

Fragmentace MSDU

Jsou-li data delší než maximální délka datového pole MAC rámce – při vysílání fragmentů se využívá kratší IFS • „vyšší priorita“

Funkce HCF

Hybrid Coordination Function – implementováno v AP (volitelně) – podpora QoS – varianta EDCA (Enhanced Distributed Channel Access) • analogie DCF • podpora tzv. AC – Access Classes (4), do nichž jsou mapovány rámce s různou prioritou, různé IFS • interní back-off pro jednotlivé fronty – varianta HCCA (HCF Coordinated Channel Access) • obdoba PCF • může se střídat s EDCA přístupem • používá kratší IFS – dokáže převzít volný kanál • podpora pro QoS

Testy

1. Test 2017

- 1) Výpočet napětí u různě zakončených kabelů
- 2) Metody error correction
- 3) Výpočet crc a kdy to nenajde chybu
- 4) co je to ARP
- 5) proč je délka rámce u ethernetu taková jaká je
- 6) princip podpisu souboru
- 7) TCP vs UDP
- 8) princip slave&master
- 9) Princip a funkce NAT
- 10) co je **Hammingova** vzdálenost a jak se používá

2. Test 2017

1) vypočítejte napětí na konci koaxiálního vedení s impedancí $Z_0 = 75\Omega$, délka $l=100\text{m}$ a zpoždění signálu 5ns/m v čase $t=0,7\mu\text{s}$, jeli ke vstupu v čase t_0 připojen zdroj stejnosměrného napětí 10V s vnitřní impedancí 75Ω , pro následující případy:

1. Konec vedení zakončen terminátorem s impedancí 75Ω
2. Konec otevřený
3. Konec je zkratový

[Řešeno na [FB](#), v [dokumentu](#)] **jak se to počítá?**

- 2) [Hammingova vzdálenost](#), kdy opravuje t-násobné chyby a proč
- 3) digitální podpis
- 4) co je [CRC](#), kdy chyby nedetekuje
- 5) **token-passing**, vysvětlit, plusy a minusy*-
- 6) adresace uzlu vs. adresace zprav
- 7) detekce kolizi v sítích Ethernet
- 8) [vysvětlit NAT](#), NAT vs. [NAPT](#)
- 9) jak **TCP** zajišťuje spolehlivost
- 10) [Síťová vrstva ISO/OSI](#)
- 11) [ICMP](#) +příklad

3. Test 2017

- 1) vypočítejte napětí
koaxiální kabel, délka 50m napětí(vstupní) 9V
 $R_i = 100$
- 2) co je to numerická apertura
- 3) vypočítejte CRC, k čemu CRC slouží
- 4) **Hammingova vzdálenost**
- 5) Multiplexování a Splitting nebo tak nějak
- 6) ISO a jak se řeší překlad adres
- 7) Dokažte něco pro CRC, kdy CRC detekuje t násobnou chybu

- 8) Rozdíl hub a switch
- 9) Rozdíl UDP a TCP
- 10) Kdy se používá -
- 11) Síťová x linková adresace
- 12) DNS

Testy 2019

1.

- 1) - Spočítat napětí na konci vedení - s zkratem, uzemněním a odporem na konci
- 2) - Výpočet CRC
- 3) - Co je ICMP
- 4) - Adresace zpráv a uzlů
- 5) - Vztah ethernetu a CSMA/CD
- 6) - Vysvětlí token-passing
- 7) - Virtuální odposlech u WIFI
- 8) - NAT a NAPT
- 9) - Jak funguje spolehlivost TCP
- 10) - Hemmingův kód a dokázat to
- 11) - Co je digitální podpis a jak funguje

2.

- 1) Spočítat napětí v ustáleném stavu na vstupu koaxiálního vedení
- 2) Numerická apertura mnohavidového optického vlákna
- 3) def. Hammingovy vzdálenosti kodu d, uvest, kdy kod detekuje t-nasobne chyby a dokazat
- 4) podstatne vlastnosti hashovací fce + kde se pouziva
- 5) multiplexovani X splitting
- 6) vyuziti CRC pro detekce chyb v datovych prenosech, jake typy chyb nejsou registrovany?
- 7) maxim. delka shlukove chyby t, kterou CRC kod s jistotou odhali? dokazat
- 8) rozdíl hub x switch obecně
- 9) rozdíl na spojeve a síťové vrstvě ISO/OSI + souvislost, uvest řešení pro nalezení MAC adresy, když známe síťovou adresu
- 10) DNS v IP sítích
- 11) UDP x TCP
- 12) implementace technologie VLAN v Ethernetu

3.

- 1) příklad je typu co byl v testu 2 r. 2017 (otevřený konec vedení)
- 2) Funkce prezentační vrstvy a konkrétní příklady
- 3) princip crc, výpočet crc pro data 111101101010101101 a polynom 1011
- 4) k čemu jsou porty. lze použít současně 1 port pro TCP a UDP komunikaci?
- 5) klient/server
- 6) jak funguje ARP, do jaké vrstvy ISO/OSI patří
- 7) popsat DNS. autoritativní vs. neautoritativní dotazy
- 8) princip fragmentace na síťové vrstvě. je nějaký rozdíl mezi fragmentací u IPv4 a IPv6?
- 9) synchronní vs. asynchronní komunikace
- 10) BPSK - popsat princip a nakreslit konstelační diagram + další typy fázové modulace
- 11) rozdíl mezi unicast a anycast
- 12) zapsat zadanou IPv6 adresu v kanonickém tvaru
- 13) jak se chová hub, když v Ethernetu dojde ke kolizi

4.

- 1) Spocítat napětí na konci koaxialního vedení
- 2) Definujte Hammingova vzdálenost, oprava t-násobné chyby
- 3) ;pojem digitální podpis a popište způsob vytvoření a overení
- 4) Princip CRC, spočítat pro 110111000111010011 a polynom 1011, kdy metoda nedetekuje chybu
- 5) Vysvětlete přínos prokládání (interleaving) používaného spolu s kódy pro opravu chyb (Forward Error Correction Codes)
- 6) Vysvětlete TDM
- 7) Popište Token-Passing, porovnat se stochastickými metodami
- 8) Rozdíl adresace uzlu a adresace zpravy
- 9) Jak je zajištěna detekce kolize v sítích Ethernet
- 10) Smysl a funkce NAT a NAT
- 11) Popsat TCP spolehlivost

Odhad budoucích otázek

- 1) Neměnné otázky ?
 - a) CRC ([doc](#), [FB](#))
 - b) Napětí na konci vedení ([doc](#), [FB](#))
 - c) Hammingova vzdálenost ([doc](#))
 - d) Protokoly TCP/UDP ([doc](#))
- 2) Optika, kritický úhel (numerická apertura) ([doc](#))
- 3) Metody přístupu k médiu ([doc](#))
- 4) Metody zajištění spolehlivosti přenosu ([doc](#))
- 5) Aktivní prvky sítě ([doc](#))
- 6) Adresace ([doc](#))
- 7) Protokoly (ICMP/ARP/NAT/DHCP) ([doc](#))
- 8) DNS ([doc](#))
- 9) Něco o Ethernetu ([doc](#)), něco o bezdrátu ([doc](#))
- 10) Vrstvy OSI + služby na nich ([doc](#), [doc](#), [img](#), [img](#))