1. přednáška

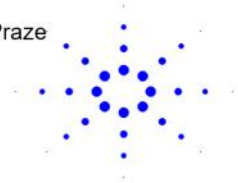
úterý 24. ledna 2023 21:00

1_Intro_ISO-OSI_cz

Počítačové sítě - B4B38PSIA

J. Holub, J. Novák
holubjan@fel.cvut.cz, jnovak@fel.cvut.cz

České vysoké učení technické v Praze
Fakulta elektrotechnická
Katedra měření



Organizace předmětu

- Přednášky:
  - 2 hodiny
  - 2 x test
    - otázky z přednášek
    - max. 2 x 5 bodů
- Cvičení
  - 2 hodinová, 9 týdnů samostatné projekty, poté laboratorní úlohy
  - laboratorní výuka v laboratoři 325
  - semestrální projekty v počítačové učebně 402
- Podmínky získání zápočtu
  - účast na cvičeních
  - zpracované výsledky laboratorních úloh – VČAS !!!
  - odevzdané samostatné projekty – VČAS !!!

Organizace předmětu

- Zkouška
  - písemný test 75 minut
  - otázky dle témat přednášek a cvičení
- Hodnocení
  - Až 10 bodů za testy v semestru
  - Až 20 bodů za rozsah a kvalitu zpracování individuálních projektů
  - Až 70 bodů ze závěrečného testu
  - celkem:
    - ≥ 90 bodů - A
    - ≥ 80 bodů - B
    - ≥ 70 bodů - C
    - ≥ 60 bodů - D
    - ≥ 50 bodů - E
    - < 50 bodů - F

Organizace předmětu – témata přednášek

1. Úvod, základní pojmy, model ISO/OSI.
2. Detekce chyb v datových přenosech, CRC
3. Fyzický kanál (metalický, optický a rádiový) a jeho vlastnosti.
4. Protokoly rodiny TCP/IP.
5. Entropie informačního zdroje, zdrojové kódování, kapacita komunikačního kanálu.
6. Utajování informace, symetrické a asymetrické šifry, distribuce klíčů, certifikáty, digitální podpis.
7. Modely komunikačních kanálů (AWGN, BSC, ...), modulace, komunikace v rozprostřeném spektru.
8. Typy datových přenosů, metody sdílení kapacity kanálu, fyzické a logické topologie.
9. Metody řízení přístupu ke sdílenému médiu a jejich vlastnosti, adresace.
10. ARQ metody, kódy pro detekci a opravy chyb.
11. Propojování distribuovaných systémů, směrování, metody řízení datového toku, QoS
12. Lokální počítačové sítě (IEEE802.3).
13. Bezdrátové technologie (WiFi, Bluetooth, ZigBee).
14. Sběrnice USB.

Organizace předmětu - cvičení

1. Úvod – bezpečnost v laboratoři, Osciloskop.
2. CRC zabezpečení.
3. Reflektrometrická měření.
4. Optické komunikace.
5. Plánování pokrytí bezdrátové sítě.

lab. 325

6. Analýza sítí TCP/IP – Wireshark.
7. Semestrální projekt
8. Semestrální projekt
9. Semestrální projekt
10. Semestrální projekt
11. Semestrální projekt
12. Semestrální projekt
13. Odevzdání projektů a zápočet.

lab. 402

Referenční model ISO/OSI (Open System Interconnection)

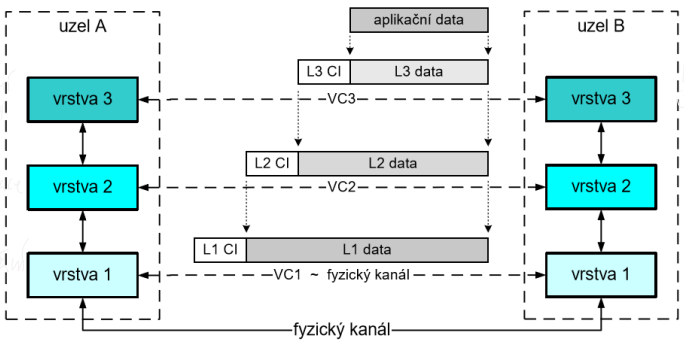
- Definován standardem ISO 7498-1
  - první vydání je již z roku 1984, platné z roku 1994
- Obecný rámec pro návrh protokolů distribuovaných systémů, do nějž jsou zasazována jednotlivá konkrétní řešení
  - většina nových řešení byla navrhována s jeho využitím
  - jiná nikoliv (např. protokoly TCP/IP), ale dnes se je lépe či hůře snažíme tímto rámcem popisovat
- 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

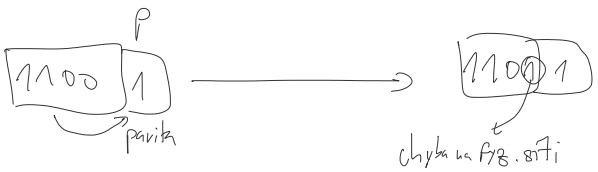
Dělení funkcí do vrstev

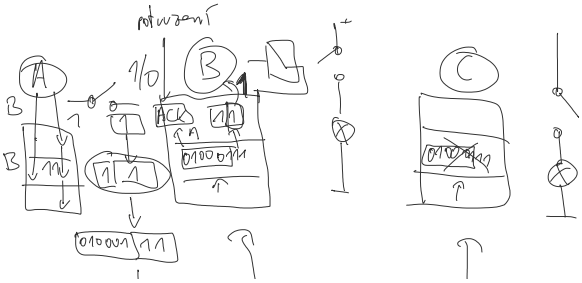
- Implementovat funkční síť je hodně složité a náročné
  - stejná situace jako při řešení velkých SW celků
- Jde o jeden rozsáhlý problém, který se vyplatí dekomponovat
  - rozdělit na menší části, které je možné řešit samostatně
- Zde: dekompozice se provede po hierarchicky uspořádaných vrstvách
  - dobře to odpovídá povaze řešeného problému
  - přináší to i další výhody
    - možnost alternativních řešení na úrovni jednotlivých vrstev
    - modularita

Dělení funkcí do vrstev

- Vrstva N poskytuje služby vrstvě N+1, využívá služeb vrstvy N-1
- Mezi odpovídajícími si vrstvami různých uzlů vznikají virtuální kanály







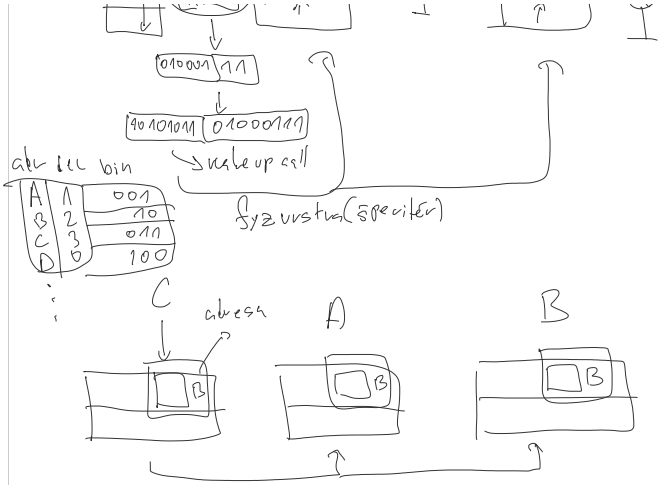
Referenční model ISO/OSI

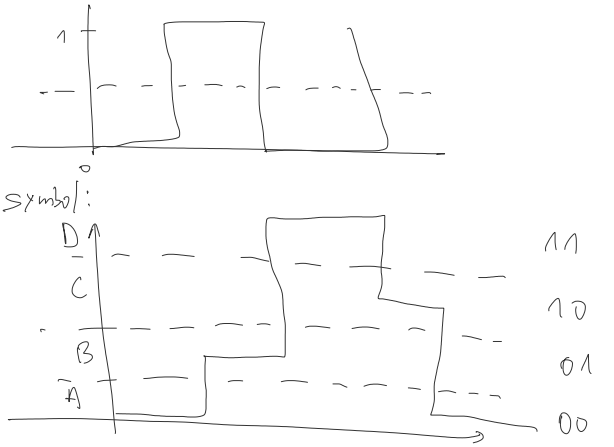
- Počet vrstev byl

Referenční model ISO/OSI

- Počet vrstev byl předmětem sporů
  - dnes se zdá 7 vrstev příliš
- Kritérii bylo:
  - činnosti na stejném stupni abstrakce ve stejné vrstvě
  - minimalizace datových toků mezi vrstvami
  - aplikovatelnost na významné existující standardy (X.25)

Aplikační vrstva
Prezentační vrstva
Relační vrstva
Transportní vrstva
Síťová vrstva
Spojová vrstva
Fyzická vrstva





Fyzická vrstva (Physical Layer)

- Zabývá se výhradně přenosem bitů (symbolů)
  - otázkami typu kódování, modulace, časování, synchronizace, elektrické parametry signálů, konektory, řídicí signály rozhraní, ...
- Nabízí služby typu
  - přijmi bit, odešli bit
- Nijak neinterpretuje to, co přenáší
  - jednotlivých bitům nepřisuzuje žádný specifický význam
- Na úrovni fyzické vrstvy se rozlišuje:
  - paralelní a sériový přenos
  - synchronní, asynchronní a arytmický přenos
  - přenos v základním a přeloženém pásmu
- Příklady standardů fyzické vrstvy:
  - RS-232, RS-485
  - IEEE802.3 (Ethernet), IEEE802.11 (Wi-Fi) …

Spojová vrstva (Data Link Layer)

- 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 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 (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 vrstva (Transport Layer)

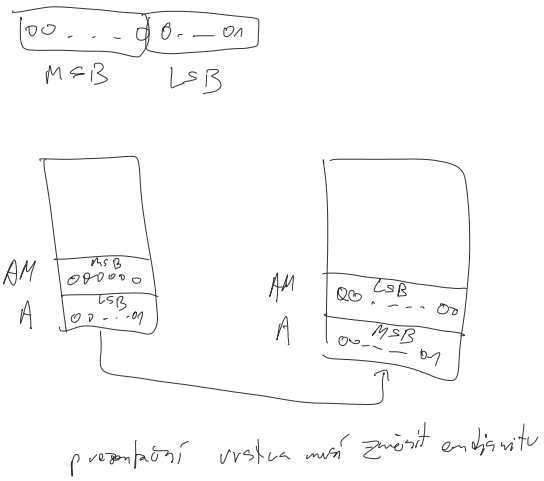
- Vyšší vrstvy mohou mít jiné požadavky na charakter komunikace, než jaký nabízejí nižší vrstvy
- Obvykle nelze měnit vlastnosti a funkce nižších vrstev
  - třeba proto, že patří někomu jinému
  - vyšší vrstvy mohou mít různé (i protichůdné) požadavky
- Úkolem transportní vrstvy zajistit potřebné přizpůsobení!
- 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
  - …

Relační vrstva (Session Layer)

- 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
  - ...

Presentační 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 odesilatele, např. kvůli
  - kódování znaků (ASCII, EBCDIC,...)
  - formátu čísel
    - malý a velký endian
  - formátu struktur, polí
  - ukazatelům (pointerům)
  - atd.
- Prezentační vrstva má na starosti potřebné konverze



Aplikační vrstva (Application Layer)

- 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

A několik souvisejících definic (pouze anglicky)

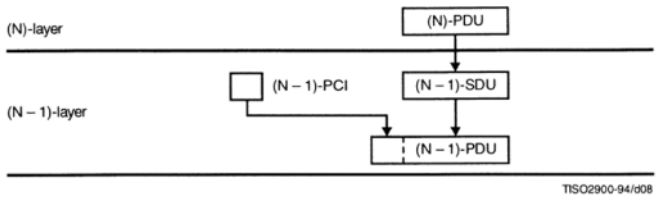
- Layer (N)
  - příslušná vrstva OSI modelu
- Sublayer
  - podvrstva - dělení funkcí vrstvy na dílčí části
- Service (N)
  - služba poskytovaná vrstvou N a vrstvami níže vrstvě N+1
- Entity (N)
  - element vrstvy N realizující část funkcí této vrstvy
- Peer Entities (N)
  - elementy téhož typu v téže vrstvě N v různých uzlech systému
- Protocol (N)
  - sada pravidel (sémantických a syntaktických) definujících komunikaci mezi entitami vrstvy N

A několik souvisejících definic (pouze anglicky)

- 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

A několik souvisejících definic (pouze anglicky)

- Souvislosti



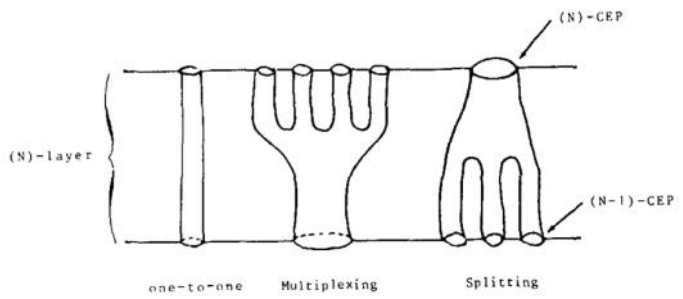
PCI Protocol-control-information
PDU Protocol-data-unit
SDU Service-data-unit

A několik souvisejících definic (pouze anglicky)

- 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 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

A několik souvisejících definic (pouze anglicky)

- Grafické znázornění

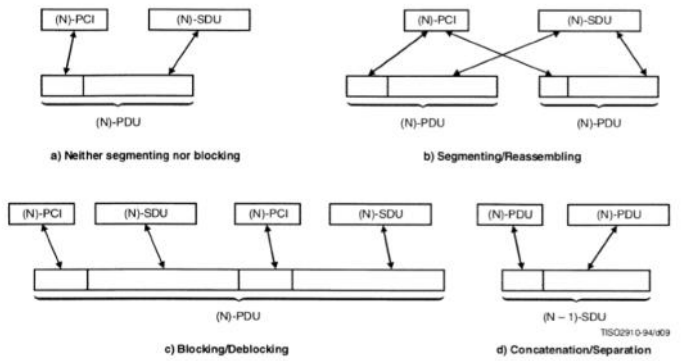


A několik souvisejících definic (pouze anglicky)

- Segmenting – Reassembling (N)
  - funkce entity vrstvy N, kdy jediné SDU N je mapováno do více PDU
- Blocking – Deblocking (N)
  - funkce entity vrstvy N, kdy více SDU je mapováno do jediného PDU
- Concatenation – Separation (N)
  - funkce entity vrstvy N, kdy více PDU vrstvy N je mapováno do jediného SDU vrstvy N-1

A několik souvisejících definic (pouze anglicky)

- Grafické znázornění



2. přednáška

pondělí 27. února 2023 10:08

2_Detekce chyb, CRC...

Počítačové sítě - B4B38PSIA

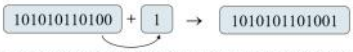
- Chyby v datových přenosech
- Kódy pro detekci chyb

Chyby v datových přenosech

- Typicky k nim dochází ve fyzické vrstvě
  - šum v kanálu
  - vnější nebo vnitřní rušení
- Výjimečně mohou vznikat i ve vyšších vrstvách
  - chyby v implementaci
  - mechanismy detekce chyb nemusí být účinné
    - pokud pracují v nižší nebo ve stejné vrstvě, ve které chyba vznikla
- Projevem je změna hodnoty přenášeného bitu či symbolu
  - jednotlivá chyba
  - shluková chyba délky *n* (*n* je počet pozic mezi první a poslední jednotlivou chybou v datovém bloku)
  - např.:
    - odeslaná data: 1011010111101101101
    - přijatá data: 1011010111100101101 - jednotlivá chyba
    - přijatá data: 1011101101100101101 - bloková chyba délky 9

Detekce chyb

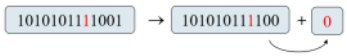
- O vysílaných datech obvykle nelze dělat žádné předpoklady
  - tzn. odesilatel může vyslat jakoukoli posloupnost znaků (bitů, symbolů)
  - příjemce tedy nemá šanci detekovat chyby, jelikož i cestou pozměněná data mohla být odeslána
- Řešením je doplnění užitečných dat o dodatečná (redundantní) data, která jsou s užitečnými daty definovaným způsobem svázána (lze je z užitečných dat dopočítat), např.:



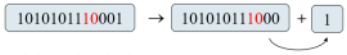
  - redundantní bit reprezentuje tzv. lichou paritu, počet jedniček ve výsledném kódovém slově je liché číslo
- Výsledná kódová slova již nejsou libovolná
  - příjemce předpokládá, že vznikla výše definovaným způsobem a byla tak také odeslána
  - příjemce může zkontrolovat, zda je přijaté slovo kódové (splňuje definovanou podmínku) nebo ne

Detekce chyb

- Dojde-li k jednonásobné chybě



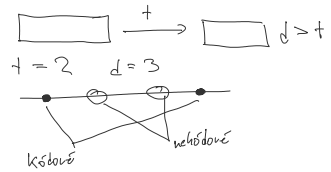
  - počet jedniček v přijatém slově je sudý a přijaté slovo tedy není kódové slovo – nebylo takto odesláno
- ALE !!!!
  - dojde-li ke dvojnásobné chybě

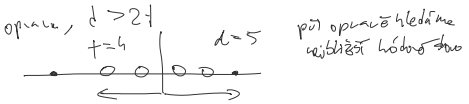


  - chyba není detekována
- Obecně parita detekuje lichý počet chyb, sudý počet není odhalen

Detekce chyb

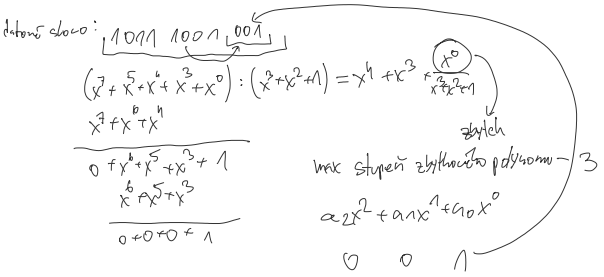
- Definujme termín „Hammingova vzdálenost" dvou kódových slov jako počet znaků, v nichž se liší
- Definujme termín „Hammingova vzdálenost kódu" *d* jako nejnižší počet znaků, v nichž se liší libovolná dvě kódová slova
  - jaká je Hammingova vzdálenost paritního kódu?
- Detekce chyb:
  - množinu všech 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 $d > t$
- A předem můžeme prozradit
  - Kód opravuje *t*-násobné chyby, pokud je Hammingova vzdálenost kódu $d > 2t$
  - Proč? Dokažte!





Cyclic Redundancy Check (CRC)

- CRC patří mezi lineární cyklické kódy
- Cílem je
  - maximalizovat Hammingovu vzdálenost kódu (a tedy schopnost detekovat nejpravděpodobnější chyby), minimalizovat velikost redundantních dat
- Princip
  - *n*-bitová data jsou reprezentována jako binární polynom M(x) stupně *n*-1, kde hodnoty koeficientů polynomu odpovídají jednotlivým datovým bitům
  - datový polynom vydělíme tzv. generujícím polynomem G(x) stupně *k*
  - zbytek po dělení R(x) (*k* bitů) přidáme jako redundantní informaci a kódové slovo délky *n*+*k* odešleme
  - příjemce postup zopakuje a pokud:
    - se nově vypočtený CRC kód (*k* bitů) liší od přijatého CRC kódu (*k* bitů), není přijaté slovo kódové
    - je nově vypočtený CRC kód shodný s přijatým CRC kódem, pak je přijaté slovo slovem kódovým
  - příjem nekódového slova indikuje chybu
  - příjem kódového slova indikuje přenos bez chyby nebo ???



Cyclic Redundancy Check (CRC)

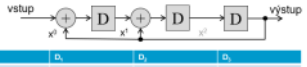
- Příklad
  - data: 1010110010
  - datový polynom:
    $M(x) = 1*x^9 + 0*x^8 + 1*x^7 + 0*x^6 + 1*x^5 + 1*x^4 + 0*x^3 + 0*x^2 + 1*x^1 + 0*x^0$
    $M(x) = x^9 + x^7 + x^5 + x^4 + x^1$
  - generující polynom: $G(x) = x^3 + x + 1$
  - Dělíme:
    $(x^9 + x^7 + x^5 + x^4 + x^1) : (x^3 + x + 1) = x^6 + x^3 + x^2$
    $x^9 + x^7 + x^6$
    $x^6 + x^5 + x^4 + x^1$
    $x^6 + x^4 + x^3$
    $x^5 + x^3 + x^1$
    $x^5 + x^3 + x^2$
    $x^2 + x^1 \rightarrow 110$
  - Zbytek $R(x) = x^2 + x$, odeslané kódové slovo bude 1010110010110

Cyclic Redundancy Check (CRC)

- Příklad – rychlejší způsob výpočtu
  - data: 1010110010
  - datový polynom:
    $M(x) = 1*x^9 + 0*x^8 + 1*x^7 + 0*x^6 + 1*x^5 + 1*x^4 + 0*x^3 + 0*x^2 + 1*x^1 + 0*x^0$
    $M(x) = x^9 + x^7 + x^5 + x^4 + x^1$
  - generující polynom: $G(x) = x^3 + x + 1$, tedy 1011
  - Dělíme:
    1010110010
    1011
    1110010
    1011
    101010
    1011
    110 → $x^2 + x$
  - Zbytek $R(x) = x^2 + x$, odeslané kódové slovo bude 1010110010110

Cyclic Redundancy Check (CRC)

- Příklad – HW implementace výpočtu
  - data: 1010110010
  - generující polynom: $G(x) = x^3 + x + 1$
  - dělička:

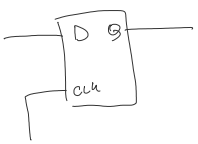


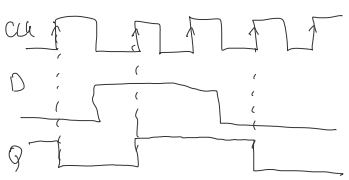
Vstup	D_1	D_2	D_3
-	0	0	0
1	1	0	0
0	0	1	0
1	1	0	1
0	1	0	0
1	1	1	0
1	1	1	1
0	1	0	1
0	1	0	0
1	1	1	0
0	$0 + x^3$	$1 + x^1$	$1 + x^2$

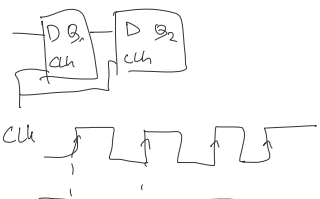
Cyclic Redundancy Check (CRC)

- Alternativní postup
  - *n*-bitová data jsou reprezentována jako binární polynom M(x) stupně *n*-1, kde

D-flip-flop (klopný obvod typu D)







Cyclic Redundancy Check (CRC)

- Alternativní postup
  - *n*-bitová data jsou reprezentována jako binární polynom M(x) stupně *n*-1, kde hodnoty koeficientů polynomu odpovídají jednotlivým datovým bitům
  - tento polynom vynásobíme x^k, kde *k* je stupeň generujícího polynomu
    - tedy přidáme *k* nul zprava
  - výsledný polynom x^k M(x) vydělíme generujícím polynomem G(x) stupně *k*
  - zbytek po dělení R(x) (*k* bitů) přičteme k polynomu x^k M(x) a kódové slovo x^k M(x) + R(x) délky *n*+*k* odešleme
  - příjemce vydělí přijatý polynom N(x) stupně *n*+*k*-1 generujícím polynomem G(x) a pokud
    - je zbytek po dělení roven nule, pak je přijaté slovo kódové
    - je zbytek po dělení nenulový, pak přijaté slovo není kódové
  - Důkaz: x^k M(x) = Q(x).G(x) + R(x)

$$[\, x^k M(x) + R(x)\,] \,/\, G(x) = Q(x).G(x)/G(x) + [R(x) + R(x)]/G(x)$$

zbytek 0 zbytek 0

CRC – detekční schopnosti

- 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) neděli 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))

CRC – detekční schopnosti

- Tvrzení: lze detekovat všechny jednonásobné chyby, pokud gen. polynom obsahuje alespoň dva členy
- Důkaz: $E(x) = x^i$, $i \geq 0$ $G(x) = x^a + x^b$, $a > b$, zároveň $a,b \geq 0$
  pokud i < a, pak $R(x) = x^i$
  pokud i ≥ a, pak $E(x)/G(x) = x^{i-a}$, $R(x) = x^{i-a+b}$

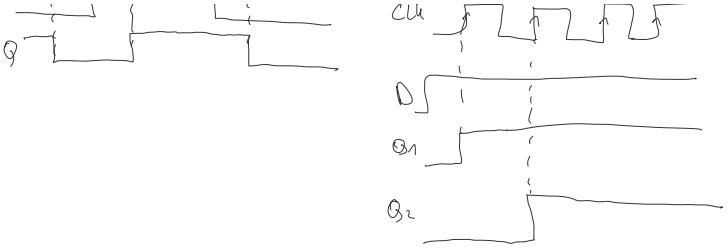
- Tvrzení: lze detekovat všechny dvojnásobné chyby, pokud generující polynom má alespoň dva členy a nedělí (x^m + 1) pro všechna *m* < délka kódového slova
- Důkaz: $E(x) = x^i + x^j$, $i > j = x^j.(x^{i-j} + 1)$
  G(x) neděli beze zbytku x^j
  zbytek již vyplývá z výše uvedeného tvrzení

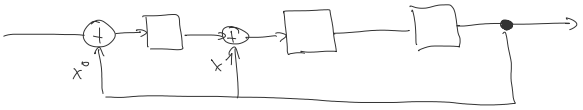
CRC – detekční schopnosti

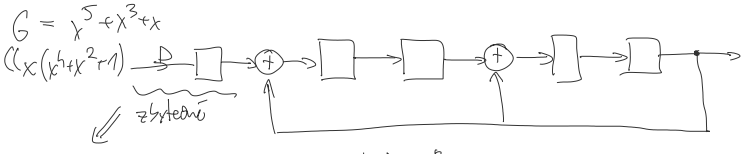
- Tvrzení: lze detekovat všechny chyby liché násobnosti, pokud je generující polynom beze zbytku dělitelný (x + 1), tzn. G(x) = (x+1)G'(x)
- Důkaz: Předpokládejme, že E(x) má lichý počet členů a současně je dělitelný (x + 1)
  - z dělitelnosti vyplývá:
    E(x) = (x + 1) T(x)
    pokud x = 1, pak E(1) = (1 + 1) T(1) = 0
  - z lichého počtů členů ale současně vyplývá:
    E(1) = 1 , sčítáme lichý počet jedniček
  - z toho vyplývá, že E(x) ≠ (x + 1) T(x)

CRC – detekční schopnosti

- Tvrzení: lze detekovat všechny shlukové chyby délky ≤ *k*, kde *k* je stupeň G(x), pokud G(x) obsahuje nenulový konstantní člen
- Důkaz: $E(x) = x^i (x^{t-1} + \ldots + 1)$, $i \geq 0$, $t \geq 2$ je shluková chyba délky *t*
  - pokud G(x) má člen x^0 a současně *t* ≤ *k*, pak E(x) není dělitelné G(x), protože:
    - x^i není dělitelné G(x)
    - $(x^{t-1} + \ldots + 1)$ není dělitelné G(x)
- Tvrzení: lze detekovat **téměř** všechny shlukové chyby délky *k+1*, kde *k* je stupeň G(x), pokud G(x) obsahuje nenulový konstantní člen
- Důkaz: $E(x) = x^i (x^{t-1} + \ldots + 1)$, $i \geq 0$, $t \geq 2$ je shluková chyba délky *t*
  - pokud G(x) má člen x^0 a současně t = k+1, pak
    - x^i není dělitelné G(x)
    - $(x^k + \ldots + 1) = S(x)$ je dělitelné G(x) pouze pokud S(x) == G(x),
    - S(x) má (*k*+1) členů, koeficienty u prvního a posledního jsou vždy 1a tedy (k-1) koeficientů může být buď 0 nebo 1, tedy 2^{k-1} variant, z toho jedna odpovídá G(x)
  - pravděpodobnost detekce chyby je tedy $1 - 2^{-(k-1)}$





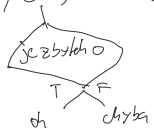


v praxi vždy generující polynom obsahuje x^0

$M(x) \,/\, G(x) = Q(x) + \frac{R(x)}{G(x)}$ ... 110101,000

$(M(x) \cdot x^k) \,/\, G(x) = Q(x) + \frac{R'(x)}{G(x)}$

$[(M(x) \cdot x^k) + R'(x)] \,/\, G(x) = Q'(x)G(x) + \frac{R'(x)}{G(x)} + \frac{R'(x)}{G(x)}$



$N(x) = M(x) \,|\, R(x)$

$N(x) + E(x) = N'(x)$

111 0001 → 1101001

$E(x) = x^6 + x^3$ → koeficienty tam, kde nastala chyba

$(x^6+x^5+x^4+x^0) + (x^6+x^3)$

$x^5+x^4+x^3+x^0 = N'x$

$N(x) = [M(x)x^k + R(x)]$

$N(x) + E(x)\ G(x)$

pokud $E(x) \,|\, G(x)$ nenulový zbytek, chybu neopravíme
chyba je detekována, pokud G(x) nedělí E(x) beze zbytku

$S(x) = x^t + \ldots + x^0$

2^{k-1}, pravděpodobnost, že chyba nebude detekována je: $\frac{1}{2^{k-1}}$

CRC – detekční schopnosti

- Tvrzení: lze detekovat **téměř** všechny shlukové chyby délky > *k+1*, kde *k* je stupeň G(x), pokud G(x) obsahuje nenulový konstantní člen
- Důkaz: Nechť polynom M(x) reprezentuje *n*-bitové datové slovo. Stupeň polynomu M(x) je tedy *n-1*. Pak:
  - existuje 2^n různých datových slov, z nich 2^{n-k} má shodné CRC a jen jedno z nich je to správné (skutečně odeslané)
  - pravděpodobnost, že chyba nebude detekována je tedy:

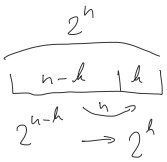
$$(2^{(n-k)} - 1) / 2^n \approx 2^{-k} \quad \text{(pro velká n)}$$

všechna špatná bližší slova → všechna slova

- Příklady vhodných generujících polynomů

Kód	generující polynom g(x)	stupeň g(x)
CRC – 12	$x^{12}+x^{11}+x^3+x^2+x+1$	12
CRC – 16	$x^{16}+x^{15}+x^2+x^2+1$	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

$\underbrace{(1-N)}_{\text{určitě detekují}}$ $\underbrace{N+1}_{\text{mohou detekovat, není jisté}}$



2^n

$\boxed{n-k \mid k}$

$2^{n-k} \xrightarrow{n} 2^k$

3. přednáška

pondělí 6. března 2023 9:14

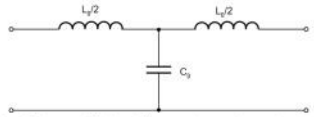
3_Media

Počítačové sítě - B4B38PSIA

- Systémy s rozprostřenými parametry
- Metalický, optický a rádiový přenosový kanál a jeho vlastnosti.

Metalická přenosová cesta

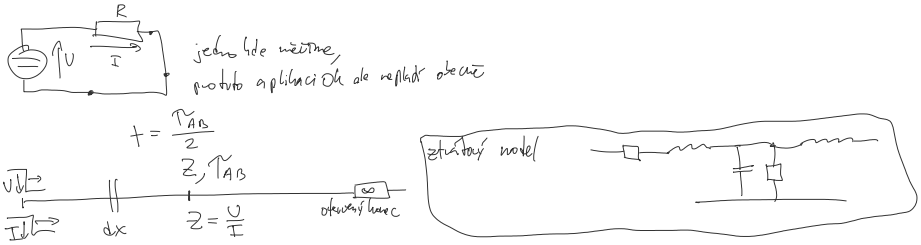
- Prvek bezeztrátového modelu metalického vedení



- L_0 a C_0 představují indukčnost a kapacitu na jednotku délky – označujeme je jako primární parametry

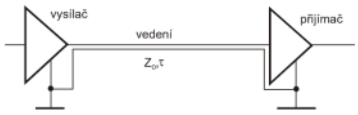
$$Z_0 = \sqrt{\frac{L_0}{C_0}} \qquad \tau = \sqrt{L_0 . C_0}$$

- Z_0 je charakteristická impedance vedení
- τ je zpoždění na jednotku délky
  - označujeme je jako sekundární parametry

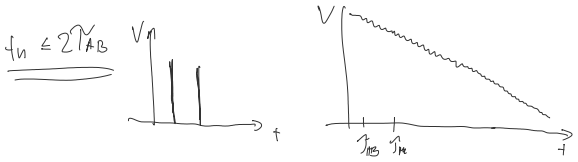


Metalická přenosová cesta

- Metalický komunikační kanál se skládá ze 3 částí



- 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



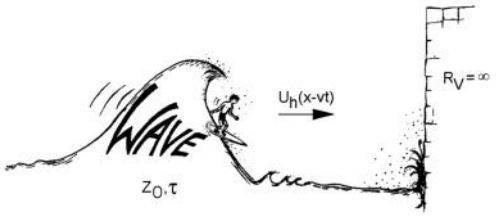
Metalická přenosová cesta

- Parametry základních typů metalických vedení

	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 – zem)	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
sběrnicový signál na plošném spoji	5 - 10	10 - 30	20 - 40	10 - 20

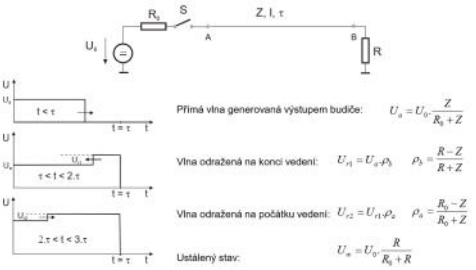
Metalická přenosová cesta

- Šíření číslicového signálu vedením - analogie



Metalická přenosová cesta

- Šíření číslicového signálu vedením



$I_a = I_L + I_R$

$\frac{U_a}{Z} = \frac{U_r}{Z} + \frac{U_a + U_r}{R}$

$U_a R = U_r R + U_r Z + U_r Z$

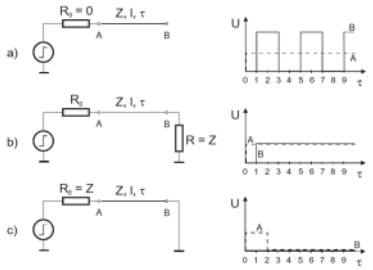
$U_a (R - Z) = U_r (R + Z)$

$U_r = U_a \cdot \frac{R - Z}{R + Z}$

$\rho_B = \frac{R - Z}{R + Z}$ $\rho_B' = \frac{Z - R}{R + Z}$

Metalická přenosová cesta

- Šíření číslicového signálu vedením - příklady



Metalická přenosová cesta – 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)

Metalická přenosová cesta

- Koaxiální kabel
  - charakteristická impedance typicky 50 nebo 75 Ω
  - 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 konektorování, dražší konektory
    - obtížnější instalace, nesnáší ostré ohyby
    - obtížnější připojování
    - vyšší cena

Metalická přenosová cesta

- 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 Ω
  - obvykle symetrické (*differential*) vedení
  - flexibilní, snadné napojování, konektorování
  - relativně levné

Metalická přenosová cesta

- Kroucený dvoudrát – 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 sítě token-ring 4 Mb/s
  - Kategorie 3 – pro datové sítě s šířkou pásma do 16 MHz
    - nejrozšířenějším příkladem je IEEE802.3 - 10BaseT
    - dnes se ještě používá pro rozvod klasické telefonie v budovách

Metalická přenosová cesta

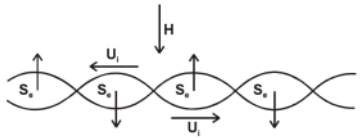
- Kroucený dvoudrát – dělení do kategorií podle EIA/TIA 568B
  - Kategorie 4 – dnes již není EIA/TIA specifikována
    - původně pro datové sítě s šířkou pásma do 20 MHz
    - token-ring 16 M/s, 10BaseT, 100BaseT4
  - Kategorie 5 – dnes již není EIA/TIA specifikována
    - kabel pro datové sítě s šířkou 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 sítě s šířkou pásma do 100 MHz
    - vhodný pro 100BaseTX i 1000BaseT Ethernet

Metalická přenosová cesta

- Kroucený dvoudrát – dělení do kategorií podle EIA/TIA 568B
  - Kategorie 6 – pro datové sítě s maximální šířkou pásma do 250 MHz
    - vyhovuje pro 1000BaseT Ethernet
  - Kategorie 6a – pro datové sítě s maximální šířkou pásma do 500 MHz
    - na specifikaci se pracuje
    - měla by vyhovovat pro 10Gb Ethernet
- ISO/IEC 11801 definuje kabel kategorie 7 (až 600 MHz)
  - jednotlivé páry jsou stíněny
  - využití pro 10Gb Ethernet na větší vzdálenosti

Metalická přenosová cesta

- Kroucený dvoudrát – 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

Metalická přenosová cesta

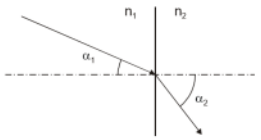
- „Nějaká“ dvojice vodičů
  - charakteristická impedance typicky 120 Ω a více
    - v průběhu vedení se mění tak, jak kolísá vzdálenost vodičů
    - tím dochází k útlumu vlivem odrazů
  - s rostoucí vzdáleností vodičů stoupá „indukčnost“ vedení a tím i citlivost k vnějšímu rušení
  - útlum takovéto dvojice 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:



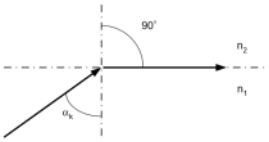
$$n_1.\sin\alpha_1 = n_2.\sin\alpha_2$$

Optická přenosová cesta

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

$$\alpha_k = \arcsin\left(\frac{n_2}{n_1}\right) \qquad (\sin 90° = 1)$$

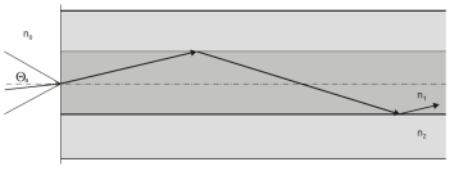
- pro $\alpha_1 > \alpha_k$ dochází k totálnímu odrazu světla na rozhraní



Optická přenosová cesta

- důležitým parametrem vlákna je numerická apertura

$$NA = n_0.\sin\Theta_a$$

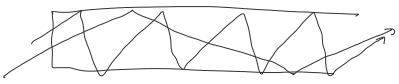


- pro vstup paprsku ze vzduchu ($n_0 \approx 1$) odpovídá numerická apertura sinu maximálního vstupního úhlu

Optická přenosová cesta

- 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)



Optická přenosová cesta

- Optická vlákna
  - 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

Optická přenosová cesta

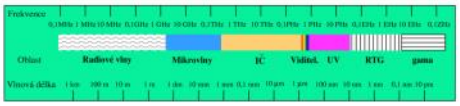
- Optická vlákna
  - používají se zejména ty vlnové délky, na nichž je nejnižší útlum (absorbce)
    - skleněná vlákna - 850 nm, 1300 nm, 1500 nm
    - plastová kolem 650 nm – 680 nm
  - útlum vláken je v závislosti na provedení, technologii výroby a vlnové délce světla v rozsahu jednotek až stovek dB/km
  - 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 aplikací pro parametrizaci a sběr dat (např. místní odečet elektroměrů)
  - Laserová komunikace
    - úzce směrová
    - velký dosah a vysoké přenosové rychlosti
    - utajení → vojenské aplikace (družice)

Bezdrátová přenosová cesta

- 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

Bezdrátová přenosová cesta

- 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
  - 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

Bezdrátová přenosová cesta

- Rozsahy rádiových vln dle IEEE 521

Symboly	Rozsah kmitočtů
HF	3 - 30 MHz
VHF	30 - 300 MHz
UHF	300 - 1000 MHz
L	1 - 2 GHz
S	2 - 4 GHz
C	4 - 8 GHz
X	8 - 12 GHz
Ku	12 - 18 GHz
K	18 - 27 GHz
Ka	27 - 40 GHz
V	40 - 75 GHz
W	75 - 110 GHz
mm	110 - 300 GHz

Bezdrátová přenosová cesta

- 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

$$f = \frac{c}{\lambda} \qquad [\mathrm{Hz, m/s, m}]$$

  - 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

Bezdrátová přenosová cesta

- Šíření elmag. vln prostředím
  - 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 …
    - na určitých frekvencích lze s dostatečným výkonem dosáhnout spojení téměř s libovolným místem na zemi

Bezdrátová přenosová cesta

- Šíření elmag. vln prostředím
  - 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)

Bezdrátová přenosová cesta

- Regulace rádiové komunikace
  - World Radiocommunications Conference (WRC)
    - jednání na úrovni států
    - výsledky jsou zahrnuty v radiokomunikačním řádu
  - radiokomunikační řád definuje
    - způsob využití frekvenčního spektra
    - rozdělení pásem
    - využití frekvenčních rozsahů jednotlivými službami
    - zásady pro koexistenci rádiových zařízení na shodných nebo blízkých frekvencích
    - koordinuje přidělování frekvenčního spektra novým zařízením a službám

Bezdrátová přenosová cesta

- 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.

Laboratory

středa 15. března 2023 13:36

$$(x^2+1)(x+1) = x^3+x^2+x+1$$

$$(x^3+x+1)(x^4+1) = x^7+x^5+x^4+x^3+x+1$$

File size 1 MB

S & W			
delay	0	10	15
time	41,25	31,45	52,6

5
263

selective repeat

window size	2	5	10	15	
delay @ 10	215,1	100,1	58,4	48,4	?

delay @ 10	215,1	100,1	58,4	48,4
delay @ 50	56,59	25,16	20,8	14,9
delay @ 100	496,2	211,7	113,1	81,9

4. přednáška

pondělí 20. března 2023 9:24

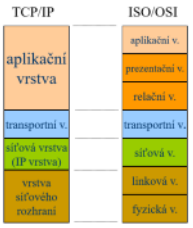
4_TCPIP

Počítačové sítě - B4B38PSIA

- Protokolový zásobník
- IP adresy
- IPv4, IPv6
- ICMP, ARP a NDP
- UDP, TCP
- DNS

Historie TCP/IP, ISO/OSI Model

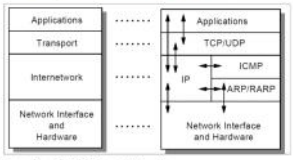
- TCP/IP je starší
  - neodpovídá plně ISO/OSI
- Vývoj v 70. letech minulého století
- 1971 - ARPANET working group
  - financováno DARPA
  - spolupráce ITU, ISO
- 1978 – dokončeno
- 1980 – ARPANET přechází na TCP/IP
- 1983 – otevřená TCP/IP implementace v BSD Unixu



Další vývoj TCP/IP

- 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 sítě
- …

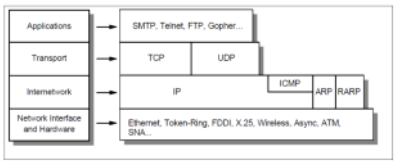
Protokolový zásobník TCP/IP



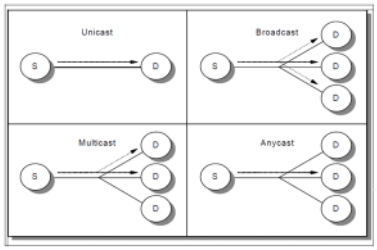
- Nebyl navržen dle OSI modelu, ale
  - Network interface and hardware ≈ fyzická a spojová vrstva
  - Internetwork ≈ síťová vrstva
  - Transport ≈ transportní vrstva
  - Applications ≈ relační až aplikační vrstva

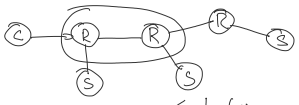
Protokolový zásobník TCP/IP

- Příklady protokolů jednotlivých vrstev
  - nejedná se o kompletní sady protokolů TCP/IP



IP Protokol – Doručení dat na IP adresu





výběr příjemce za nás řeší routery (při anycastu)

IP Protokol – Doručení dat na IP Adresu

- 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)

2^{32} 32 bit IPv4

2^{128} 128 bit IPv6

IP 00001010 ... 0 00001111

MAC – zůstává stejný ze stejným fyz. zařízením

Jak by "fungovalo" doručování pouze pomocí MAC:

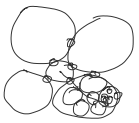
povrch Země $S = 4\pi R_Z^2$

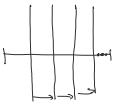
$S = 4\pi \cdot (6371000)^2$

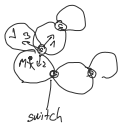
$\frac{2^{128}}{4\pi (6371000)^2} = 6671 \cdot 10^{20}$ IPv6/m²

$6{,}671 \cdot 10^{23}$ IPv6/m²

N H







Tabulka switche:

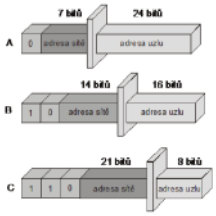
M	2
J	3

IP Protokol – 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

IP Protokol – třídy adres

- 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



IP Protokol – IP Adresy

- 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, zbývající 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

Maska podsítě

11 . . . . 1111 | 00 . . . 0

určuje, kde je definována hranice v ip. adrese

může 255.255.240.0

ale ne 255.255.240.15!

↳ tohoto odpovídá 1111 . . . 0001111

IP Protokol – IP Adresy

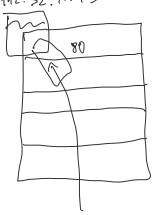
- Vyhrazené IPv4 adresy
  - netid, hostid=0: adresa sítě (147.229.0.0)
  - netid=0, hostid: adresa uzlu (0.0.0.5)
  - 255.255.255.255 limited broadcast (omezená všeobecná adresa), neprochází přes router
  - netid, hostid=11..1 directed broadcast (147.229.255.255), řízená všeobecná adresa
  - 127.x.x.x 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

IP Protokol – IP Adresy

- 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
  - 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

IPv6 2^{128}
IPv4 2^{32}

192.32.1.15 (:80) ← není nutno
dobře známé porty



IP Protokol – IP Adresy

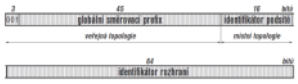
- Zápis IPv6 adresy v tzv. kanonickém tvaru
  - šestnáctková čísla malými písmeny
  - vynechání počátečních nul je povinné
  - konstrukce „::" musí mít maximální efekt
    - dvojici „::" se musí použít na nejdelší (případně první) sekvenci nul
- Při použití v URL se IPv6 adresa uzavírá do hranatých závorek
  - 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

IP Protokol – IP Adresy

- Typy IPv6 adres
  - ::/128 - nedefinovaná adresa
  - ::1/128 - loopback
  - 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
  - aktuální info lze nalézt na
    - http://www.iana.org/assignments/ipv6-address-space
- Známé prefixy
  - 64:ff9b::/96 - adresy s vloženou IPv4 (IPv6 klient, IPv4 server – NAT64)
  - 2002::/16 - přenos IPv6 přes IPv4 sítě

IP Protokol – IP Adresy

- Globální individuální IPv6 adresa
  - 2000::/3

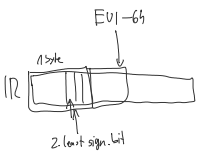


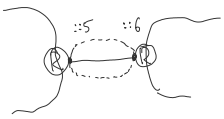
- Globální směrovací prefix
  - typicky 48 bitů
    - i delší pro malé sítě
  - identifikuje koncovou síť, přidělen zmocněnou autoritou zvenčí
- Identifikátor podsítě
  - typicky 16 bitů
- Identifikátor rozhraní
  - vždy 64 bitů (kromě adres s prefixem ::/3)

IP Protokol – IP Adresy

- Identifikátor rozhraní
  - vždy 64 bitů (kromě adres s prefixem ::/3)
  - odvozen dle IEEE EUI-64
- Pokud rozhraní již EUI-64 identifikátor má
  - převezme se s invertovaným druhým nejméně významným bitem nejvyššího bajtu
    - tzv. modifikované EUI-64
    - kvůli snadnému vytváření jednoduchých lokálních identifikátorů
  - příznak globality
    - EUI-64 - 0 celosvětově globální, 1 lokální identifikace
    - modifikované EUI-64 – opačně
- Vytvoření modifikovaného EUI-64 z Ethernet MAC adresy

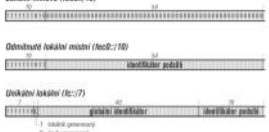
MAC – 6B





IP Protokol – IP Adresy

- Individuální lokální IPv6 adresy
  - podobné neveřejným adresám v IPv4



  - následuje modifikovaný EUI-64 identifikátor, hostitel si je generuje sám
- Unikátní lokální adresy (náhrada site-local)
  - příznak L = 0 pro budoucí centrální autoritu, zatím vše lokálně
  - „unikátní" globální identifikátor (hash adresy a času generující stanice)

IP Protokol – IP Adresy

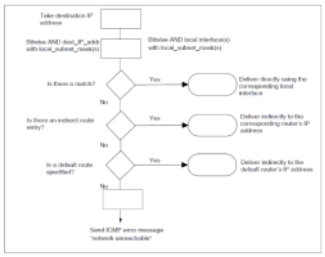
- Skupinové IPv6 adresy

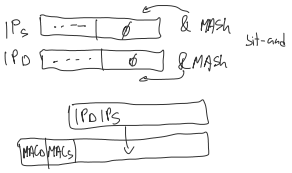
– nesmí být použita jako adresa odesilatele, adresy ff0x::0 jsou rezervovány

IP Protokol – IP Adresy

- 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 (lokalitě)
    - 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, volné 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

IP Protokol – IPv4 „Transmission Routing“





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

IPv4 paket

– Volby – třibitové 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 odesilatele
– Cílová adresa – IP adresa příjemce
– Volby – rozšíření o další funkce, běžně se nepoužívá
– Padding – zarovnání pole Volby na 32 bitů

IPv6 paket

– 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)

IPv6 Paket – zřetězené hlavičky

- 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

IPv6 Paket – zřetězené hlavičky

- Rozšiřující hlavičky – položka Další hlavička (Next header)
  - pořadí je předepsáno (kvůli náročnosti a rychlosti zpracování)

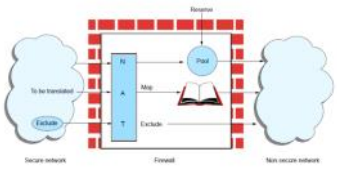
a) bez rozšiřujících hlaviček

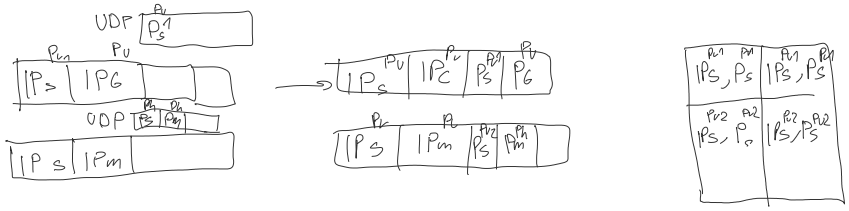
b) s hlavičkou *Směrování*

c) s hlavičkami *Směrování* a *Fragmentace*

NAT – Network Address Translation

- Předpokladem je, že pouze nízký počet uživatelů z privátní sítě potřebu současně přístup do veřejného Internetu
- Jejich privátní adresa je při přechodu do veřejné části sítě nahrazena adresou veřejnou (přeložena) a naopak





Problémy s překladem adres

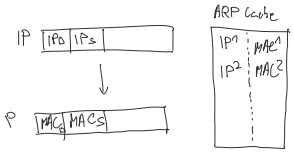
- Network Address Translation (NAT)
  - NAT by měl být transparentní pro komunikující uzly
    - vyžaduje nový výpočet CRC v hlavičkách vyšších vrstev
    - problém např. s FTP - IP adresa je i v datovém poli aplikačního paketu, musí být také správně přeložena
    - I další aplikace mohou mít obdobné problémy
  - otázka – kdy vracet veřejnou adresu do bloku adres volných pro překlad?
    - IP protokol je bezestavový – nejsme schopni zjistit, zda bude komunikace pokračovat
    - TCP poskytuje informaci o stavu 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 portu je nahrazeno „fragmentation ID" ve fragmentech
  - uzel ve veřejné síti pak není schopen rozlišit pakety s tímtéž „fragmentation ID" od dvou různých privátních uzlů
    - nepravděpodobné, leč možné

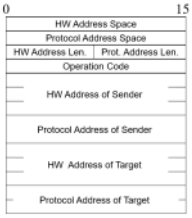
ARP Protokol

- 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 IP→MAC
    - 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 odesilateli ARP dotazu
  - ARP cache lze aktualizovat při příjmu ARP žádostí
    - možná jen aktualizace, nikoliv vytvoření nového záznamu



ARP Protocol

- Address Resolution Protocol



  - 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 odesilatele
  - Protocol Address of Sender
    - IP adresa odesilatele
  - HW Address of Target
    - cílová MAC adresa
  - Protocol Address of Target
    - cílová IP adresa

ICMP 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

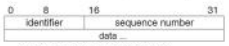
ICMP Protocol

- ICMPv4 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

ICMP Protokol

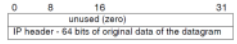
- Echo a Echo reply
  - struktura datového pole ICMP zprávy



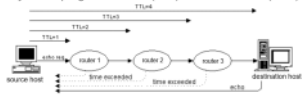
  - používá např. aplikace ***ping***
    - odesilatel vyšle zprávu echo (8) k cíli
    - cíl odpoví zprávou echo reply (0) odesilateli
    - lze např. testovat, zda jsou hostitel či router aktivní
  - zpracování zprávy echo může být administrátorem z důvodu bezpečnosti zakázáno
    - na hostiteli
    - na routeru
  - využito také aplikací ***tracert*** jako testovací paket
    - viz následující slajd

ICMP Protocol

- Time Exceeded
  - struktura níže je v datové části ICMP zprávy

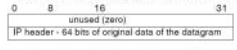


  - pole ***code*** poskytuje podrobnou informaci
    - 0 – transit TTL exceeded
    - 1 – reassembly TTL exceeded
  - využito v programu tracert (Win) nebo traceroute (Unix)

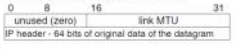


ICMP Protocol

- Destination Unreachable
  - struktura níže je v datové části ICMP zprávy



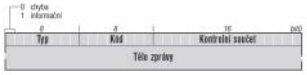
  - pole ***code*** poskytuje podrobnou informaci
    - 0 – network unreachable
    - 1 – host unreachable
    - 2 – protocol unreachable
    - 3 – port unreachable
    - 4 – fragmentation needed but disabled



    - …

ICMP Protocol

- ICMP v6 zpráva



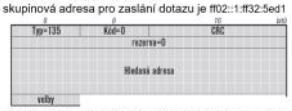
  - 1 – cíl nedosažitelný
  - 2 – příliš velký paket
  - 3 – vypršela životnost paketu
  - 4 – problém s parametry (chybné kódy v hlavičce)
  - 128 – echo request
  - 129 – echo reply
  - …
- kód definuje specifický kód chyby

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)

NDP Protokol

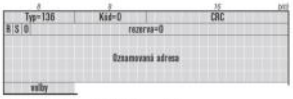
- Neighbor Discovery Protocol
  - hledání souseda
    - skupinové adresy s prefixem ff02:0:0:0:0:1:ff00::/104
    - posledních 24 bitů hledané adresy se připojí za tento prefix
  - příklad (hledáme linkovou adresu pro 2001:db8:1:1:022a:fff:fe32:5ed1)
  - skupinová adresa pro zaslání dotazu je ff02::1:ff32:5ed1



  - ve volitelných položkách může poslat vlastní linkovou adresu
    - kvůli odeslání odpovědi

NDP Protokol

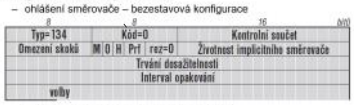
- Neighbor Discovery Protocol
  - ohlášení souseda
    - odpověď na výzvu



    - R – router, S – solicited, O - override
    - oznamovaná adresa je IP adresa
    - linková adresa je ve volitelných položkách
  - může být i nevyžádané (změna linkové adresy)
    - multicast na ff02::1

NDP Protokol

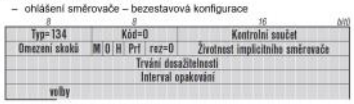
- Neighbor Discovery Protocol
  - ohlášení směrovače – bezestavová konfigurace



  - Omezení skoků – doporučení pro IP hlavičku
  - M | O – Managed | Other statefull
    - 1 | X – vše prostřednictvím DHCPv6
    - 0 | 1 – adresa, prefix, směrování, ostatní přes DHCPv6
    - 0 | 0 – DHCPv6 není k dispozici
  - H – podpora mobility
  - Prf – priorita implicitního směrovače (pokud je životnost nenulová)

NDP Protokol

- Neighbor Discovery Protocol
  - ohlášení směrovače – bezestavová konfigurace



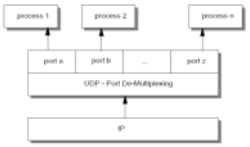
  - životnost implicitního směrovače
    - čas v sekundách, jak dlouho lze využívat
  - trvání dosažitelnosti
    - jak dlouho považovat uzel za dosažitelný po ověření dosažitelnosti
  - interval opakování
    - interval mezi dvěma výzvami sousedovi při ověřování dosažitelnosti
  - ve volbách může být linková adresa směrovače, prefix sítě, jeho časová platnost, MTU …

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 …)
    - původně definovány organizací IANA, dnes přidělovány ICANN
  - soket (socket)
    - struktura definující komunikační kanál pro aplikaci (výše popsaná trojice)
      - první implementace v BSD soketech (BSD Unix)

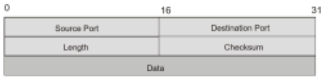
UDP Protokol

- 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 ….



UDP Packet

- Hlavička paketu



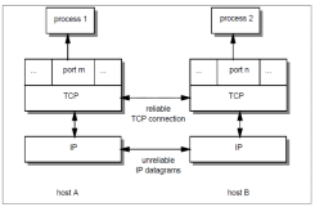
  - velikost 8 bajtů
  - Source Port – číslo portu odesilatele
  - Destination Port – číslo portu příjemce
  - Length – délka UDP paketu
    - včetně UDP hlavičky a datového pole
  - Checksum – kontrolní součet (volitelný)
    - včetně tzv. pseudo-IP hlavičky, UDP hlavičky a dat

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
  - řízení datového toku
    - mechanismus okének
  - segmentace dat do paketů

TCP Protokol

- Spolehlivý spojovaný plně duplexní komunikační kanál



TCP Paket

- Hlavička TCP paketu

0	1	2	3
0 1 2 3 4 5 6 7 8 9	0 1 2 3 4 5 6 7 8 9	0 1 2 3 4 5 6 7 8 9	0 1 2 3 4 5 6 7 8 9
Source Port		Destination Port	
Sequence Number			
Acknowledgment Number			
Data Offset	Reserved	URG ACK PSH RST SYN FIN	Window
Checksum			Urgent Pointer
Options			Padding
Data Bytes			

  - source port
    - odesilatel
  - destination port
    - příjemce

TCP Paket

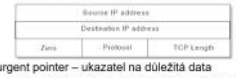
- Hlavička TCP paketu
  - sequence number – pořadové číslo
    - pořadové číslo prvého datového bajtu v paketu
    - pokud je nastaven příznak SYN, SN(n) znamená, že následující první datový bajt bude mít SN = n+1
  - acknowledgement number – číslo potvrzení
    - platné pokud je nastaven ACK příznak
    - obsahuje další očekávané SN, AN(n+1) potvrzuje přijetí až po bajt (n)
  - data offset
    - délka TCP hlavičky v DWORDech (32 bit)
    - ukazuje, kde začíná datové pole paketu
  - reserved
    - 6 nulových bitů
  - URG flag
    - je použito pole urgent pointer – ukazatel na důležitá data

TCP Paket

- Hlavička TCP paketu
  - ACK flag
    - potvrzovací číslo (acknowledgement number) je platné
  - PSH flag
    - push function – vynucené odeslání dat
  - RST flag
    - reset spojení
  - SYN flag
    - synchronizace pořadových čísel při otevírání spojení
  - FIN flag
    - ukončení spojení
  - window
    - platné pouze při nastaveném ACK
    - definuje množství dat, které je příjemce schopen přijmout (počínaje bajtem s potvrzovacím číslem v témž paketu)

TCP Paket

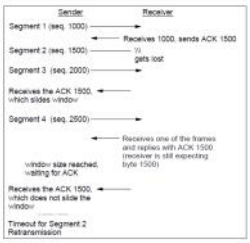
- Hlavička TCP paketu
  - checksum – kontrolní součet
    - včetně pseudo-IP hlavičky, TCP hlavičky a datového pole

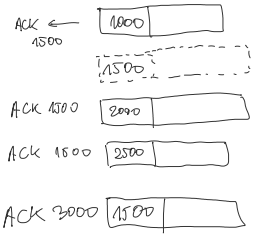


  - urgent pointer – ukazatel na důležitá data
    - definuje oblast důležitých dat (příznak URG musí být nastaven)
  - options
    - volitelné položky hlavičky
    - buď pevná (1 bajt) nebo proměnná délka
    - např. časová značka, max. velikost segmentu, koeficient položky window …
  - padding
    - doplňuje velikost hlavičky na celý DWORD

TCP – Potvrzovací mechanismus

- Sekvenční a potvrzovací číslo
- Velikost segmentu např. 500 bajtů
- Hodnota timeoutu odvozena od RTT (round trip time)





Vytvoření a zrušení TCP spojení

- Vytvoření: tzv. 3-way handshake

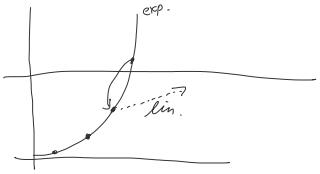
- Zrušení (z pohledu iniciátora zrušení):
  - FIN odeslán
  - ACK přijat zpět, čekání na FIN z druhé strany
  - FIN přijat, ACK odeslán
  - ACK přijat – spojení oboustranně zrušeno

TCP Congestion Control

- Několik současně spolupracujících mechanismů
- Slow start
  - rychlost odesílání na novém spojení je pomalu navyšována s cílem nalézt limit (max. packet rate)
  - velikost vysílacího okna (congestion window size - *cwnd*) začíná na velikosti jednoho segmentu (*segsize*)
    - zvyšuje se po příjmu ACK dokud nedojde ke ztrátám paketů
  - exponenciální růst
    - 1 (1 ACK – zvýšení na 2)
    - 2 (2 ACK – zvýšení na 4)
    - 4 (4 ACK – zvýšení na 8)
    - …

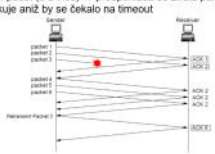
TCP Congestion Control

- Congestion avoidance
  - kombinováno s pomalým startem
    - proměnná *slow start threshold* (*ssthres*), inicializována na 0xffff
  - v případě ztráty dat (indikováno timeoutem nebo duplikovaným ACK)
    - hodnota *ssthres je nastavena na polovinu cwnd*
    - pokud nastal timeout, *cwnd = segsize*
  - pokud *cwnd* < ***ssthres*** (fáze pomalého startu)
    - exponenciální růst *cwnd*
  - jinak fáze předcházení zahlcení
    - *cwnd += segsize*segsize/cwnd*
    - lineární růst



TCP Congestion Control

- Fast retransmit
  - není třeba vyčkávat na timeout, pokud dojde ke ztrátě paketu
  - využití duplikovaných potvrzení (ACK)
    - nízký počet duplikovaných ACK → předpokládá se změna v pořadí paketů, nikoliv ztráta
    - vyšší počet (3 a více) → předpokládá se ztráta paketu a vysílání se opakuje aniž by se čekalo na timeout



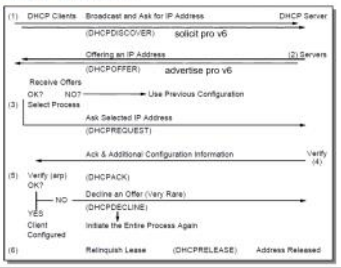
TCP Congestion Control

- Fast retransmit with fast recovery
  - pokud jsou přijaty 3 duplikovaná potvrzení
    - *ssthres = cwnd/2* (ale minimálně 2**segsize*)
    - Ztracený segment je odeslán znovu
    - *cwnd = ssthres + 3*segsize* (3 duplikáty ACK indikují že 3 segmenty po tom ztraceném dorazily OK)
    - pokud je přijat další duplikát ACK, *cwnd += segsize*
    - dovolí-li to hodnota *cwnd*, je vyslán další segment
  - pokud přijde ACK pro novější segment
    - všechny segmenty poslané po tom ztraceném jsou potvrzeny
    - *cwnd = ssthres*
      - předchází zahlcení – *cwnd* je nyní poloviční než když došlo ke ztrátě paketu

DHCP Protocol

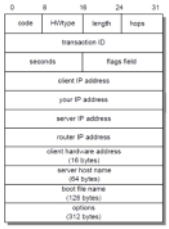
- Dynamic Host Configuration Protocol
  - distribuce konfigurace TCP/IP
  - umožňuje bootování bezdiskových hostitelů
  - vychází ze staršího protokolu BOOTP
    - BOOTP klienti mohou být obslouženi DHCP serverem
  - DHCP zprávy se přenášejí v UDP paketech
    - nezabezpečené
    - možné útoky prostřednictvím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

DHCP Protokol



DHCP Protocol

- DHCP Packet



  - code: 1 – žádost, 2 – odpověď
  - HWtype: 1 – Eth., 6 – IEEE802
  - …
  - length: délka HW adresy
  - hops: klient nastaví na 0, inkrementováno směrovačem při předání – detekce smyček
  - transaction ID – náhodné číslo
  - seconds: čas od počátku procesu bootu
  - flags: MSB pro žádost o zaslání odpovědi broadcastem (když klient ještě nezná svoji adresu)

DHCP Protocol

- DHCP Packet

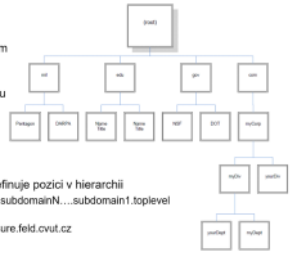
  - client address: IP nebo 0.0.0.0
  - your address: IP přiřazená serverem, pokud je v žádosti 0.0.0.0
  - server address: nastavuje server
  - router address: adresa relay routeru, nikoliv konfigurovaný směrovač
  - client hw address: nastavuje klient
  - server host name: volitelný řetězec zakončený nulou
  - boot file name: volitelné, poskytuje server
  - options: volitelné položky

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

DNS (Domain Name System)

- DNS
  - 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



DNS (Domain Name System)

- Top-level domény
  - generické →
  - států – např. cz, sk …
  - www.icann.org

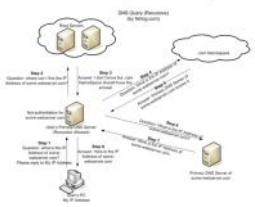
Domain name	Meaning
aero	The air transport industry
biz	Business use
cat	The Catalan culture
com	Commercial organizations
coop	Cooperatives
edu	Educational organizations
gov	U.S. governmental agencies
info	Informational sites
int	International organizations
jobs	Employment-related sites
mil	The U.S. military
mobi	Mobile devices sites
museum	Museums
name	Family and individual sites
net	Network infrastructures
org	Non-commercial organizations
pro	Professional sites
travel	The travel industry

DNS (Domain Name System)

- 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 sharingu"
- 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
  - …

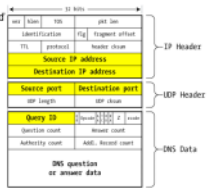
DNS (Domain Name System)

- Zpracování DNS dotazu
  - rekurzivní nebo **iterativní** (většinová varianta)



DNS (Domain Name System)

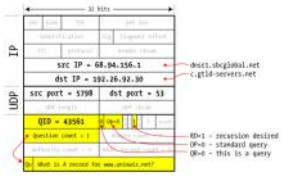
- Formát DNS paketu
  - query ID: náhodné číslo
  - QR: 0 pro dotaz, 1 pro odpověď
  - op.code:
    - 0 – standardní dotaz
    - 1 – inverzní dotaz
    - 2 – dotaz na status serveru
  - AA: autoritativní odpověď
  - TC: zkráceno
    - příliš dlouhá data pro UDP
  - RD: požadavek rekurze
  - RA: potvrzení rekurze
  - Z: vše 0
  - rcode: kód odezvy
  - question, answer authority a additional rec. count
    - počty jednotlivých typů záznamů



DNS packet on the wire

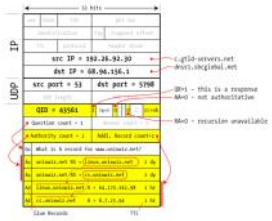
DNS Query / Response Sequence

- Krok 4 (o 2 slajdy výše) – dotaz na server



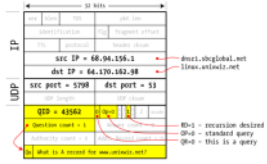
DNS Query / Response Sequence

- Krok 5 – odezva od serveru



DNS Query / Response Sequence

- Krok 6 – dotaz na autoritativní server



DNS Query / Response Sequence

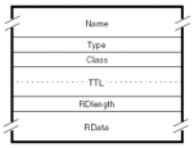
- Krok 7 – odpověď od autoritativního serveru

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

Typy DNS záznamů

- Záznamy (Resource records)
  - obecný formát záznamu



  - name
    - sekvence jmenovek (každá až 63 znaků, 1. musí být písmeno), oddělené znakem tečka)
    - malá a velká písmena se nerozlišují

Typy DNS záznamů

- Resource records
  - type

Type	Value	Meaning	RFC def
A	1	A host address	1035
NS	2	An authoritative name server	1035
CNAME	5	The canonical name for an alias	1035
SOA	6	Marks the start of a zone of authority	1035
MB	7	A mailbox domain name (experimental)	1035
MG	8	A mail group member (experimental)	1035
MR	9	A mail rename domain name (experimental)	1035
NULL	10	A NULL resource record (experimental)	1035
WKS	11	A well known service description	1035
PTR	12	A domain name pointer	1035
HINFO	13	Host information	1035
MINFO	14	Mailbox or mail list information	1035
MX	15	Mail exchange	1035
TXT	16	Text strings	1035
RP	17	Responsible person record	1183
AFSDB	18	Andrew File System database	1183
X25	19	X.25 resource record	1183
ISDN	20	ISDN resource record	1183
RT	21	Route Through resource record	1183
NSAP	22	Network Service Access Protocol record	1348

Typy DNS záznamů

- Resource records
  - type

Type	Value	Meaning	RFC def
NSAP-PTR	23	NSAP Pointer record	1348
KEY	25	The public key associated with a DNS name	2535
AAAA	28	An IPv6 address record	3596
LOC	29	GPS resource record	1876
NXT	30	Defines the services available in a zone	2672
CERT	37	Certificate resource records	4398
A6	38	Forward mapping of an IPv6 address	2874
DNAME	39	Delegation of IPv6 reverse addresses	2672
DS	59	Delegated Signer record (DNS security)	4034
RRSIG	46	Resource record digital signature	4034
NSEC	47	Next Secure record (DNS security)	4034
DNSKEY	48	Public Key record (DNS security	4034

Typy DNS záznamů

- 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)
  - RDlength
    - délka pole RData
  - RData
    - řetězec popisující daný záznam
    - formát závisí na typu (a třídě) záznamu
- Přístup do DNS – program NSLOOKUP
  - zkuste si to ….
- Dynamické DNS záznamy
  - spolupráce DHCP ↔ DNS

Přednáška 6

čtvrtek 4. května 2023 9:18

6_Zdroje informace...

Počkejte prosím, než OneNote načte tento výtisk...

Základní pojmy

- **Zpráva** - jakákoliv posloupnost rozlišitelných znaků
- **Symboly** - rozlišitelné prvky ve zprávě (grafické znázornění … 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

Teorie informace

- Vychází z teorie pravděpodobnosti a matematické statistiky

- Přenosová cesta: prostředí, kterým se šíří signál
- Přenosový kanál: souhrn technických prostředků nutných pro nezávislý přenos signálu
- Základní otázky přenosu informace:
  - míra využití kapacity přenosového kanálu
  - bezporuchový přenos

Informační entropie

- Míra neurčitosti jevu – **informační entropie *H***

Neurčitost jistého jevu (P=1) je 0, neurčitost prázdného jevu (P=0) je ∞

$$H = f\left(\frac{1}{P}\right)$$

- **Množství informace *I(X)*** ve zprávě je rovno entropii, která se jejím přijetím odstraní:

$$I(X) = H(X) = f\left[\frac{1}{P(X)}\right]$$

- Claude Elwood Shannon (abs. MIT, 1916-2001)
  - jednotka: bit [b] nebo shannon [Sh]

$$I(X) = H(X) = \log_2\left[\frac{1}{P(X)}\right] = -\log_2 P(X)$$

Kapacita přenosového kanálu C

Uvažujeme signál s nejvyšší užitečnou složkou f_{max}
Takový signál může být plně zrekonstruován ze vzorků, snímaných s frekvencí $f > 2f_{max}$

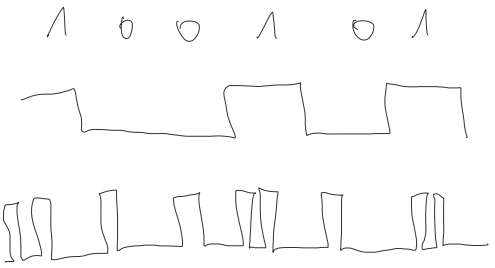
Kvantujeme-li signál na 2^n diskrétních úrovní, potom $C_{max} = 2f_{max}\, n$ [bit/s]

Tato kapacita je zároveň maximem dosažitelným na přenosovém kanále o šířce $f_{max.}$

V případě zašuměného kanálu (bílý šum s normálním rozložením pravděpodobnosti)

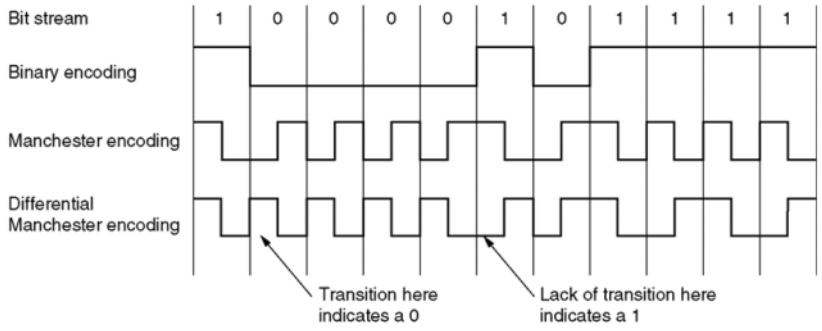
$$C_{max} = f_{max}\, log_2\left(1 + \frac{P_S}{P_N}\right) = f_{max}\, log_2\left(1 + e^{\frac{SNR}{10}}\right)$$

Počkejte prosím, než OneNote načte tento výtisk…



Počkejte prosím, než OneNote načte tento výtisk...

Nejčastěji používaná kódování signálu



Základní typy chybových modelů pro reálné číslicové přenosové kanály

„Bez paměti“:

- AWGN kanál
- BSC kanál
- BEC, BAC, …

„S pamětí“:

- Gilbert-Elliott 1960

Počkejte prosím, než OneNote načte tento výtisk…

Počkejte prosím, než OneNote načte tento výtisk...

Počkejte prosím, než OneNote načte tento výtisk...

Přednáška 7

čtvrtek 4. května 2023 9:46

7_Analogov
Ã© a ÃÃ-...

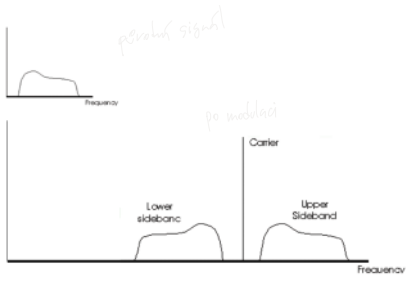
Počkejte prosím, než OneNote načte tento výtisk...

Počkejte prosím, než OneNote načte tento výtisk...

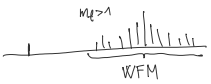
Počkejte prosím, než OneNote načte tento výtisk...

Počkejte prosím, než OneNote načte tento výtisk...

Spektrum AM signálu pro obecný modulační signál

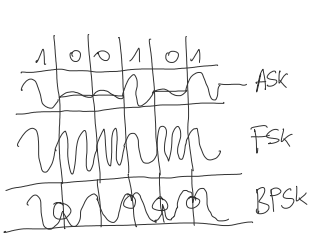


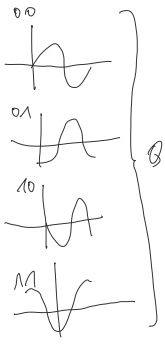
Počkejte prosím, než OneNote načte tento výtisk...

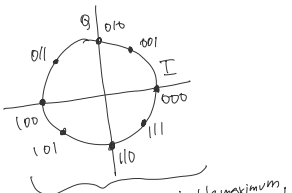


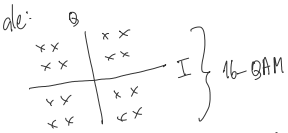
Počkejte prosím, než OneNote načte tento výtisk...

Počkejte prosím, než OneNote načte tento výtisk...









256-QAM – nejčastější modulace pro optické přístroje

ASK

$$a(t) = A\cos(\omega t + \varphi)$$

$$a_{ASK}(t) = d(t).A\cos(\omega t + \varphi)$$

- $d(t)$ nabývá např. hodnot "0" ; "1"

FSK

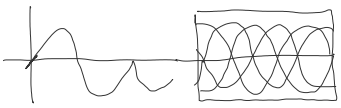
$$a_{FSK}(t) = A\cos\left[2\pi\left(f_S \pm \Delta f\right)t\right]$$

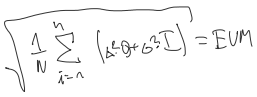
PSK (M-stavová)

$$a_{PSK} = a.\sin\left[\omega t + \frac{2\pi(i-1)}{M}\right]$$

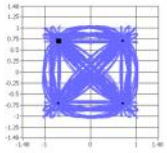
$M = 2$: *BPSK - binární PSK*
$M = 4$: *QPSK - kvadraturní PSK*
$M = 8$: 8ϕ-PSK

Počkejte prosím, než OneNote načte tento výtisk...



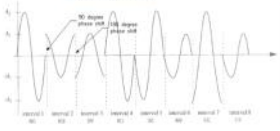


Př.: reálná PSK



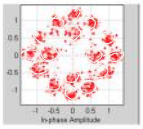
Př.: reálná 8-QAM

(časová rovina)



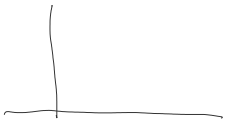
reálná 16-QAM

(IQ rovina)



Počkejte prosím, než OneNote načte tento výtisk...

Počkejte prosím, než OneNote načte tento výtisk...



Počkejte prosím, než OneNote načte tento výtisk...

Přednáška 8

úterý 9. května 2023 9:17

8_ZÃ¡kladn
´- principy...

Počkejte prosím, než OneNote načte tento výtisk...

Počkejte prosím, než OneNote načte tento výtisk...

Počkejte prosím, než OneNote načte tento výtisk...

pci express – sério paralelní

Počkejte prosím, než OneNote načte tento výtisk...

Počkejte prosím, než OneNote načte tento výtisk...

Počkejte prosím, než OneNote načte tento výtisk...

Počkejte prosím, než OneNote načte tento výtisk...

sériová synchronní komunikace

SPI, I²C

– mezi čipy

UART – Universal Asynchronous Receiver Transmitter

8N2

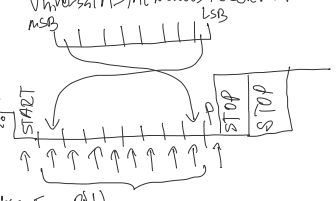
E

O

počet stop bitů

počet bitů

parita (None, Even, Odd)



maximální rozdíl časů mezi sender/receiver

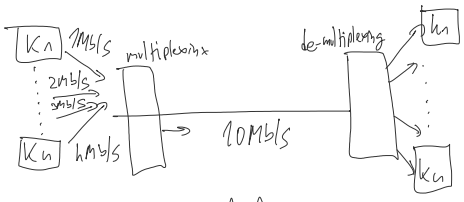
$$\frac{0{,}5T_b \text{ (1/2 délky bitu)}}{12T_b} \doteq 0{,}04 \rightarrow \text{rozdíl frekvencí oscilátorů}$$

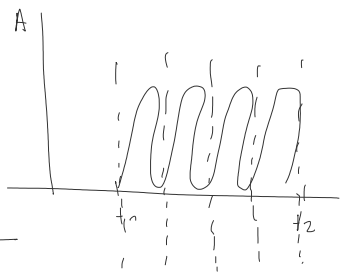
4%

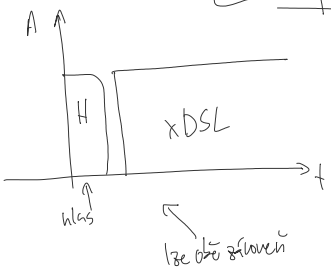
T_b^N → nominální hodnota

→ potom max 2% odchylka

frekvenční multiplexing

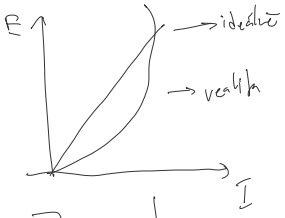


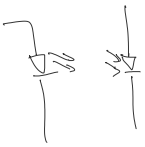




Počkejte prosím, než OneNote načte tento výtisk...

Wavelength Division Multiplexing





proto se elektrická multiplexace nedělá

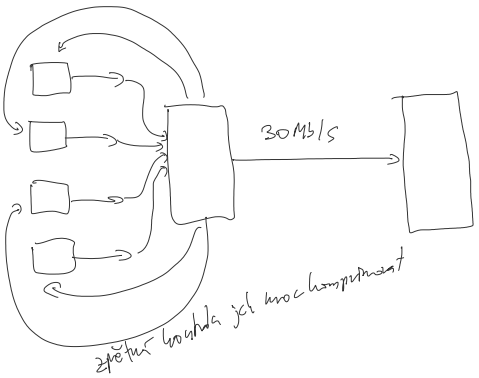
dělá se pouze opticky

Počkejte prosím, než OneNote načte tento výtisk...

data se buffrovují, potom se vyšlou dostupnou rychlostí

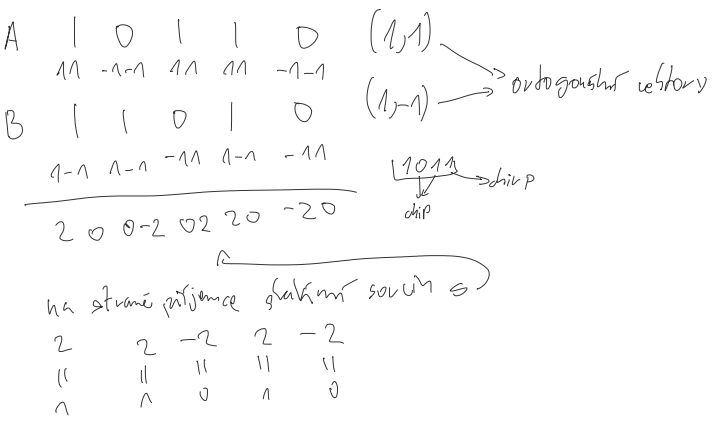
problém s přenosem variabilních datových toků (video streaming)

Počkejte prosím, než OneNote načte tento výtisk...



Počkejte prosím, než OneNote načte tento výtisk...

Počkejte prosím, než OneNote načte tento výtisk...

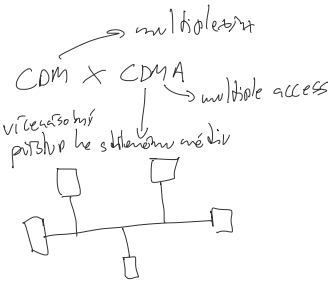


Počkejte prosím, než OneNote načte tento výtisk...

Počkejte prosím, než OneNote načte tento výtisk...

Počkejte prosím, než OneNote načte tento výtisk...

Počkejte prosím, než OneNote načte tento výtisk...



TDM x TDMA

Počkejte prosím, než OneNote načte tento výtisk...

sloty:

Počkejte prosím, než OneNote načte tento výtisk...

Počkejte prosím, než OneNote načte tento výtisk...

Počkejte prosím, než OneNote načte tento výtisk...

Počkejte prosím, než OneNote načte tento výtisk...

Počkejte prosím, než OneNote načte tento výtisk...

Počkejte prosím, než OneNote načte tento výtisk...

Počkejte prosím, než OneNote načte tento výtisk...

Počkejte prosím, než OneNote načte tento výtisk...

Počkejte prosím, než OneNote načte tento výtisk...

Počkejte prosím, než OneNote načte tento výtisk...

Počkejte prosím, než OneNote načte tento výtisk...

Počkejte prosím, než OneNote načte tento výtisk...

Přednáška 9

pondělí 22. května 2023 9:19

9_Internet working

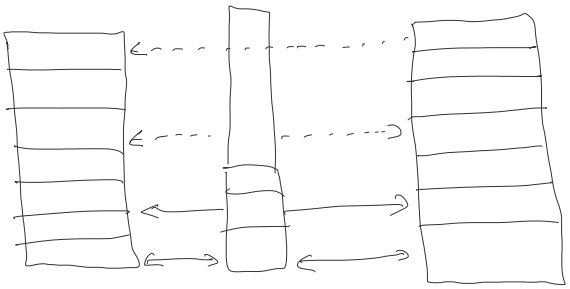
Počkejte prosím, než OneNote načte tento výtisk...

Počkejte prosím, než OneNote načte tento výtisk...

Počkejte prosím, než OneNote načte tento výtisk...

Počkejte prosím, než OneNote načte tento výtisk...

Počkejte prosím, než OneNote načte tento výtisk...



Počkejte prosím, než OneNote načte tento výtisk...

Počkejte prosím, než OneNote načte tento výtisk...

Počkejte prosím, než OneNote načte tento výtisk...

Počkejte prosím, než OneNote načte tento výtisk...

Počkejte prosím, než OneNote načte tento výtisk...

Počkejte prosím, než OneNote načte tento výtisk...

Počkejte prosím, než OneNote načte tento výtisk...

Počkejte prosím, než OneNote načte tento výtisk...

Počkejte prosím, než OneNote načte tento výtisk...

Počkejte prosím, než OneNote načte tento výtisk...

Počkejte prosím, než OneNote načte tento výtisk...

Přednáška 10

pondělí 22. května 2023 9:46

10_Ethernet

Počkejte prosím, než OneNote načte tento výtisk...

Počkejte prosím, než OneNote načte tento výtisk...

Počkejte prosím, než OneNote načte tento výtisk...

Počkejte prosím, než OneNote načte tento výtisk...

Počkejte prosím, než OneNote načte tento výtisk...

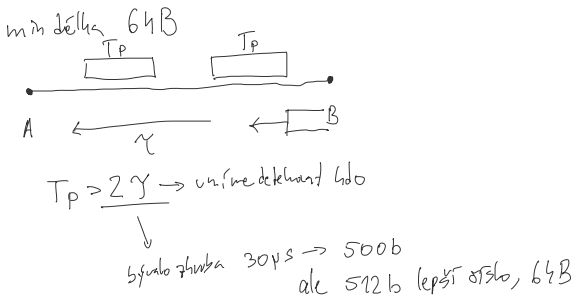
Počkejte prosím, než OneNote načte tento výtisk...

Počkejte prosím, než OneNote načte tento výtisk...

Počkejte prosím, než OneNote načte tento výtisk...

Počkejte prosím, než OneNote načte tento výtisk...

Počkejte prosím, než OneNote načte tento výtisk...



Počkejte prosím, než OneNote načte tento výtisk...

Počkejte prosím, než OneNote načte tento výtisk...

Počkejte prosím, než OneNote načte tento výtisk...

Počkejte prosím, než OneNote načte tento výtisk...

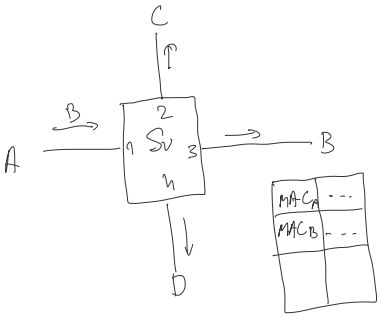
Počkejte prosím, než OneNote načte tento výtisk...

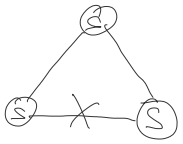
Počkejte prosím, než OneNote načte tento výtisk...

Počkejte prosím, než OneNote načte tento výtisk...

Počkejte prosím, než OneNote načte tento výtisk...

Počkejte prosím, než OneNote načte tento výtisk...





spanning tree zjistí zda smyčky, pokud ano, logicky je rozpojí

dnes plný duplex – můžeme vysílat i přijímat

Počkejte prosím, než OneNote načte tento výtisk...

Počkejte prosím, než OneNote načte tento výtisk...

Počkejte prosím, než OneNote načte tento výtisk...

Počkejte prosím, než OneNote načte tento výtisk...

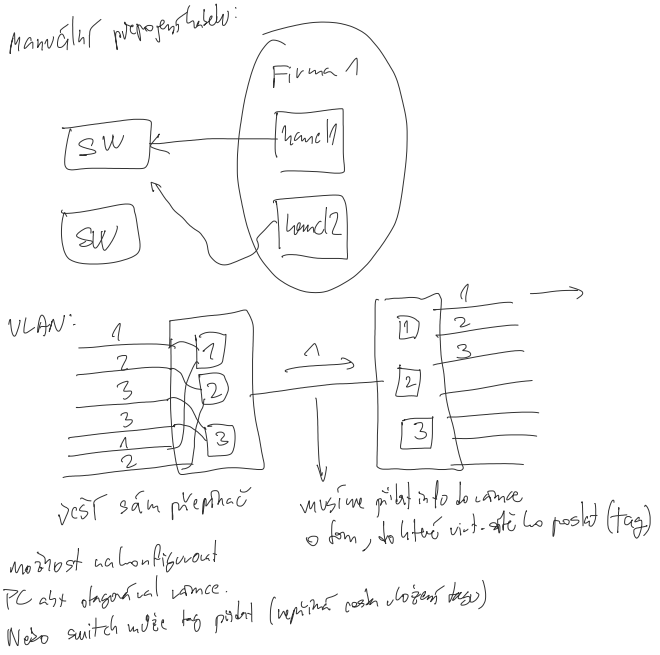
Počkejte prosím, než OneNote načte tento výtisk...

Počkejte prosím, než OneNote načte tento výtisk...

Počkejte prosím, než OneNote načte tento výtisk...

Počkejte prosím, než OneNote načte tento výtisk...

Počkejte prosím, než OneNote načte tento výtisk...



Přednáška 11

pondělí 22. května 2023 10:36

11_Wireless

Počkejte prosím, než OneNote načte tento výtisk...

Počkejte prosím, než OneNote načte tento výtisk...

Počkejte prosím, než OneNote načte tento výtisk...

Počkejte prosím, než OneNote načte tento výtisk...

Počkejte prosím, než OneNote načte tento výtisk...

Počkejte prosím, než OneNote načte tento výtisk...

Počkejte prosím, než OneNote načte tento výtisk...

Počkejte prosím, než OneNote načte tento výtisk...

Počkejte prosím, než OneNote načte tento výtisk...

Počkejte prosím, než OneNote načte tento výtisk...

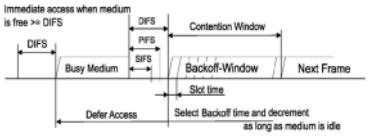
Počkejte prosím, než OneNote načte tento výtisk...

Počkejte prosím, než OneNote načte tento výtisk...

master - slave

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

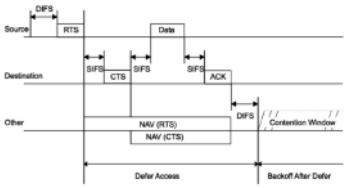


Počkejte prosím, než OneNote načte tento výtisk...

Počkejte prosím, než OneNote načte tento výtisk...

Virtuální odposlech kanálu (CS)

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



Počkejte prosím, než OneNote načte tento výtisk...

Počkejte prosím, než OneNote načte tento výtisk...

Počkejte prosím, než OneNote načte tento výtisk...

Počkejte prosím, než OneNote načte tento výtisk...

Počkejte prosím, než OneNote načte tento výtisk...

Počkejte prosím, než OneNote načte tento výtisk...

Počkejte prosím, než OneNote načte tento výtisk...

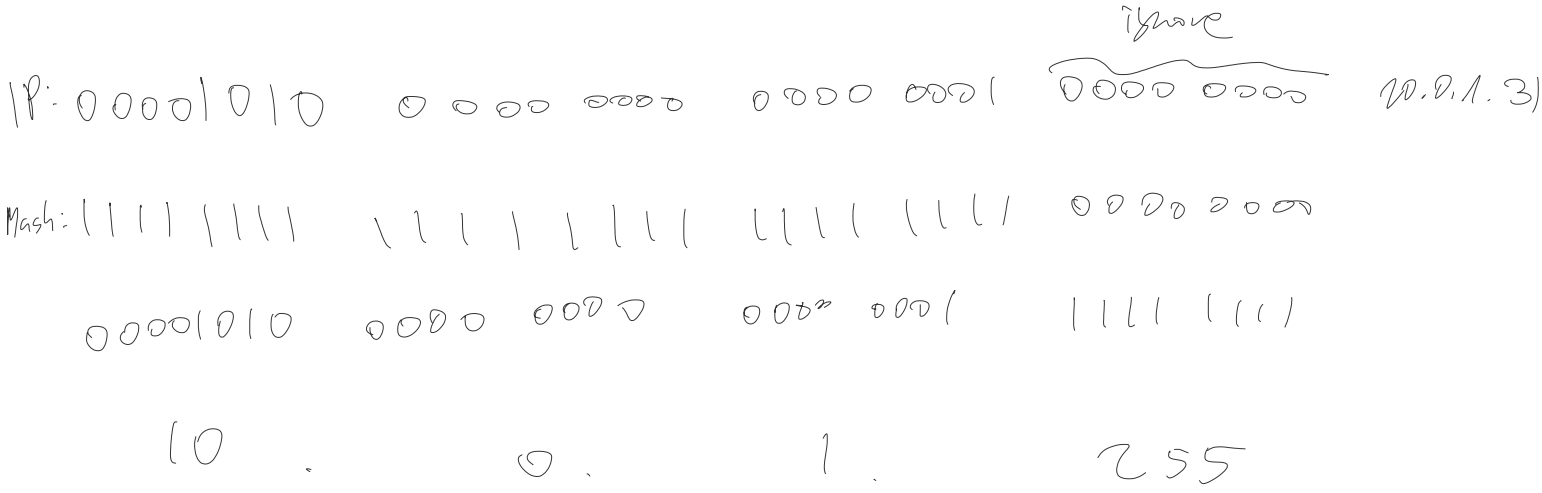
Počkejte prosím, než OneNote načte tento výtisk...

Počkejte prosím, než OneNote načte tento výtisk...

Počkejte prosím, než OneNote načte tento výtisk...

Počkejte prosím, než OneNote načte tento výtisk...

Zabezpečení

- WEP (Wired Equivalent Privacy)
  - součást původního standardu 802.11
  - proudová šifra RC4 se 40 bitovým klíčem
    - spolu s 24 bitovým inicializačním vektorem 64 bitů
      - inicializační vektor se mění pro každý rámec
    - po odstranění vládních (USA) restrikcí 104 bitů (celkem 128)
  - cílem bylo zajistit stejnou úroveň bezpečnosti jako po metalickém vedení
    - lze prolomit v řádu minut (i delší klíče)
- WPA (WiFi Protected Access)
  - podle pracovní verze (draft 3) IEEE802.11i
  - stejná šifra (RC4), ale delší inicializační vektor (48 b) a klíč (128 b)
  - dynamická změna klíče
  - autentikace rámců
    - detekce podvržených rámců

Počkejte prosím, než OneNote načte tento výtisk...