PSIA

8. Počítačové sítě, ISO/OSI model, vlastnosti fyzických vrstev, topologie, řízení přístupu k médiu, kódování, spolehlivost datových přenosů, protokoly rodiny TCP/IP

ISO/OSI model (International Organization for Standardization/Open Systems Interconnection model)

- ISO OSI model je rozdělený na vrstvy. Teorie je taková, že v každé vrstvě se řeší něco jiného a není potřeba znát fungování jiných vrstev. Třeba emailový klient nepozná, jestli mu data přišla přes Wi-Fi nebo kabelem. Data vytvořená v aplikační vrstvě (packet) se obalí hlavičkou nižší vrstvy, postupně se uzavírá do dalších a dalších hlaviček, poslední je hlavička ethernetového rámce. Zařízení se vždy dívají jen na hlavičku z vlastní vrstvy - třeba router posílá packety dál podle IP adresy a je mu jedno, jestli to je TCP nebo UDP.
- Hlavním cílem je umožnit snadné propojování distribuovaných systémů

Vrstva	Vrstva anglicky	Protokoly	Název v TCP/IP	Zařízení	Pomůcka
Aplikační	Application	FTP, HTTP, SSH	Aplikační		All
Prezentační	Presentation	SSL, MIME	Aplikační		People
Relační	Session	SQL, PAP	Aplikační		Sleeping/Resting
Transportní	Transport	TCP, UDP	Trasportní		Through
Síťová	Network	IP	Síťová	Router	Networking
Spojová	Link	MAC, Ethernet	Vrstva síťového rozhraní	Switch	Lectures
Fyzická	Physical	RS-232, RS-485, Ethernet	Vrstva síťového rozhraní	Hub	Fail

Fyzická

- Zabývá se výhradně přenosem bitů (symbolů)
- otázkami typu kódování, modulace, časování, synchronizace, elektrické parametry signálů, konektory, řídicí signály rozhraní
- nijak neinterpretuje to, co přenáší
- paralelní a sériový přenos
- synchronní, asynchronní a arytmický přenos
- přenos v základním a přeloženém pásmu
- RS-232, RS-485, IEEE802.3 (Ethernet), IEEE802.11 (Wi-Fi)

Spojová

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

Síťová

- Přenáší bloky dat označované jako pakety
- 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 (přibližně)

- Může používat různé algoritmy směrování:
  - adaptivní, neadaptivní
  - izolované, distribuované
- Je poslední vrstvou, kterou musí mít přenosová infrastruktura (s výhradou velmi jednoduchých systémů) – není např. u většiny průmyslových distribuovaných systémů
- Asi nejrozšířenější implementací síťového protokolu je protokol IP – podporovaný protokoly pro výměnu informací o směrování mezi směrovači

Transportní

- 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

Relační

- Zajišťuje sestavení, řízení a zrušení relací
  - pro spojovanou komunikaci
- Dále může zajišťovat:
  - synchronizaci (např. více datových toků)
  - šifrování dat
  - kompresi dat
  - podpora transakčního zpracování dat

Prezentační

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

Aplikační

- **původní představa**:
  - bude obsahovat aplikace
  - problém: aplikací je moc, musely by být všechny standardizovány
    - to nejde stihnout - nemělo by to ani smysl
- **později**:
  - aplikační vrstva bude obsahovat pouze „jádro“ aplikací, které má smysl standardizovat
    - například 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

Layer (N)

- příslušná vrstva OSI modelu
  Sublayer
- podvrstva - dělení funkcí vrstvy na dílčí části
  Service (N)

- služba poskytovaná vrstvou N a vrstvami níže vrstvě N+1
  Entity (N)
- element vrstvy N realizující část funkcí této vrstvy
  Peer Entities (N)
- elementy téhož typu v téže vrstvě N v různých uzlech systému
  Protocol (N)
- sada pravidel (sémantických a syntaktických) definujících komunikaci mezi entitami vrstvy N
  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 (N) a volitelně uživatelských dat (N)
  SDU – Service Data Unit (N-1)
- informace předávaná mezi vrstvami N a N-1
  Multiplexing – **Demultiplexing** (N)
- funkce entity vrstvy N, kdy jediné spojení vrstvy N-1 je použito pro více spojení vrstvy N
  Splitting – **Recombining** (N)
- funkce entity 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

Zpracování chyb při přenosu

Forward error correction - dopředná korekce

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 multimédií

ARQ metody

Automatický opakovaný dotaz (Automatic repeat request, ARQ), je metoda kontroly chyb při přenosu dat, která využívá potvrzení (zprávy odeslané příjemcem, které oznamují, že správně přijal zprávu) a časové limity (stanovené časové úseky, které mají uplynout, než má být potvrzení přijato) k dosažení spolehlivého přenosu dat přes nespolehlivý komunikační kanál.

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 rámci
- 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

Ověření správnosti dat

- Řešením je doplnění užitečných dat o dodatečná (redundantní) data, která jsou s užitečnými daty definovaným způsobem svázána (lze je z užitečných dat dopočítat)
- Např. parita - redundantní bit reprezentuje tzv. lichou paritu, počet jedniček ve výsledném kódovém slově je liché číslo - !detekuje jen lichý počet chyb!
- Definujme termín „Hammingova vzdálenost kódu“ d jako nejnižší počet znaků, v nichž se liší libovolná dvě kódová slova
- Detekce chyb:
  - množinu všech slov rozdělíme na slova kódová a slova nekódová.
  - t-násobná chyba vždy změní kódové slovo na nekódové, pokud se každá dvě kódová slova liší ve více než t znacích.
  - Kód **odhaluje** t-násobné chyby, pokud je Hammingova vzdálenost kódu d > t
  - Kód **opravuje** t-násobné chyby, pokud je Hammingova vzdálenost kódu d > 2t

Cyclic Redundancy Code (CRC)

- 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

Příklad
Generující polynom: $C(x) = x^3 + x^2 + 1 \quad \rightarrow \quad 1101$
Zpráva: $M(x) = x^7 + x^4 + x^3 + x \quad \rightarrow \quad 10011010$

Odesílatel:

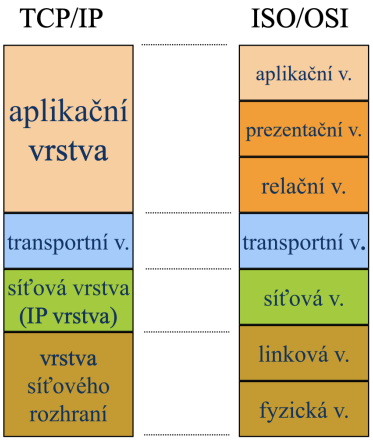
1. Posuneme data o stupeň generujícího polynomu
   $M(x) = x^{10} + x^7 + x^6 + x^4 \quad \rightarrow \quad 10011010000$
2. Vydělíme
   $(x^{10} + x^7 + x^6 + x^4) : (x^3 + x^2 + 1) = \dots$
   $\vdots$
   $x^2 + 1 \quad \rightarrow \quad 101 = R(x)$
   (zbytek po dělení)
3. Odešleme původní zprávu $M(x)$ následovanou zbytkem po dělení
   $P(x) = M(x) + R(x) = 10011010101$

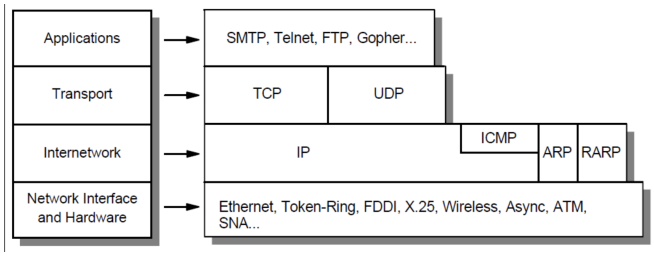
Příjemce:

1. Přijme se polynom P(x) + E(x)
   - E(x) reprezentuje chyby
   - E(x) = 0 znamená bezchybný přenos
2. Dělení (P(x) + E(x)) polynomem C(x)
   - Pokud je výsledek= 0, buď
     - Nedošlo k chybě (E(x) = 0, P(x) je dělitelné C(x) beze zbytku)
     - (P(x) + E(x)) je beze zbytku dělitelné C(x), chyba nebyla detekována

- Detekce chyb
  - chyby reprezentovány chybovým polynomem E(x)
    - shodná délka jako má kódové slovo
  - odesláno kódové slovo N(x), přijato slovo N'(x) = N(x)+E(x)
  - chyba je detekována pokud G(x) nedělí E(x) beze zbytku
    - neboli: je-li E(x) násobkem G(x), chyba není detekována
- Jaké chyby lze detekovat?
  - všechny jednonásobné chyby, pokud má polynom G(x) alespoň 2 členy
  - všechny dvojnásobné chyby, pokud generující polynom nedělí $(x^m + 1)$ pro všechna *m* < délka kódového slova a má alespoň 2 členy
  - všechny chyby liché násobnosti, pokud je generující polynom G(x) beze zbytku dělitelný (x + 1)
  - všechny shlukové chyby délky ≤ *k* (*k* je stupeň G(x)), pokud G(x) obsahuje nenulový konstantní člen
  - téměř všechny shlukové chyby délky *k+1* (k je stupeň G(x)), pokud G(x) obsahuje nenulový konstantní člen
  - téměř všechny shlukové chyby délky > *k*+1 (stejný předpoklad o G(x))

TCP/IP





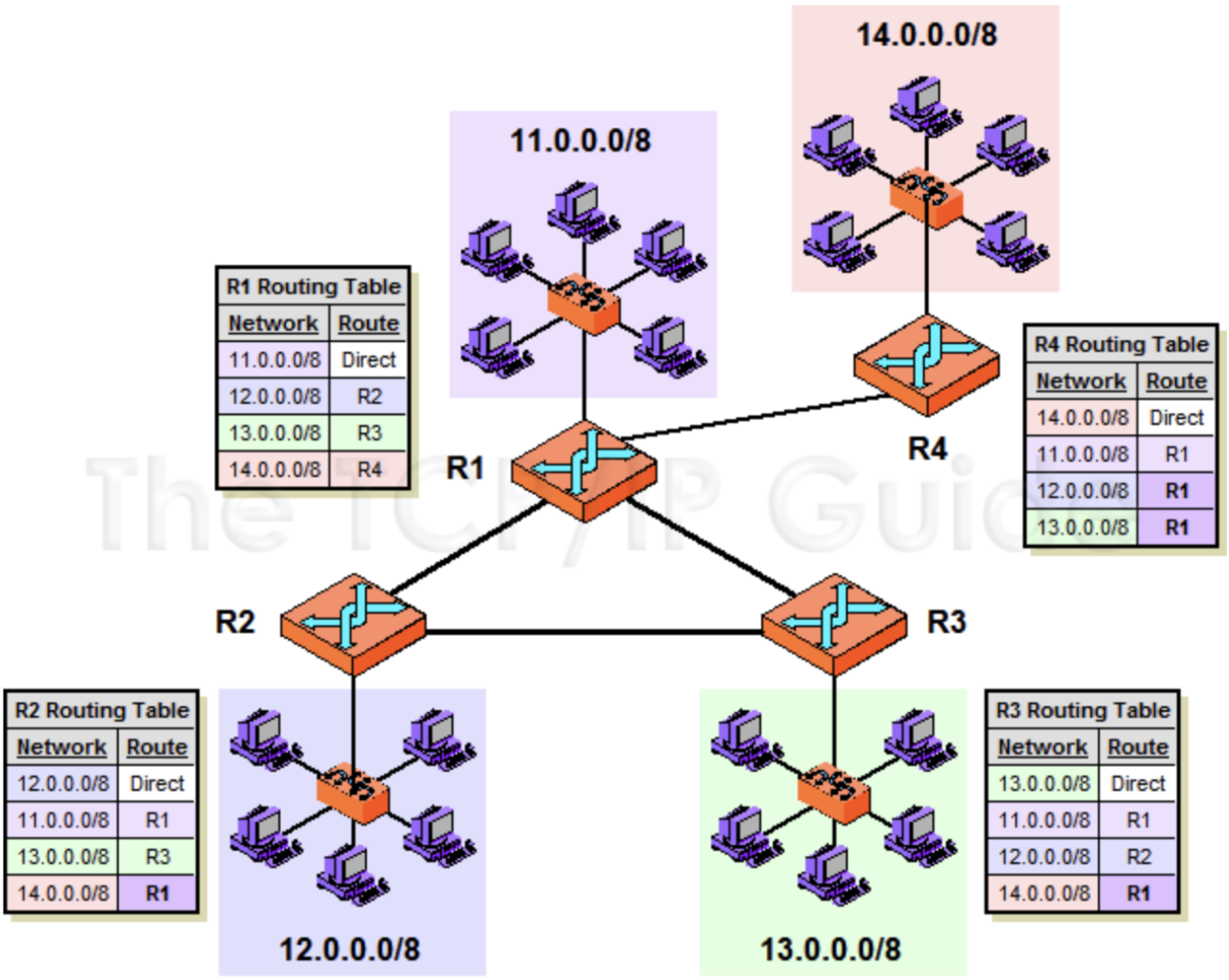
Protokoly TCP/IP, IPv4, IPv6, ICMP, ARP, NDP, TCP, UDP, DHCP, systém DNS

- vše v této prezentaci
- https://moodle.fel.cvut.cz/pluginfile.php/281115/mod_resource/content/4/4_TCPIP.pdf

Princip směrování v IP sítích

Pokud je po přijetí IP datagramu zjištěno, že není určen pro toto zařízení, měl by nutně být předán dále tak, že bude předán podle záznamů ve směrovací tabulce dalšímu cíli. V každém IP datagramu je uvedena IP adresa cíle, pro který je určen. Tato cílová IP adresa je porovnávána postupně se všemi záznamy ve směrovací tabulce. Tabulka je setříděna podle délky masky v jednotlivých záznamech od nejdelších (nejvíce jedniček zleva) po nejkratší (nejméně jedniček zleva), což vyjadřuje velikost cílových podsítí. Nejprve jsou tedy záznamy pro jednotlivé počítače nebo malé podsítě a teprve dále jsou záznamy pro postupně větší a větší podsítě. Postup porovnání s každým záznamem ve směrovací tabulce je následující:

1. je proveden logický součin cílové IP adresy a masky ze zkoumaného řádku tabulky
2. je-li výsledek roven cíli uvedenému ve zkoumaném záznamu, je nalezena shoda
3. není-li nalezena shoda, je zpracován další řádek tabulky
4. není-li již k dispozici další záznam v tabulce a shoda dosud nebyla nalezena, je ohlášena nedosažitelnost cílové sítě pro zkoumaný IP datagram



Řízení přístupu k médiu

Deterministický princip

Kolize vůbec nenastávají.

Master-Slave

- vyhrazený uzel Master se dotazuje uzlu typu Slave
- Slave nesmí samostatně vysílat, komunikace probíhá pouze přes Mastera
- např.: průmyslové distribuované systémy
  cons: závislost na výpadku Mastera
  pros: jednoduchá implementace

Token Passing

- jednotlivé uzly jsou rovnocenné
- oprávnění k vysílání má držitel pověření (tokenu), které si uzly v kruhu předávají mezi sebou

- držení tokenu je pro jeden uzel časově omezeno
  cons: dlouhý čas na zformování kruhu na začátku nebo při ztrátě tokenu
  pros: nezávislost na jednom uzlu

TDMA (Time Division Multiple Access)

- Umožňuje více uživatelům sdílet stejný frekvenční kanál dělením signálu do různých časových slotů
- Uživatelé vysílají v rychlém sledu za sebou, jeden po druhém, každý používá svůj vlastní časový slot. To umožňuje více stanicím sdílet stejné přenosové médium (např. kanál rádiových frekvencí), při využití pouze části kapacity kanálu.

Delegated Token

- existuje vyhrazený uzel (arbitr), který vysílá speciální výzvu umožňující ostatním uzlům vysílat
- díky adresaci zpráv mohou všechny uzly přijímat současně
- nevýhodou je závislost na uzlu arbitra

Nedeterministický princip

Kolize nastávají a protokol s nimi počítá.

Protokol CSMA (Carrier Sense Multiple Access)

- všechny uzly jsou rovnocenné
- uzel před započetím vysílání čeká až skončí vysílání předchozí (Carrier Sense)
- na médiu vysílá a přijímá více uzlů. Vysílání jednoho uzlu je obecně přijímáno všemi ostatními uzly užívajícími médium. (Multiple Access)

CSMA/CA (Collision Avoidance)

- uzel informuje ostatní o úmyslu vysílat
- Wifi

CSMA/CD (Collision Detection)

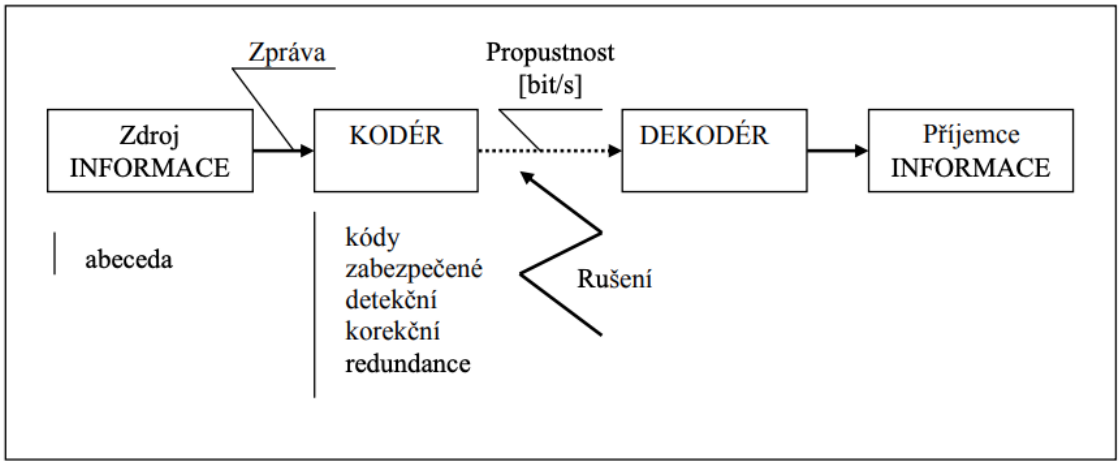
- po detekci kolize všechny uzly čekají náhodnou dobu před dalším pokusem o vysílání

CSMA/CR (Collision Resolution)

- všem uzlům je přiřazeno identifikační číslo či kód priority
- při výskytu kolize jeden z uzlů pokoušejících se vysílat současně dostane prioritu vysílat podle identifikačního čísla či kódu priority (oproti počkání náhodnou dobu a znovuvyslání jako v CSMA/CD)

Kódování

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.
- **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.

Kódování dat

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.

Výtahy zpráv (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 ← nejsou bezpečné pro ukládání hesel
Krypthorafické funkce: bcrypt, argon2(d,di,id),**PBKDF2,SCrypt**

Digitální podpis
Jedná se o 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
  - autentizaci(kdo zprávu podepsal)
  - nepopiratelnost (autor nemůže v budoucnu zapřít, že zprávu podepsal)
- zpráva (soubor) bude čitelná (použitelná) i v případě, že nemáme příslušné nástroje pro ověření její pravosti

Spolehlivost datových přenosů

Typy chybových modelů

- kanály “bez paměti”:
  - AWGN kanál
  - BSC kanál
- kanály “s pamětí”:
  - Gilbert-Elliott 1960

AWGN kanál (Additive white Gaussian noise)

- (jediný) zdroj chyb v kanále je aditivní šum
- nezohledňuje řadu typů chyb (únik, vícecestné šíření, interference, …)
- požití v modelech satelitních komunikací

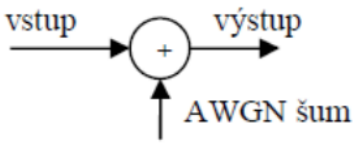
BSC kanál (Binary Symmetric Channel)

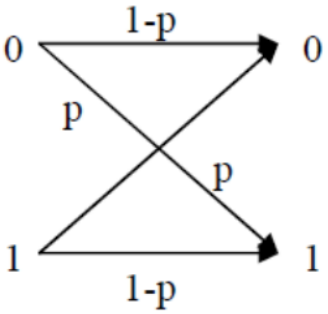
- p – pravděpodobnost chybného přenosu bitu

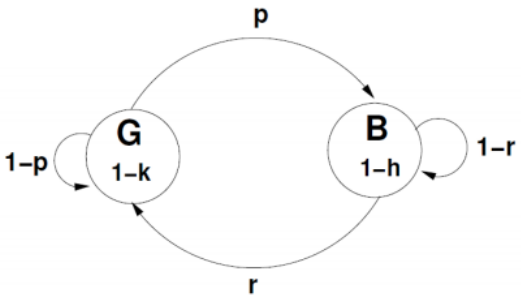
Gilbert-Elliott

- 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 B do stavu G
- 1-k … pravděpodobnost chybného přenosu bitu v G stavu (obvykle = 0)
- 1-h … pravděpodobnost chybného přenosu bitu v B stavu (např. 0.5)





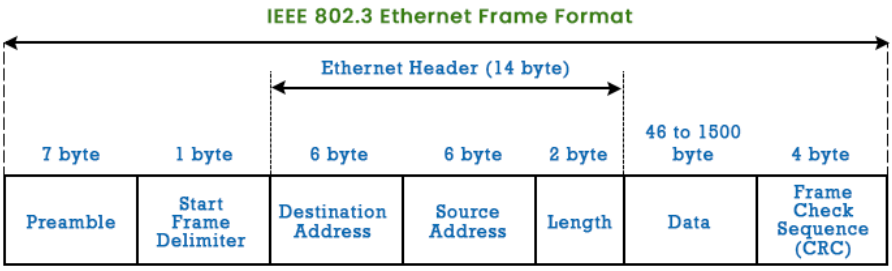


Ethernet

Vznikl počátkem 70. let u firmy Xerox (3 Mbit/s)
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 802.3a

Ethernet Type	Bandwidth	Cable Type	Maximum Distance
10Base-T	10Mbps	Cat 3/Cat 5 UTP	100m
100Base-TX	100Mbps	Cat 5 UTP	100m
100Base-TX	200Mbps	Cat 5 UTP	100m
100Base-FX	100Mbps	Multi-mode fiber	400m
100Base-FX	200Mbps	Multi-mode fiber	2Km
1000Base-T	1Gbps	Cat 5e UTP	100m
1000Base-TX	1Gbps	Cat 6 UTP	100m
1000Base-SX	1Gbps	Multi-mode fiber	550m
1000Base-LX	1Gbps	Single-mode fiber	2Km
10GBase-T	10Gbps	Cat 6a/Cat 7 UTP	100m
10GBase-LX	10Gbps	Multi-mode fiber	100m
10GBase-LX	10Gbp	Single-mode fiber	10Km



Podvrstva MAC využívá CSMA/CD (Carrier Sense Multiple Access with Collision Detection)

propojování v ethernet síti realizováno pomocí:

- opakovače (repeater) - slouží ke zvýšení fyzického dosahu sítě(max 2-4 kvůli zpoždění - pak nefunguje CSMA/CD)
- rozbočovače (hub) - stejné jako repeater, jen více portů
- most (bridge) - sloužily především k filtraci komunikace
- přepínač (switch) - nešíří kolize (hranice kolizní domény je na portu přepínače), převod obecné topologie na stromovou provádí algoritmus Spanning tree

Wi-Fi

Využívají rádiový komunikační kanál

- Výhodou je vysoká flexibilita – žádná nezbytná infrastruktura, kromě napájení
  - jednoduché změny topologie - přemístění uzlů, rozšiřování
- Nevýhodou je potřeba frekvenčního pásma

Rozdělení:

- Ad-hoc sítě(přímá komunikace mezi uzly bez síťové infrastruktury)
- Stacionární sítě (využívá více AP pro pokrytí oblasti, má SSID)

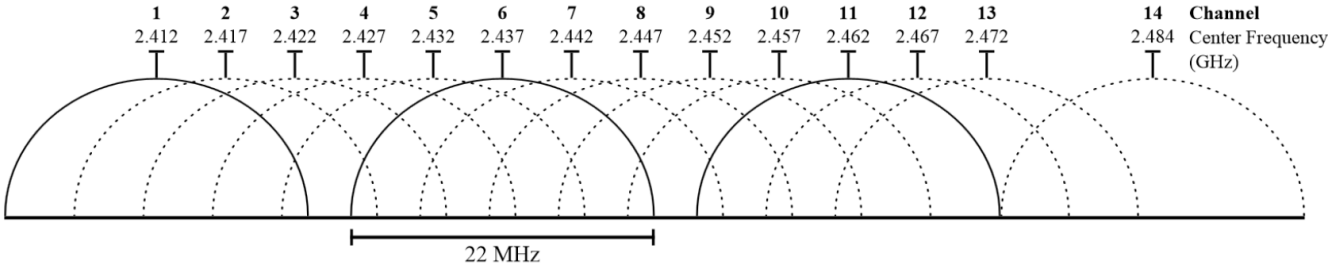
CSMA/CA (…/Collision Avoidance) - přístupová metoda

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
  Zabezpečení: WEP, WPA, WPA2(bloková šifra AES)

Standard	Frequency Band	Bandwidth	Modulation Scheme	Channel Arch.	Maximum Data Rate	Range
802.11	2.4 GHz	20 MHz	BPSK to 256-QAM	DSSS, FHSS	2 Mbps	20 m
b	2.4 GHz	21 MHz	BPSK to 256-QAM	CCK, DSSS	11 Mbps	35 m
a	5 GHz	22 MHz	BPSK to 256-QAM	OFDM	54 Mbps	35 m
g	2.4 GHz	23 MHz	BPSK to 256-QAM	DSSS, OFDM	54 Mbps	70 m
n	2.4 GHz, 5 GHz	24 MHz and 40 MHz	BPSK to 256-QAM	OFDM	600 Mbps	70 m
ah	900 MHz	1, 2, 4, 8, and 16 MHz	BPSK to 256-QAM	SC, OFDM	40 Mbps	1 km

- Pásmo 2.4 GHz je dnes využito následovně
  - 14 částečně se překrývajících kanálů (odstup 5 MHz)
    - 11 USA, 13 Evropa, 14 Japonsko



  - povolen EIRP 100 mW (20 dBm)
  - při použití směrových antén je třeba snížit výkon!!

Adresace na linkové vrstvě

- 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 …)
- 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
- Adresace polohou

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
- uživatelské MAC rámce jsou vždy přiřazeny do právě jedné VLAN
- Spanning Tree algoritmus je implementován pro každou VLAN

Vlastnosti fyzických vrstev

Přenosová média

- Metalické vedení
  - Koaxiální kabel
    - obtížnější instalace, nesnáší ostré ohyby
    - obtížnější připojování
    - dražší cena
    - nižší útlum na jednotku délky
    - vysoká odolnost vůči elektromagnetickému rušení
  - Kroucený dvoudrát (twisted pair)
- Optické vedení
  - odraz světla na rozhraní dvou prostředí s odlišným indexem lomu
  - standardně pouze pro spojení bod-bod
  - **vysoká přenosová kapacita**
  - vysoká odolnost vůči elektromagnetickému rušení
  - obtížný odposlech
  - obtížné spojování
- 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

Topologie

Kruh

Data musí projít všechny uzly mezi odesílatelem a příjemcem. Výpadek jednoho uzlu ochromí celou síť.

Hvězda

Každý počítač je připojený pomocí kabelu k centrálnímu prvku - hubu nebo switchi. Mezi každými dvěma stanicemi existuje vždy jen jedna cesta. To znamená, že selhání jedné stanice neomezí provoz sítě, ovšem kolaps centrálního prvku znamená kolaps i pro celou síť.

Strom

Vychází z hvězdicové topologie spojením aktivních síťových prvků, které jsou v centrech jednotlivých hvězd. V případě, že selže jeden síťový prvek, výpadek ovlivní pouze část sítě pod něj spadající. Ostatní části sítě ale mohou dále pracovat.

Sběrnice

Spojení zprostředkovává jediné přenosové médium (sběrnice), ke kterému jsou připojeny všechny uzly sítě. Má nízké pořizovací náklady, ale omezenou rychlost přenosu a také v ní může docházet ke kolizím. Je vhodná spíše pro malé a dočasné sítě.

Bezpečnost

Bezpečnost na síti se řeší dvěma způsoby:

- Symetrické klíče: Odesílatel má symetrický klíč, tímto klíčem zašifruje zprávu. Příjemce má stejný klíč a pomocí něj zprávu přečte. Je to výpočetně jednodušší než asymetrické klíče, ale je potřeba vyřešit bezpečné předání klíčů. Taky nejde vůbec poznat, kdo zprávu zašifroval. Jakmile klíč unikne, lze pomocí něj přečíst všechny zprávy.
- Asymetrické klíče: Klíč má dvě části, veřejnou a soukromou. Veřejná část je volně přístupná, a je výpočetně nemožné zjistit z ní soukromý klíč. Server, řekněme banka, má u sebe uložený svůj soukromý klíč. Ten dokáže přečíst všechny zprávy, které byly zašifrovány odpovídajícím veřejným klíčem. Veřejný klíč je registrovaný u certifikační autority danou bankou, certifikační autorita potvrzuje, že klíč opravdu patří bance. Klienti posílají svá data bance zašifrovaná pomocí veřejného klíče, a jediná banka je dokáže pomocí svého soukromého klíče číst. Je ale důležité, aby certifikační autorita (klidně i lokální databáze certifikátů) byla důvěryhodná - viz chyba Superfish u Lenova, hodně hezky to vysvětluje computerphile na youtube.
- Podepisování: Ověření pravosti dat. Můžete si to představit jako šifrování naopak, jen tomu nikde tak moc neříkejte. Chceme-li zajistit, že s daty(dokumentem) nebylo nijak manipulování nebo ověřit jejich původce, využijeme právě podpis. Obvyklý postup je vytvoření hashe dokumentu a následně zašifrování pomocí privátního klíče (ten může být součástí certifikátu). Osoba, která chce ověří pravost dokumentu, dešifruje hash pomocí veřejného klíče, spočítá nový hash dokumentu a porovná. Je vhodné mít různý certifikát pro podpis dokumentů a pro ověření identity. Pokud máte stejný, tak při ověřování identity pomocí certifikátu (podepisujete náhodná data), můžete nevědomky podepsat nějaký hash dokumentu a někdo vás tak klamem přinutí k podpisu nějakého dokumentu.

SSL a TLS
Transport Layer Security je novější verze SSL. SSL už je deprecated. Používá symetrickou kryptografii, ale k bezpečnému předání klíčů používá asymetrické klíče (nejčastěji DH key exchange). TLS se používá v HTTPS (bezpečné verzi HTTP), komunikace mezi klientem (K) a serverem (S) se navazuje takto:
K: posílá úvodní packet se seznamem podporovaných šifer a verzí TLS
S: odpovídá, posílá šifru a verzi TLS, která se bude používat a svůj veřejný klíčARP
K: ověří veřejný klíč u certifikační autority. Pokud je platný, tak vygeneruje symetrický klíč (ve skutečnosti vygeneruje Master secret, to je složitější), ten zašifruje pomocí veřejného klíče a pošle serveru
S: přečte zprávu pomocí svého soukromého klíče, tím získal symetrický klíč. Teď mají obě strany symetrický klíč a mohou komunikovat.
Důležitý poznatek: Zejména při používání free nebo sdílených certifikátů, zelený zámeček (HTTPS) neznamená nutně bezpečí. Znamená to jen, že komunikace je šifrovaná a po cestě ji nelze odposlechnout. Nicméně na druhé straně může být klidně satan.
RSA
Asymetrická šifra, která se používá třeba u SSH. Máme náhodná hodně velká prvočísla p a q, a číslo $N = p \times q$, které je veřejně známé. Najdeme e, které je nesoudělné s $\varphi(N) = (p-1)(q-1)$. Najdeme d, aby $e \times d = 1 mod \varphi(N)$.
Veřejný klíč je (N, e), soukromý klíč je (N, d). Zprávu Z zašifrujeme $C = Z^e mod N$, a dešifrujeme $Z = C^d mod N$.
Diffie-Hellmann
Dá se použít k vytvoření symetrického klíče mezi dvěma stranami (Alicí a Bobem) bez pomoci certifikační autority. Máme veřejná čísla p, q, a tajná čísla a od Alice a b od Boba. Alice pošle Bobovi q^a mod p, a Bob pošle Alici q^b mod p. Z toho mohou oba spočítat klíč K = g^(a*b) mod p, ale po

odposlechnutí komunikace nelze kód zjistit.

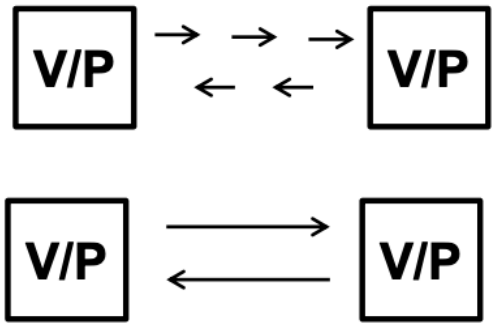
Man in the middle

*Man in the middle (MIM) je útok, během kterého útočník přeruší komunikaci mezi oběma stranami a vede ji přes sebe, u toho pak mění obsah komunikace. V příkladu Diffie-Hellmannovy výměny klíčů může MIM vygenerovat vlastní číslo x, a komunikovat s Alicí pomocí klíče g^(a*x*)* a s Bobem pomocí klíče g^(x*b), uprostřed zprávy rozbalí, přečte a zašifruje pomocí druhého klíče. Ani jeden z komunikujících se nemůže dozvědět, že komunikace byla narušena. Lze se chránit například využitím VPN nebo obecně předem dohodnutým a bezpečně předaným symetrický klíčem.

Typy datových přenosů

Podle směru přenosu

- jednosměrný
  - simplex
- obousměrný střídavý



Podle počtu současně využitých kanálů

- sériový
- paralelní

Podle způsobu synchronizace

- 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)

Sdílení kapacity kanálu

- Frekvenční multiplex - FDM
- Časový multiplex - TDM

- Kombinovaný časový a frekvenční multiplex