1. **Uveďte základní typy počítačových sítí (WAN, MAN, ...) a jejich vlastnosti (použití, topologie, rozlehlost, přenosová rychlost, příklady).**

LAN - lokální sítě. Spojují uzly v rámci jedné budovy nebo několika blízkých budov, vzdálenosti stovky metrů až km (při použití optiky).

- Ethernet(10Mb/s), Fast Ethernet(100Mb/s), Gigabit Ethernet 1Gb/s (IEEE 802.3), Desetigigabitový Ethernet 10Gb/s
- Token Bus (IEEE 802.4) – sběrnicová s předáváním pověření
- Token ring (IEEE 802.5) – kruhová síť
- Bezdrátové sítě (Wi-Fi, IEEE 802.11)

MAN - Metropolitní sítě. Propojují lokální sítě v městské zástavbě, slouží pro přenos dat, hlasu a obrazu. Spojuje vzdálenosti řádově jednotek až desítek km. Rychlost MAN sítí bývá vysoká a svým charakterem se řadí k sítím LAN.

- protokol Distributed Queue Dual Bus (DQDB) (IEEE 802.6) – na koncepci ATM

WAN - rozsáhlé sítě. Spojují LAN a MAN sítě s působností po celé zemi nebo kontinentu, na libovolné vzdálenosti. Přenosové rychlosti se velmi liší podle typu sítě. Začínají na desítkách kbit/s, ale dosahují i rychlostí řádu Gbit/s. Příkladem takové sítě může být Internet.

- ISDN, ATM

PAN - osobní síť. Jedná se o velice malou počítačovou síť (například Bluetooth, IrDA nebo ZigBee), kterou člověk používá pro propojení jeho osobních elektronických zařízení, jakými jsou např. mobilní telefon, PDA, notebook apod.

BAN – sensory na těle propojeny s PC a posílají info (např. o stavu srdce, ujité vzdálenosti...)

2. **Uveďte rozdíl mezi sítěmi s přepínáním paketů, přepínáním zpráv a přepínáním kanálů. Jaké jsou jejich výhody a nevýhody?**

přepínání paketů – neexistuje pevný kanál; o cestě každého paketu se rozhoduje zvlášť na přepínačích (linková vrstva – přepínání rámců, síťová – přepínání paketů)

+ urychlení přenosu,
- možná ztráta, duplicita

přepínání zpráv – speciální případ přepínání paketů (je to jeho předchůdce), přepínání mezi 2 body

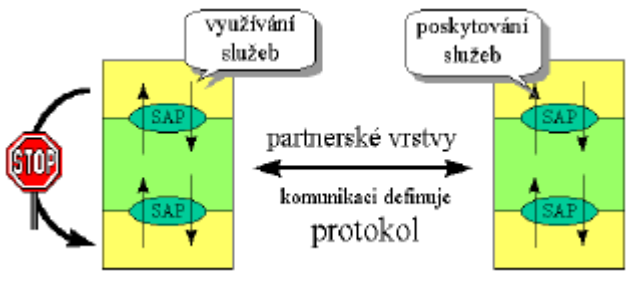
+ lze použít jeden kanál vícekrát
- delší doba čekání při vícenásobném přenosu

přepínání kanálů – existuje kanál mezi 2 body → data jdou tímto kanálem; kanál je virtuální; kanál se vytvoří před navázáním spojení nastavením přepínačů v bodech sítě → kanál se dále chová jako přímý spoj

+ spolehlivost
- zabere kanál, čas

3. **Zakreslete příklad hierarchického modelu komunikačních protokolů a znázorněte úrovně, rozhraní, protokoly, body přístupu protokolové datové jednotky a služby. Jaký je rozdíl mezi protokolem a službou.**

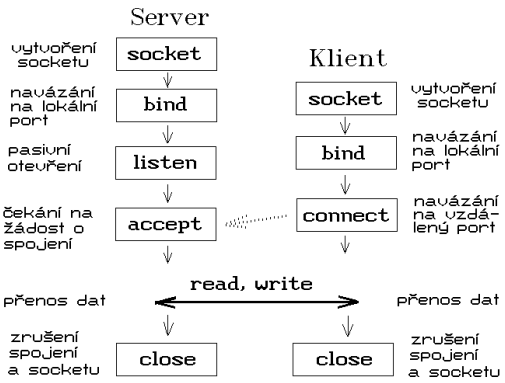
Komunikace povolena pouze mezi sousedními vrstvami. V terminologii ISO/OSI jsou přístupové body mezi vrstvami označeny jako SAP (Service Access Point) → přes ně si předávají info v podobě spec. balíčků



Služby se týkají se vertikální komunikace mezi vrstvami a jsou

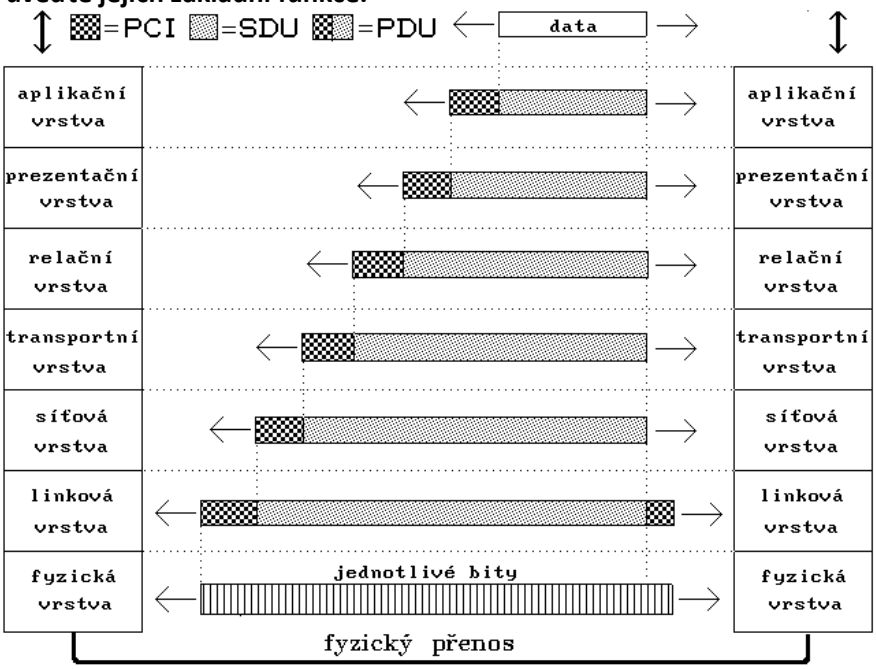
skrze rozhraní. Nejsou vidět zvenčí (krom identifikace přechodových bodů). Rozhraní nemusí být standardizováno, stejně tak ani služby.
Protokoly se týkají horizontální komunikace mezi stejnými vrstvami, jsou vidět zvenčí a musí být standardizováný

4. Vyjmenujte a popište základní služby pro navázání spojení, přenos dat a ukončení spojení u spojově orientovaného protokolu (např. BSD sockety).
Naváže se spojení a po něm jdou pak data; velká režie, spolehlivé; např. TCP/IP
Server:
Vytvoření socketu – systémové volání *socket* – v parametrech druh spojení, konkrétní protokol
Navázání na lokální port – vazba mezi portem a sonetem nevzniká automaticky při vzniku socketu, je třeba ji vytvořit následně – příkaz *bind*
Otevření portu – *listen* – socket pasivně čeká na příchozí žádosti o navázání spojení, jako parametr délka fronty; když přijde žádost → OS žádost přijme a vytvoří nový socket, který naváže na port volajícího → navázání spojení mezi klientem a serverem, přes tento socket bude probíhat další komunikace, na původním socketu čekání na další požadavky na navázání spojení



Klient:
Vytvoření socket, navázání na lokální port – obdobně jako u serveru
Navázání na vzdálený port – systémové volání *connect* – jako parameter adresa vzdáleného počítače a port na tomto počítači → navázání spojení

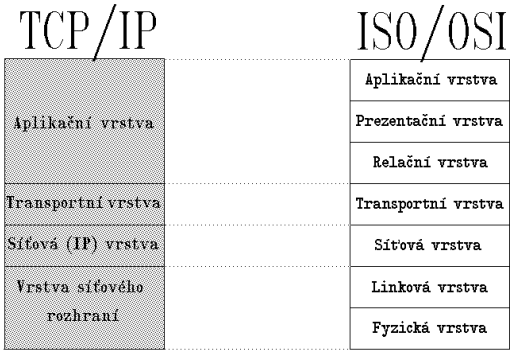
5. Nakreslete protokolový zásobník, vyjmenujte sedm základních úrovní referenčního modelu ISO/OSI a uveďte jejich základní funkce.



Fyziská vrstva - úkolem zajistit přenos jednotlivých bitů mezi příjemcem a odesilatelem prostřednictvím fyzické přenosové cesty. Musí se řešit např. jakou úrovní napětí bude

reprezentována logická jednička a jakou logická nula, jak dlouho "trvá" jeden bit, kolik kontaktů a jaký tvar mají mít konektory kabelů, jaké signály jsou těmito kabely přenášeny, jaký je jejich význam, časový průběh apod.
Linková vrstva - má za úkol zajisti bezchybný přenos bloků dat (rámců), musí správně rozpoznat začátek a konec rámce, jeho jednotlivé části, kontrolovat bezchybný přenos rámců, případně opakování chybně přenesených.
Síťová vrstva - zajišťuje potřebné směrování přenášených rámců – paketů – volbu cesty a předávání paketů po této trase.
Transportní vrstva - zabývá se komunikací mezi odesílatelem a příjemcem, zajišťuje přenos dat mezi koncovými uzly, při odesílání dat zajišťuje sestavování paketů, do kterých rozděluje data, a při příjmu je skládá do původního tvaru.
Relační vrstva - navazování, udržování a rušení relací (sessions) mezi koncovými účastníky, pokud je třeba komunikaci nějak řídit (např. určovat, kdo má kdy vysílat, nemohou-li to dělat oba účastníci současně), zajišťuje to tato vrstva, která má také na starosti vše, co je potřeba k ukončení relace a zrušení existujícího spojení.
Prezentační vrstva - konverze, koprese, šifrování přenášených dat
Aplikační vrstva - poskytuje aplikacím přístup ke komunikačnímu systému a umožnit tak jejich spolupráci. (FTP, http, telnet...)

6. **Zakreslete protokolový zásobník TCP/IP, uveďte základní protokoly a uveďte jejich funkce a význam.**



Vrstva síťového rozhraní má na starosti vše, co je spojeno s ovládáním konkrétní přenosové cesty resp. sítě, a s přímým vysíláním a příjmem datových paketů. Je závislá na použité přenosové technologii.
Vzhledem k velmi častému připojování jednotlivých uzlů na lokální sítě typu Ethernet je vrstva síťového rozhraní v rámci TCP/IP často označována také jako Ethernetová vrstva (Ethernet Layer).

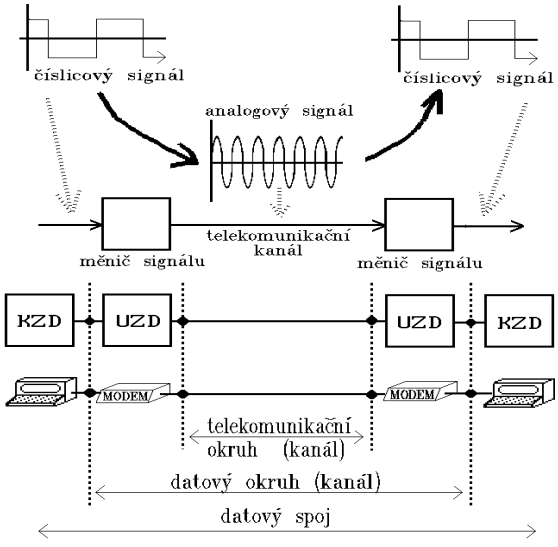
Vrstva síťová, v terminologii TCP/IP označovaná jako Internet, IP vrstva. Úkol této vrstvy je v prvním přiblížení stejný, jako úkol síťové vrstvy v referenčním modelu ISO/OSI - stará se o to, aby se jednotlivé pakety dostaly od odesilatele až ke svému skutečnému příjemci, přes případné směrovače resp. brány. Vzhledem k nespojovanému charakteru přenosů v TCP/IP je na úrovni této vrstvy zajišťována jednoduchá (tj. nespolehlivá) datagramová služba.
IP, ARP, ICMP

Transportní vrstva, nebo též jako TCP vrstva, neboť je nejčastěji realizována právě protokolem TCP. Hlavním úkolem této vrstvy je zajistit přenos mezi dvěma koncovými účastníky, kterými jsou v případě TCP/IP přímo aplikační programy (jako entity bezprostředně vyšší vrstvy). Podle jejich nároků a požadavků může transportní vrstva regulovat tok dat oběma směry, zajišťovat spolehlivost přenosu, a také měnit nespojovaný charakter přenosu (v síťové vrstvě) na spojovaný.Dalším používaným protokolem na úrovni transportní vrstvy je například protokol UDP, který na rozdíl od TCP nezajišťuje mj. spolehlivost přenosu.

Vrstva aplikační - jejími entitami jsou jednotlivé aplikační programy, které na rozdíl od referenčního modelu ISO/OSI komunikují přímo s transportní vrstvou.
HTTP, DNS, SSH

7. **Uveďte čím je limitována frekvence změn číslicového signálu a čím je limitován počet úrovní tohoto signálu při přenosu komunikačním kanálem.**

Spojová organizace (správa spojů) uživateli poskytuje telekomunikační kanál či okruh s určitými technickými parametry, které definují, jaké signály je schopen přenášet. Uživatel ovšem může mít jiné požadavky na přenosové schopnosti okruhu, po kterém potřebuje přenášet signály jiných parametrů. Proto se na oba konce okruhu připojuje zařízení, které potřebné úpravy signálu zajišťuje (viz obr. 8.1.). Toto zařízení, fungující jako měnič signálu, se v odborné terminologii nazývá ukončujícím zařízením datového okruhu (UZD) - data circuit terminating equipment (DCE).



Obr. 8.1.: Datový spoj a okruh

Uvažujme následující typický příklad: přenosový okruh nechť je běžným komutovaným telefonním okruhem, tedy okruhem analogovým, schopným přenášet analogové signály v rozmezí 300 až 3400 Hz. My ho ovšem potřebujeme využívat pro přenos číslicových dat, tedy jako okruh číslicový. Již dříve jsme si ukázali, že takovýto postup je možný - pomocí modulace. Místo diskrétního číslicového signálu tedy budeme přenášet vhodný analogový signál, který je telefonní okruh schopen přenést, a který budeme modulovat (tj. měnit jeho průběh) podle toho, jaká data (resp. číslicový signál, který je vyjadřuje) chceme přenést. Potřebujeme k tomu ale takové zařízení, které je schopno zajistit jednak potřebnou modulaci analogového signálu, jednak i opačný proces, tzv. demodulaci, tedy zpětné získání číslicového signálu ze signálu analogového. Toto zařízení se nazývá modem, což je zkratka od MOdulátor/DEModulátor.

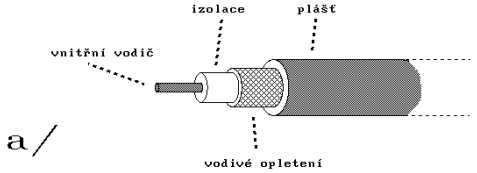
(nevim http://www.earchiv.cz/a91/a146c110.php3)

8. **Uveďte základní typy komunikačních médií, jejich vlastnosti, zjednodušený náčrtek a kde se používají.**

Koaxiální kabel (a) - Tvoří jej vnitřní vodič, kolem kterého je nanesena izolující vrstva dielektrika. Koaxiální kabely se používají např. v lokálních sítích Ethernet.

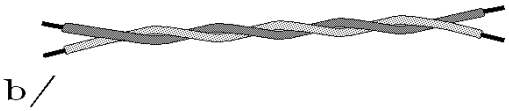
tlustý – tloušťka kabelu je 0,5 palců, díky tloušťce přenáší signál až do vzdál 500 m

tenký - tloušťka kabelu je 0,25 palců, přenáší signál do vzdál necelých 200m

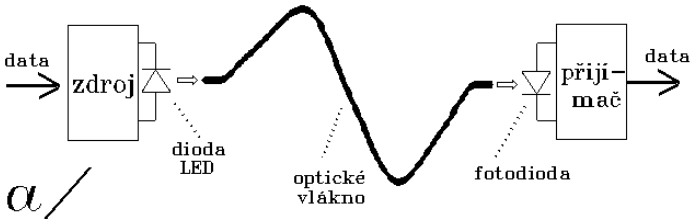


Kroucená dvojlinka (b) – zkroucení párů vodičů – zlepšuje to el. vlastnosti kabelu, *nestíněná* – tenčí, pro běžné použití, *stíněná* – větší odolnost proti rušení

Použití např. v telefonní technice



Optické kabely – přenos číslicových dat pomocí světelných impulsů, optické, s tenkým jádrem obaleným vhodným pláštěm

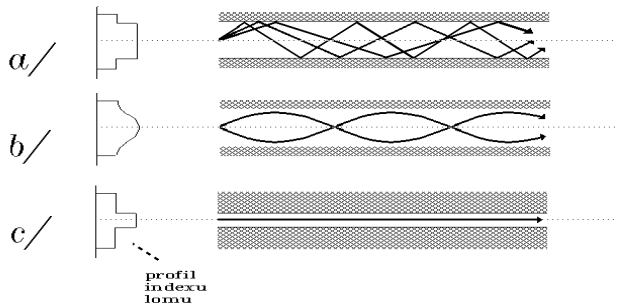


9. Jaké druhy optických vláken znáte? Čím se od sebe liší?

s konstantním indexem lomu – nepoužívají se, 10Mb/s na vzdálenost 1km, pokud paprsek šikmo=>odráží se=>nižší rychlost

s proměnným indexem lomu - průběh indexu v ideálním případě parabola - 1Gb/s na 3-5km, výhodou relativně nízká cena, snažší spojování, velká numerická apertura a možnost buzení luminiscenční diodou

Jednovidové (single mode) - průměr 2-5 mikrometrů, už nemůžu vysílat šikmo=> nedochází k odrazům - 1-10Gb/s na až 100km, nejvyšší přenosové rychlosti. Schopnosti vést jediný vid bez odrazů i ohybů se dosahuje buďto velmi malým průměrem jádra (řádově jednotky mikrometrů), nebo velmi malým poměrným rozdílem indexů lomu jádra a jeho pláště.



10. Co je to přenos dat v základním pásmu a v přeneseném pásmu

Pokud je použita nějaká forma modulace a podle přenášených dat se mění některá z jeho charakteristik, například fáze, amplituda či frekvence, pak jde o přenos v tzv. přeloženém pásmu.

Naproti tomu přenos v tzv. základním pásmu je takový, při kterém se fakticky přenášený analogový signál sám od sebe nemění, ale mění se až v závislosti na datech, která má přenášet.

Principiální rozdíl mezi přenosem v základním a přeloženém pásmu je tedy v tom, že frekvence změn skutečně přenášeného signálu je v prvním případě rovna frekvenci změn přenášených dat, zatímco ve druhém případě (v případě přenosu v přeloženém pásmu) je frekvence změn přenášeného signálu (jeho kmitočet) výrazně vyšší.

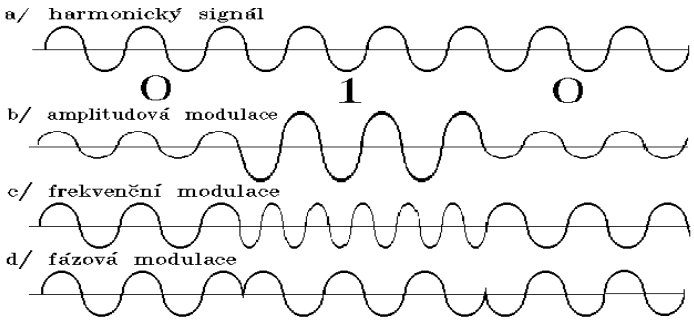
Zajímavým důsledkem rozdílů mezi přenosem v základním a přeloženém pásmu je i jejich typický dosah - u přenosů v základním pásmu bývá menší, a u přenosů v přeloženém pásmu naopak větší, často i dosti výrazně. Důvodem je fakt, že v tomto druhém případě je skrz příslušnou přenosovou cestu fakticky přenášen takový analogový signál, který tato přenosová cesta přenáší nejlépe, s nejmenšími ztrátami, nejmenším útlumem a zkreslením.

11. Základní typy modulací, jejich vlastnosti a použití.

Amplitudová – při které jsou jednotlivé logické hodnoty vyjádřeny různými hodnotami amplitudy (rozkmitu) harmonického signálu (AM), využívá rozhlas

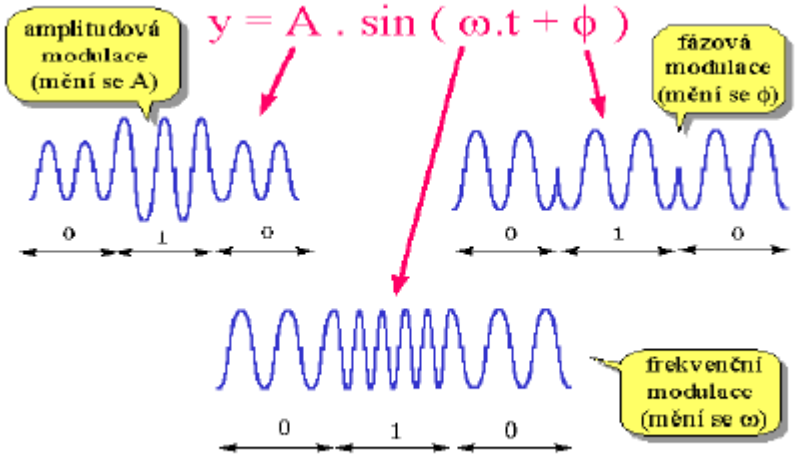
Frekvenční – při které jsou jednotlivé logické hodnoty vyjádřeny různými frekvencemi (kmitočty) harmonického signálu (FM), analogové televizní soustavy

Fázová – při které jsou jednotlivé logické hodnoty vyjádřeny různou fází (posunutím) harmonického signálu (PM), využití: rozhlas na středních a krátkých vlnách

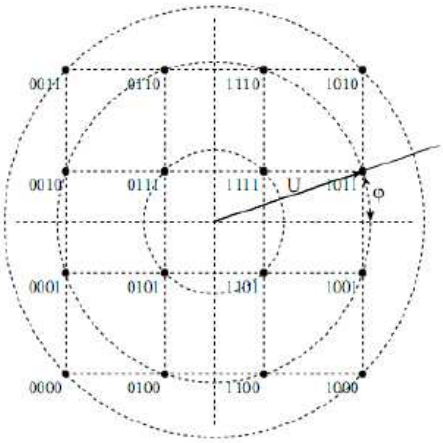


Obr. 4.2.: Modulace při přenosu v přeloženém pásmu

12. **Je dán binární signál, který je modulován tak, že během jedné změny amplitudy nosné se přenáší dva bity. Zakreslete, jak bude vypadat výstupní signál amplitudové modulace, bude-li se přenášet binární kombinace (10100111)2.**
13. **Je dán binární signál, který je modulován tak, že během jedné změny nosné se přenáší dva bity. Zakreslete, jak bude vypadat výstupní signál frekvenční modulace, bude-li se přenášet binární kombinace (10100111)2.**
14. **Je dán binární signál, který je modulován tak, že během jedné změny nosné se přenáší dva bity. Zakreslete, jak bude vypadat výstupní signál diferenciální fázové modulace, bude-li se přenášet binární kombinace (10100111)2.**

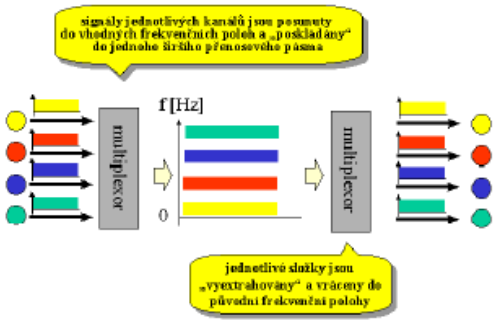


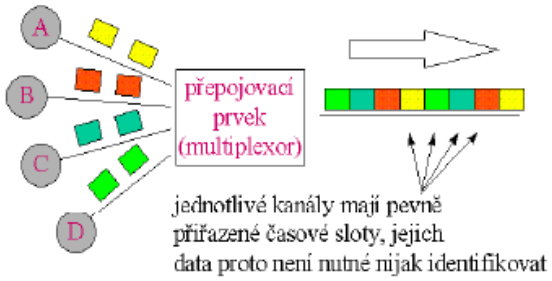
15. **Do fázové roviny zakreslete příklad amplitudo-fázové modulace pro kódování 4 bitů.**



16. **Jaký je rozdíl mezi frekvenčním a časovým multiplexem. Zakreslete jednoduchý obrázek.**
<u>frekvenční multiplex (analog)</u> – každý signál má svojí frekvenci a na té je vysílán → všechny signály smíchány do jednoho s větší šířkou pásma → přenos → rozložení zpět na jednotlivé frekvence
Víceméně pohled – rozdělit datovou cestu na jednotlivé kanály a ty se svým způsobem chovají nezávisle – každý set jiná část přenosové kapacity

<u>časový multiplex (digital)</u> – přenosová cesta je pravidelně (např. cyklicky) přidělována jednotlivým kanálům. Způsob přidělování je předem znám => data jedou a podle způsobu přidělování se ví, která jedou





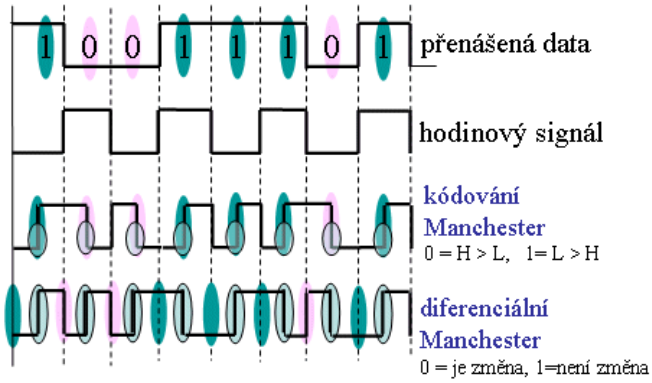
17. **Přenosový systém T1 používá rámec, který vznikne jako časový multiplex jednoho řídicího bitu a 24 kanálů po 8 bitech (8 datových a jeden pro signalizaci). T1 rámec je vysílán 8000 krát za sekundu. Naznačte jak byste umístili jednotlivé kanály do rámce.**

18. **Jak se liší modulace od kódování signálu? Co to znamená, že signál je kódován „bez návratu k nule".**
<u>Modulace</u> – přenášen signál, který se šíří médiem nejlépe → často sinusové signály → informace se přenáší prostřednictvím změn → měníme charakter nosného signálu modulačním (např. sin)
<u>Kódování signálu</u> – zabezpečení signálu např. proti chybám
<u>Bez návratu k nule – NRZ</u> – je implementačně náročnější, zůstává v hladině, ve které byl, dokud nepřijde signál, který mění jeho hodnotu, pouze hodnoty 1, 0, neexistuje žádná třetí neutrální hodnota, hrozí nebezpečí ztráty synchronizace u příjemce

19. **Jaký je rozdíl mezi diferenciálním kódováním a kódováním které není diferenciální?**
Diferenciální a nediferenciální variantu má např. kódování Manchester.
U kódování Manchester jsou oba signály sloučeny tak, že v každém bitovém intervalu dochází nejméně k jedné změně signálu. Tato změna je uprostřed bitového intervalu – nese užitečná data, současně tato změna slouží i k potřebám synchronizace.
Může být nutná ještě jedna změna, např. když jsou po sobě jdoucí signály reprezentovány stejně orientovanou změnou – pak musí být provedena ještě jedna opačná změna.

U diferenciálního Manchesteru je 0 změna signálu a hodnota 1 je beze změny. Delší posloupnost 1 by však mohla způsobit ztrátu synchronizace, proto se provádí uprostřed ještě jedna změna, ta slouží pouze pro časování.

Takže zatímco u "normálního" (nikoli diferenciálního) kódování Manchester slouží jedna hrana oběma účelům současně (a eventuelní druhá hrana vlastně jen připravuje půdu pro novou změnu), u diferenciálního kódování Manchester má každý účel svou vlastní hranu.

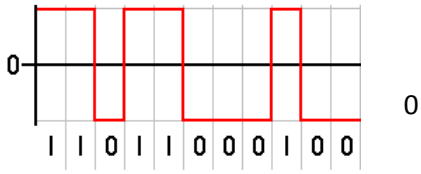


20. Popište metody NRZ-L, NRZ-M (NRZ-S). Uveďte jejich výhody a nevýhody.

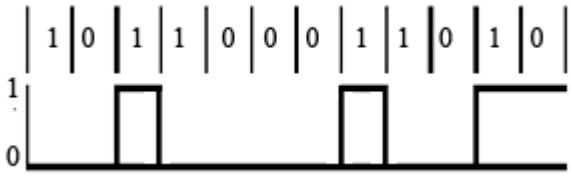
Z anglického „Non Return To Zero“ (bez návratu k nule). V tomto kódování je jednička "1" reprezentována konkrétní význačnou hodnotou (například kladným napětím). Nula "0" je reprezentována jinou význačnou hodnotou (například záporným napětím). Žádné další hodnoty se ve výsledném (nezašuměném) signálu nevyskytují, neexistuje zde třetí neutrální hodnota (například nulové napětí) jako je tomu u kódování s návratem k nule. Kvůli absenci neutrální hodnoty nelze toto kódování v základním tvaru použít pro synchronní přenosy, je potřeba přidat synchronizaci.

Nevýhody: nelze použít pro synchronní přenosy
Výhody: méně náročné kódování

NRZ – L: hodnota "1" je reprezentována například kladným napětím, hodnota "0" je reprezentována menším kladným napětím (případně hodnota "1" je reprezentována například záporným napětím, hodnota kladným napětím)



NRZ "Mark": hotnota "1" je reprezentována změnou, hodnota "0" je pokud změna nenastává. K přechodu dochází na sestupné hraně hodinového signálu pro daný bit.

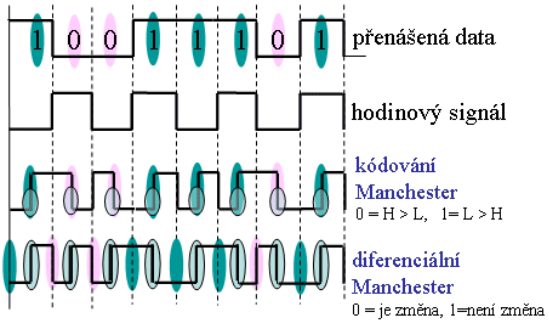


21. Popište metody kódování s dvojí fází (Manchester, diferenciální Manchester) a uveďte kde se používají.

Použití: např. u Ethernetu (Manchester), Token Ring (dif. Manchester)

Popis: Kódování Manchester je způsob zakódování dat, který se využívá pro přenos dat počítačovou sítí na fyzické vrstvě ISO/OSI modelu, např. v Ethernetu či Token Ringu.
V případě synchronního přenosu dat mezi odesílatelem a příjemcem je nutný synchronizační signál. Manchesterský kód spojuje původní datový signál se synchronizačním signálem a tedy umožňuje synchronní komunikaci

Manchester - 0 se kóduje přechodem do 0, 1 přechodem do 1;



Inverzní Manchester – opak Manchesteru, používal se v Ethernetu, jen u sítí do 100Mb/s
Diferenciální Manchester - 0 přechodem na začátku bit. intervalu, 1 bez přechodu; kóduje se změnou; používal se u sítí typu Token Ring; nezávisí na polaritě signálu

Dále viz 19

22. Vysvětlete rozdíl mezi spojově orientovaným a nespojovaným modelem komunikace. Pro každý z nich uveďte jejich výhody a nevýhody.

UDP (nespojový), na rozdíl od TCP (spojový) nezajišťuje mj. spolehlivost přenosu.

Spojový model: př. TCP, nejprve se stanice domluví na společné komunikaci, spojí se a teprve poté přenos dat, na konci poté dojde k ukončení spojení; zajištěno:

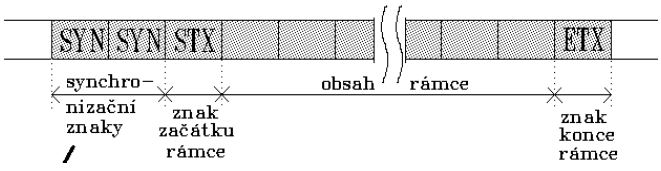
proudový přenos dat – není potvrzován každý paket, ale skupina (window)
spolehlivost – zajištěna potvrzováním příjmu skupiny paketů; ztracené nebo opožděné pakety příjemce nepotvrdí a odesílatel je pošle znovu
plně duplexní operaci – TCP umožňuje přijímat i odesílat data současně

výhodné pro větší přenosy dat

Nespojový model: Zpráva se považuje za jeden celek spolu s adresou příjemce. Doručení zprávy je nezávislé na doručení ostatních zpráv, zprávy mohou být doručeny ve špatném pořadí nebo ztraceny. Vhodné pro krátké zprávy, např. UDP.

23. Naznačte obecnou strukturu rámce na linkové úrovni pro délkově orientovaný protokol, znakově orientovaný protokol a bitově orientovaný protokol.

Znakově orientovaný

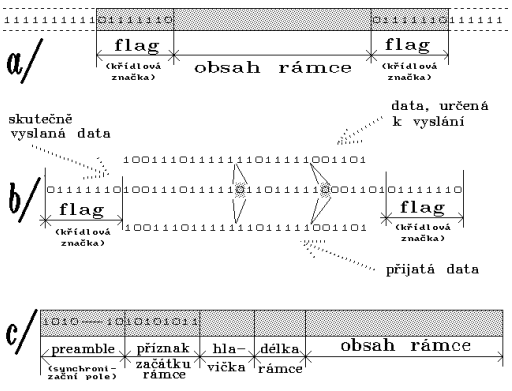


Potřebujeme-li pak přenášet data, tvořená posloupnostmi běžných ASCII znaků, vložíme blok znaků mezi dvojici speciálních: STX a ETX - řídící znaky přenosu.

Když potřebujeme přenést (jako data) i některé řídící znaky, nebo v případě, kdy místo znaků přenášíme obecná binární data - *vkládání znaků*, kdy je před řídící znaky STX a ETX vložen ještě jiný řídící znak - znak DLE (Data Link Escape, změna významu následujícího znaku). Ten se ovšem může vyskytovat i mezi vlastními daty, a proto se zde každý jeho výskyt zdvojuje.

Synchronní přenos - pomocí speciálních znaků SYN, které uvozují každý synchronně přenášený blok znaků. Synchronizace na úrovni rámců se při synchronním přenosu může dosahovat stejně, jako při přenosu asynchronním - pomocí řídících znaků přenosu.

Bitově orientovaný - Je založen na myšlence indikovat začátek a konec rámců nikoli řídícím znakem, ale skupinou bitů. Přenášená data jsou vyhodnocována bit po bitu, dokud není nalezena hledaná skupina bitů, indikující začátek rámce resp. jeho konec. Počet bitů, které tvoří vlastní obsah rámce, pak nemusí nutně být násobkem osmi.



Jednou z možností pro bitově orientovaný přenos je použít stejnou skupinu bitů, tzv. *křídlovou značku (flag)* pro uvození i zakončení rámce - a. Tato křídlová značka se pak ovšem nesmí vyskytovat "uvnitř" vlastního rámce.

Obvykle je křídlová značka tvořena posloupností "01111110", a potřebná transparence dat se zajišťuje vkládáním bitů (bit stuffing), při kterém je za každých pět po sobě jdoucích jedničkových datových bitů automaticky vložen jeden nulový bit (který příjemce zase automaticky odstraňuje) - b.
Další možností je uvození celého rámce (po tzv. preambuli neboli synchronizačním poli) tzv. příznakem začátku rámce (start-of-frame delimiter), za kterým následuje hlavička (header) předem stanoveného formátu, a údaj o délce rámce - c. Tato varianta se používá především u lokálních sítí.

24. Jaký je rozdíl mezi rámcem a paketem

Rámec – data přenášená (připravena) na linkové úrovni (větší obálka)
Paket – data přenášená (připravena) na síťové úrovni (menší obálka)

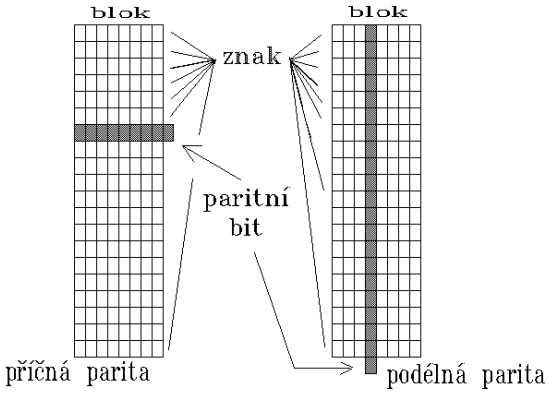
Na úrovni každé vrstvy (s výjimkou té nejnižší, fyzické vrstvy) se data přenáší po větších skupinách. Konkrétní specifické pojmenování těchto bloků je pak závislé na tom, o kterou konkrétní vrstvu jde - alespoň v případě dvou dalších vrstev, které se nacházejí nad nejnižší fyzickou vrstvou. Blokům dat, přenášeným na úrovni linkové vrstvy, se říká rámce (frames). Např. v dnešních lokálních sítích bývá linková vrstva nejčastěji „obydlena" technologií Ethernet a z ní vyplývajícími přenosovými protokoly. Takže zde je na místě mluvit o Ethernetových rámcích.
O patro výše - vrstva síťová - blokům dat, přenášeným na úrovni této vrstvy, se již neříká rámce, ale pakety (packets). Typické protokoly IP (z rodiny TCP/IP) a IPX/SPX (z rodiny „Novellských" protokolů) - proto je správné mluvit o IP paketech, IPX paketech (resp. paketech IPX/SPX) apod.
Rámec je větší obálkou, a paket obálkou menší, která se pro potřeby přenosu vkládá do větší obálky

25. Uveďte, jak se určuje Hammingova vzdálenost a jak se z ní dá určit kdy je kód detekční a kdy samoopravný.

Hammingova vzdálenost je počet pozic, na kterých se řetězce stejné délky liší, neboli počet záměn, které je potřeba provést pro změnu jednoho z řetězců na druhý
Detekční – pokud minimální Hammingova vzdálenost d_0, D = d_0 – 1, dokážeme detekovat D chyb
Samoopravný - K = 0,5 * (d_0 - 1) - pro d_0 liché; K = 0,5 * (d0 - 2) - pro d_0 sudé.... K – počet chyb, které jsme schopni opravit

26. Co jsou to paritní kódy, jakou mají detekční schopnost, uveďte příklad použití.

Nejjednodušší detekční kód - zabezpečení sudou nebo lichou paritou - přidává k datovým bitům jeden další bit a dokáže detekovat chybu v jednom bitu. Samoopravný kód, který umožňuje následnou opravu chyby v jediném bitu (tzv. rozšířený Hammingův kód), přidává ke každému 8-bitovému bytu navíc pět bitů (resp. 6 bitů ke každému 16-bitovému slovu).



Obr. 3.1.: Zabezpečení paritou

V praxi je výhodnější zabezpečovat celé posloupnosti znaků resp. celé přenášené bloky dat. Dodatečné bity, používané k detekci chyb, se pak nepřidávají znovu ke každému znaku, ale jen jednou k celému bloku dat (a přenesou se spolu s ním). Je-li pak chyba detekována,

nelze ji v rámci bloku lokalizovat až na jednotlivé znaky. Místo toho musí být celý blok prohlášen za chybný a přenesen znovu.

Podélná parita - longitudinal parity
je jedním možným způsobem zabezpečení celého bloku dat, chápaného jako posloupnost jednotlivých znaků. Zde se nekontroluje sudý resp. lichý počet jedničkových bitů v jednotlivých znacích, ale sudý resp. lichý počet jedničkových bitů ve stejnolehlých bitových pozicích všech znaků v bloku.
Použití podélné parity se někdy kombinuje i se zabezpečením jednotlivých znaků pomocí sudé resp. liché parity, která se pak pro odlišení od podélné parity označuje jako příčná či znaková parita (transversal, lateral parity).

27. Co jsou to cyklické kódy, kde se používají. Uveďte vztahy pro výpočet zabezpečení zprávy a kontrolu jejího zabezpečení.
Jde o kódy používané k zabezpečení dat při jejich přenosu (nebo i při jejich skaldování) a mají za úkol umožnit detekci případných chyb v těchto datech. Jsou to tedy kódy detekční, podobně jako tzv. parita či kontrolních součty. Odesilatel aplikuje na odesílaná data algoritmus, který vyplývá z povahy detekčního kódu. Výsledkem je pak zabezpečovací údaj, který odesilatel „přišpendlí" k původním datům, a odešle je příjemci. Ten aplikuje na přijatá data přesně stejný algoritmus, a výsledek porovná se zabezpečovacím údajem, který obdržel od odesilatele. Dostatečnou spolehlivost nabízí cyklické kódy (CRC).

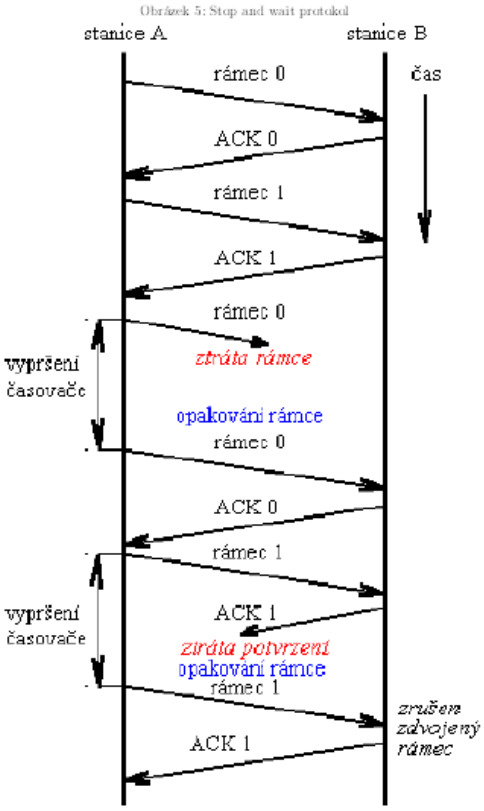
T(x) … výsledná zpráva
G(x) ... generující polynom
M(x) = ... původní zpráva
R(x) = M(x) mod G(x) ... zbytek po dělení

výsledná zpráva T(x) = M(x) + R(x)

28. Co je to transparentnost přenosu. Jak lze dosáhnout transparentnosti přenosu u bitově orientovaných protokolů a jak u znakově orientovaných.
Transparentní přenos znamená přenos dat, který žádná data neztratí ani nezkreslí. Problém při tom představují hlavně různé řídící znaky, které přenos nesmí interpretovat, nýbrž zacházet s nimi právě pouze jako s daty. Transparentní přenos tedy vyžaduje, aby se řídící znaky v datech buď "obalily" nějakými metaznaky, anebo aby se řídící znaky přenosové cesty úplně oddělily od přenášených dat.

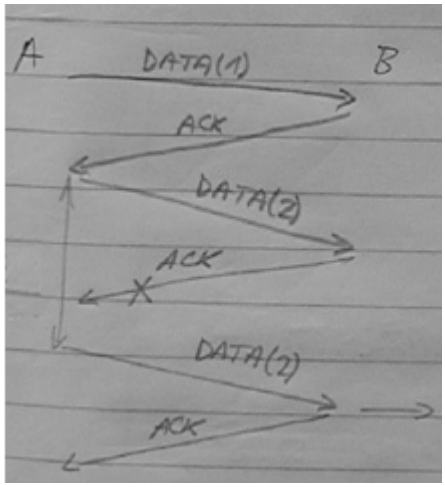
Bitově - potřebná transparence dat se zajišťuje vkládáním bitů (bit stuffing), při kterém je za každých pět po sobě jdoucích jedničkových datových bitů automaticky vložen jeden nulový bit (který příjemce zase automaticky odstraňuje)
Znakově – Vložíme blok znaků mezi dvojici speciálních: STX a ETX - řídící znaky přenosu. Když potřebujeme přenést (jako data) i některé řídící znaky, nebo v případě, kdy místo znaků přenášíme obecná binární data - *vkládání znaků*, kdy je před řídící znaky STX a ETX vložen ještě jiný řídící znak - znak DLE (Data Link Escape, změna významu následujícího znaku). Ten se ovšem může vyskytovat i mezi vlastními daty, a proto se zde každý jeho výskyt zdvojuje.

29. Co je to protokol Stop a Wait, kde se používá, jaké má vlastnosti. Uveďte typy rámců a strukturu jimi přenášené řídicí informace.
Odesilatel si po odeslání každého bloku dat nejprve počká na jeho explicitní potvrzení (nebo na vypršení časového limitu, do kterého by měl potvrzení dostat), a teprve pak podnikne další akci - podle přijatého potvrzení buď odešle další blok, nebo opakuje přenos již jednou odeslaného bloku. Je vhodné jen pro takové sítě, ve kterých je doba přenosu zanedbatelná -



tedy například pro lokální sítě. Lze použít kladné nebo záporné potvrzování, případně kombinaci obojího.

30. Navrhněte jednoduchý algoritmus pro vysílač a přijímač simplexního protokolu Stop a Wait. Pokud data přijdou do B, ale ztratí se ACK → opakování přenosu → v B je duplicita dat



31. Jak se liší protokol Stop a Wait od protokolů s klouzajícím okénkem?

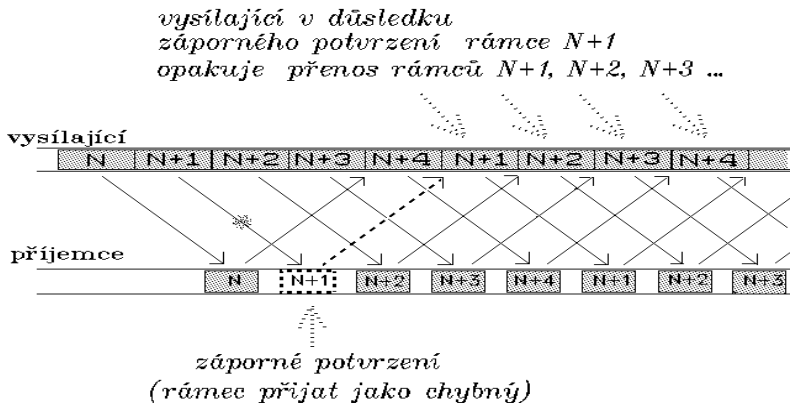
Stop-and-wait vyšle jeden rámec a čeká na potvrzení, případně vypršení časovače, je velmi neefektivní na kanálech s velkým zpožděním.

Metody klouzajícího okénka – stanice smí vysílat více rámců (dle šířky vysílacího okna), při odeslání se pro každý rámec nastartuje časovač, po přijetí rámce se vysílá ACK, v případě chyby nic nebo NACK, obě okénka kloužou po sekvenčních číslech.

Vysílací okno – buffer s vysílanými rámci, které dosud nebyly potvrzeny

Přijímací okno – buffer na přijímané rámce, které dosud nebyly doručeny vyšší vrstvě přijímače

32. Zakreslete průběh přenosu dat protokolem s klouzajícím okénkem a se sekvenčním příjmem. Jaký musí platit vztah mezi velikostí vysílacího a přijímacího okénka a proč.



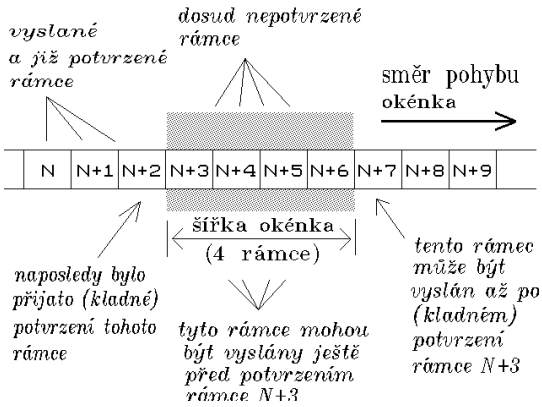
tzv. Go-Back-N; 1 vyrovnávací paměť

- ztratí-li se a1 => bez ohledu na to, co dál došlo, se vše zahodí a přenos znovu od a1
- Velikost okénka: W = N - 1, N je cisel pro ozn. ramce, W vel. Okna

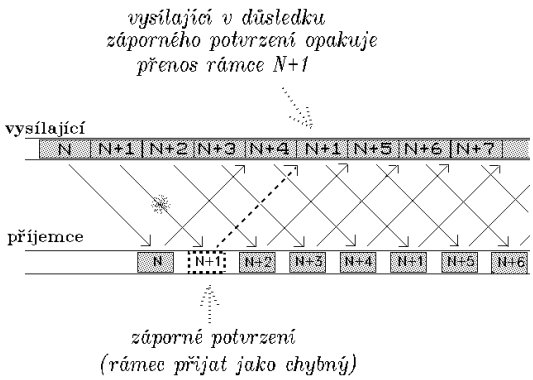
33. Zakreslete průběh přenosu dat protokolem s klouzajícím okénkem a s nesekvenčním příjmem. Jaký musí platit vztah mezi velikostí vysílacího a přijímacího okénka a proč.

Selective repeat → znovu se vyšle jen ten rámec, který nedošel

Velikost okénka: N – 1 (vysílací), N / 2 (přijímací)



Velikost okénka



Selective repeat

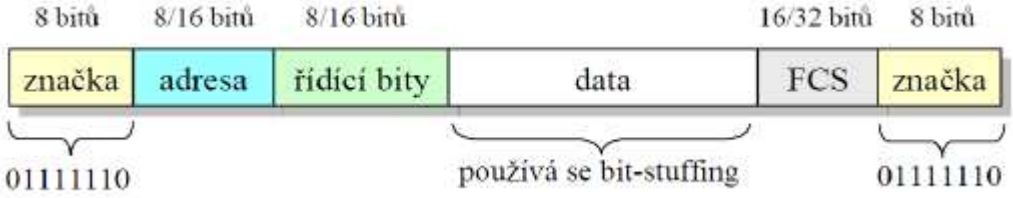
34. Co je to Petriho síť. Zakreslete Petriho síť pro simplexní protokol Stop a Wait s kladným potvrzováním.

Petriho síť je matematická reprezentace diskrétních distribuovaných systémů. Petriho síť graficky reprezentuje strukturu distribuovaného systému pomocí bipolárního orientovaného grafu.

35. Co je to Petriho síť. Zakreslete Petriho síť pro simplexní protokol Stop a Wait se záporným potvrzováním

36. Zakreslete formát rámce protokolu HDLC, vysvětlete význam jednotlivých polí a uveďte popis struktury řídicího pole.

HDLC je komunikační protokol linkové vrstvy, nadstavba protokolu SDLC, která detekuje chyby a řídí tok dat. Původně byl určen pro synchronní přenos dat, později byla norma HDLC rozšířena i pro asynchronní přenos.



Křídlová značka (Flag)

Každý HDLC rámec začíná a končí křídlovou značkou. Křídlová značka se skládá z osmi bitů: 0111 1110. Šest po sobě jdoucích jedniček určuje křídlovou značku. Jdou-li dvě křídlové značky po sobě, znamená to, že se jedná o prázdný rámec, se kterým se dále nepracuje. Pokud vstupní data obsahují více než pět jedniček za sebou, vloží se za každou pátou jedničku automaticky jedna nula. Toto se dá využít jen u bitově orientovaného přenosu.

Adresní pole

Adresní pole je dlouhé 8 bitů. Označuje adresu stanice, které je paket určen. Využívá ho mód NRM, kdy mezi sebou komunikuje více stanic. Je však nutné, proto ho obsahuje i protokol HDLC. Jedná se o linkovou adresu.

Řídicí pole

Řídicí pole je u U-rámců osmibitové. U I-rámců a S-rámců může být buď osmibitové nebo šestnáctibitové. Řídicí pole rozlišuje 3 typy HDLC-rámců:

- Informační rámce - určeny pro přenos dat, mohou však přenášet i některé řídicí informace.

- Nečíslované rámce - U-rámce (v nejnižších dvou bitech je 11) se používají pro přenos dat a pro řídicí funkce (inicializace, řízení linky) a také k přenášení příkazů a odpovědí:
- Rámce supervizoru - S-rámce (v nejnižších dvou bitech je 10) se používají pro řízení toku dat (požadavek na vysílání, potvrzování I-rámců atd.), S-rámce mohou být používány až když je linka inicializována, zpravidla neobsahují datové pole. S-rámec může potvrzovat správně přijatý rámec.

P/F bit

V NRM módu řídicí stanice nastaví tento bitu na P (=Pool). To znamená, že podřízená stanice smí vysílat data. Podřízená stanice nechává při vysílání tento bit nastaven. Tím signalizuje, že chce ve vysílání pokračovat. U posledního vysílaného rámce tento bit nastaví na (F=Final).

(http://cs.wikipedia.org/wiki/HDLC)

37. Jaké znáte decentralizované metody přístupu ke komunikačnímu médiu a čím se kvalitativně liší.

Rozdělení podle existence náhodného prvku při rozhodování kam vysílat
Řízené (deterministické) – Token Ring (Aloha)
Neřízené (nedeterministické) – levnější implementace než řízené; Ethernet (CSMA/CD)

Centralizované přístupové metody mají své výhody, ale i své nevýhody. Největší nevýhodou centralizovaných metod je asi to, že centrální autorita představuje příslovečné "single point of failure" - neboli jedno místo, jehož vyřazením (poruchou, závadou atd.) je vyřazena z provozu celá síť. Tuto nevýhodu naopak nemají distribuované metody, které nemají žádnou centrální autoritu, a uplatňování pravidel přístupové metody "rozkládají" rovnoměrně mezi všechny uzly.
I distribuované (decentralizované) přístupové metody se přitom mohou dělit na **řízené (deterministické)** a **neřízené (nedeterministické)**, s tím že obě tyto dílčí varianty mají smysl. Naopak u centralizovaných přístupových metod měly smysl spíše jen deterministické přístupové metody (zatímco nedeterministické by nepřinášely žádnou výhodu oproti deterministickým).
U distribuovaných metod však nedeterministické metody smysl mají. To proto, že jejich implementace může být výrazně jednodušší (lacinější) než implementace deterministických metod. Lze to ostatně demonstrovat na příkladu Ethernetu, který používá distribuovanou a nedeterministickou přístupovou metodu, a jeho implementace je relativně velmi jednoduchá. Naproti tomu například síť Token Ring používá distribuovanou a deterministickou přístupovou metodu, a jeho implementace je kvůli tomu složitější. S tím pak souvisí i komerční úspěšnost - Ethernet je dnes mnohem rozšířenější než Token Ring.
(http://www.earchiv.cz/b06/b0100001.php3)

38. Proč může dojít u metod náhodného přístupu k zahlcení komunikačního média, jak se tento stav projevuje, jak se řeší a jak mu lze předejít?

Aloha; Nedočkal-li se cíl potvrzení příjmu odeslaných dat → poslal je znova → dokud nedošlo k potvrzení → způsobovalo zahlcení sítě (chodí nové požadavky na vysílání, ale jejich vysílání končí kolizí); řešení – použít jiné metody :), synchronizace vysílání jedn. terminálů (start vysílání), detekce signálů od jiných stanic (naslouchají)

39. Vysvětlete základní princip metod náhodného přístupu. Jak se od sebe liší Aloha a CSMA?

Náhodný přístup - není zajištěno pořadí vysílání uzlů. Žádný uzel tak nemá garantováno, že se mu podaří přenést určité množství dat za určitou dobu.

Jedním z důležitých momentů celé koncepce sítě **Aloha** bylo to, že se jednotlivé uzly nesnaží monitorovat, zda právě neprobíhá nějaké vysílání.
Existuje ovšem celá škála přístupových metod, které možnost „příposlechu" využívají. Obecně se takovéto metody označují jako „metody **CSMA**"
Zajímavou otázkou ale je, jak se u metod CSMA má zachovat uzel, který díky příposlechu nosné zjistí že „éter" je právě obsazený. Možností je několik:

- jednou z nich je ta, že si zájemce o vysílání počká na skončení právě probíhajícího přenosu, a ihned poté začne vysílat sám. Ovšem s rizikem, že v době kdy čeká na konec probíhajícího přenosu, pojme stejný úmysl i jiný uzel, resp. jiné uzly, a také ony začnou čekat na konec -> kolize
- Alternativou je to, aby uzel, který detekuje právě probíhající vysílání, nebyl ve svém snažení až tak moc vytrvalý (či: naléhavý, angl.: persistent), v tom smyslu aby vytrvale čekal na konec vysílání a pak okamžitě uplatnil svůj požadavek na přenos. Místo toho příslušný uzel může i se svým požadavkem chvilku posečkat (odmlčet se, na vhodně zvolenou dobu), a pak postupovat znovu od začátku, tj. znovu zjišťovat jestli je „éter" volný nebo nikoliv.
- Kompromis mezi

40. Jak se liší naléhající CSMA od nenaléhající CSMA a co je to p-naléhající CSMA.

Zajímavou otázkou ale je, jak se u metod CSMA má zachovat uzel, který díky příposlechu nosné zjistí že „éter" je právě obsazený. Možností je několik:)

- **Naléhající CSMA** – pokud vysílá jiná stanice, čeká na uvolnění kanálu → ihned začne vysílat. Dojde-li ke kolizi s jiným vysíláním → odloží opakované vysílání na náhodně zvolenou pozdější dobu.
- **Nenaléhající CSMA** – test kanálu → vysílá jiná stanice → odloží vysílání na náhodně zvolenou (postup opakuje dokud není kanál volný). Dojde-li ke kolizi s jiným vysíláním → odloží vysílání na náhodně zvolenou pozdější dobu.
- **p–naléhající CSMA** - kompromis mezi dvěma výše uvedenými metodami. S pravděpodobností p se chová jako naléhající, s pravděpodobností (1–p) jako nenaléhající CSMA

(viz závěr 39)

41. Co je to CSMA/CD? Uveďte příklad lokální počítačové sítě, která tuto metodu používá.

Neřízená přístupová metoda **CSMA/CD** - na jedné straně jednoduchá a s malou režií, na druhé straně nezaručující, že se zájemce o vysílání skutečně dostane ke slovu, a fungující pouze statisticky (což má mj. za důsledek, že chování Ethernetu se při rostoucí zátěži začíná naopak zhoršovat)

První dvě písmena, **CS**, jsou od anglického Carrier Sense (česky: příposlech, detekce nosné). Znamenají to, že když některý uzel chce vysílat, nejprve poslouchá, zda nevysílá někdo jiný - snaží se detektovat signál (tzv. nosnou) pocházející od vysílání jiného uzlu.
Pokud uzel zjistí, že nikdo právě nevysílá, může začít vysílat sám. Sběrnicová topologie, v jejímž rámci jsou všechny uzly přímo připojeny na jediný vícebodový spoj, to umožňuje každému a přímo. Je tedy možný tzv. vícenásobný přístup (Multiple Access, odsud druhá dvě písmena, **MA**), který znamená nejen současné fyzické připojení více uzlů na jedno společné přenosové médium, ale i možnost současného příjmu více uzly, a dokonce i možnost současného vysílání více uzly.
Díky příposlechu nedochází k tomu, že by jeden uzel zahájil vysílání v době, když již nějakou dobu probíhá vysílání jiného uzlu (i když technicky by mohl, díky vícenásobnému přístupu). Může však dojít k tomu, že v této době projeví zájem o vysílání více uzlů. Všechny sice spořádaně počkají, až právě probíhající vysílání skončí, ale pak se doslova "utrhnou ze řetězu"

a začnou vysílat všechny najednou. Pak dochází k tzv. kolizi (collision), která je ale jednoznačně rozpoznatelná (viz výše). Každý uzel, který začal vysílat, může kolizi rozpoznat a z ní si pak odvodit, že nezačal vysílat sám. Dokonce je povinen to dělat, jak mu přikazují poslední dvě písmena v názvu přístupové metody CSMA/CD - **CD** neboli Collision Detect (detekce kolizí).

42. Vysvětlete základní princip metod rovnoměrného přístupu. Jak se liší od metod náhodného přístupu?

- Jde o deterministické (řízené) metody, mají jednoznačně definovaná pravidla, výsledek není ovlivněn náhodou (vs náhodný přístup) a je plně predikovatelný
  • vždy vedou k výsledku (u náhodného je výsledek nejistý)
  – např. metody token paging – vysílá pouze ten, který má *Token*, jednotlivé uzly si Token předávají (v logickém kruhu)
  • Token Ring, FDDI

43. Vysvětlete princip protokolu s bitovou mapou

Bitové mapy se využívají ke komprimaci signálu, v němž je ve velkém množství zastoupen jeden znak. Máme-li takovýto soubor, může se stát, že metoda potlačení nul není příliš efektivní, protože „nuly“ jsou ve skupinách po dvou či třech. V tomto případě by metoda bitových map dosáhla výrazně lepšího kompresního poměru.
Potlačovaný znak se nahradí v bitové mapě za „0“. adg**a => adga + 111001

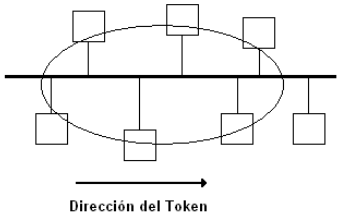
44. Vysvětlete princip metody předávání pověření ve fyzickém kruhu (Token Ring). Nakreslete jednoduché schéma, vysvětlete problém rekonstrukce kruhu a proč může nastat.

Předávání pověření – malý paket s nezaměnitelným obsahem. Kdo ho má, vysílá. V síti jen 1x. Stanice tvoří kruh a předávají si pověření. Jedna stanice je monitorovací – stará se o to, aby předávání fungovalo OK, aby se pověření neztratilo. Nezahlcuje se.
Rekonstrukce kruhu - když se ztratí pověření (token), tak někdo pošle do kruhu svou prioritu, ten kdo má vyšší ji zvýší. Komu se vrátí ta jeho priorita (má nejvyšší), tak se stane monitorem a předchozí stanice pak záložním. Monitor záloze občas zavolá, když neúspěšně, tak záloha převezme úlohu monitoru bez rekonstrukce

Vždy musí být jeden uzel ve funkci aktivního monitoru, který řeší nestandardní situace, má řídící funkci.

Právo vysílat po sdíleném médiu má ten, kdo je momentálním držitelem speciálního oprávnění (oprávnění vysílat). Toto oprávnění může mít prakticky libovolnou "fyzickou" podobu, resp. na jeho konkrétní fyzické podstatě příliš nezáleží - nejčastěji to je speciální (a malý) blok dat. Podstatné je pouze to, aby každý dokázal spolehlivě rozpoznat, zda je či není momentálním držitelem takovéhoto oprávnění, a aby toto oprávnění bylo možné předávat mezi uzly navzájem. Tedy aby toto oprávnění mohlo "kolovat" mezi potenciálními zájemci o vysílání. Pro správné a korektní fungování metody token passing je bezpodmínečně nutné, aby byl definován logický kruh - tedy pořadí, ve kterém si jednotlivé uzly cyklicky (dokola) předávají to, co pro ně reprezentuje zmíněné oprávnění. Důležité je, že tento kruh je skutečně pouze logickou záležitostí a nevynucuje si žádnou konkrétní fyzickou topologii. Na principu "token passing" tak mohou fungovat sítě s různými fyzickými topologiemi - například síť Token Ring se skutečně kruhovou fyzickou topologií, nebo třeba síť Token Bus, s fyzicky sběrnicovou topologií.

45. Vysvětlete princip metody předávání pověření v logickém kruhu (Token Bus). Nakreslete jednoduché schéma a vysvětlete problém rekonstrukce

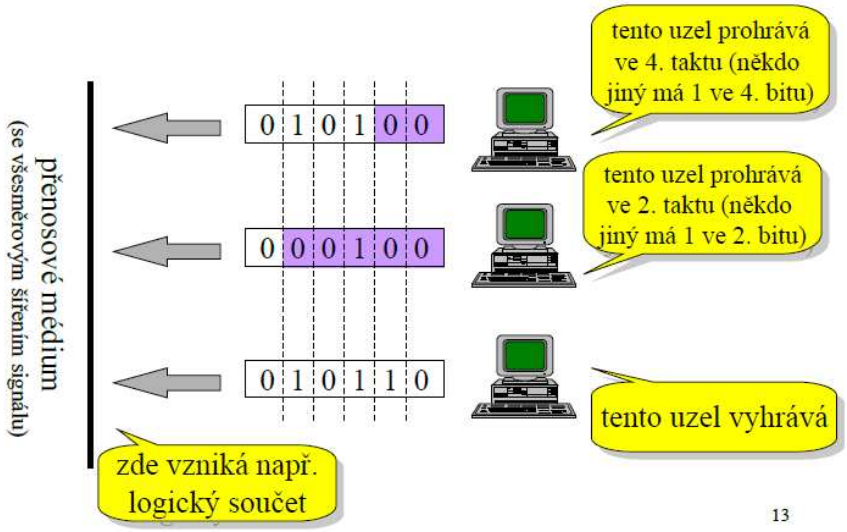


logického kruhu a proč se musí řešit. Jak se postupuje při rozpadu kruhu?
Pověření se předává na stejném principu jako u Token Ringu, jde prostě o logický kruh. Zbytek – fyzická topologie – je sběrnicová.

Obnova je realizována pomocí vysílání pověření libovolným uzlem v síti, který delší dobu detekuje nečinnost samotné sítě. V tomto případě se stav vyhodnotí jako kolize a začne probíhat algoritmus binárního vyhledávání adres podle vzestupného pořadí. Po tomto kroku se vytvoří nová síť (logický kruh).

46. Jak se liší metody rovnoměrného přístupu od metod prioritního přístupu? Co je to metoda prioritního přístupu řízení kódem?

Prioritní přístup – o tom, kdo bude vysílat, rozhoduje priorita stanice. Než chtějí stanice vysílat, pošlou svoji prioritu → vítěz vysílá. Technika výpočtu priority může být různá, dle přenosového média.



Rovnoměrný přístup – předávání pověření, viz výše.

47. Co je to problém monopolizace přístupu v mnohabodových sítích, kdy vzniká a jak se řeší. Uveďte algoritmus.

Monopolizace – uzel s vysokou prioritou žádá o povolení vysílat => vždy vyhrává
Řešení:

1. zavedení dynamické priority:
   -pole priority se rozdělí na dvě části - dynamickou(větší význam) a statickou prioritu
   - při neúspěšném pokusu vysílat zvýším dynamickou prioritu o 1
   - dynamická priorita musí být v rozsahu n ... to se ale může zdát hodně
   - doba obsloužení max. N
2. jednobitová dynam. priorita
   - doba obsloužení požadavku v 2n-1 (tj. prodlouží se to)
   - použití v případě bezdrátových přenosů

Přístupová metoda CSMA/CD, používaná v Ethernet, to řeší následovně: interval, ze kterého se vybírá náhodná doba pro odmlčení, se při každém neúspěšném pokusu zdvojnásobuje. Dělá se to tak celkem 16x, a teprve pokud se to ani na šestnáctý pokus nepodaří, přístupová metoda to vzdá a ohlásí neúspěch. **(nevim jestli se to toho týká???)**

48. Uveďte typy protokolu Ethernet, přenosové rychlosti, rozlehlost sítě, topologii a formát rámce. Jaký je rozdíl mezi rámci podle standardu Ethernet II a standardu IEEE 802.3?

Rámce - tam, kde rámec IEEE 802.3 má ve své hlavičce údaj o celkové délce rámce, tam (tj. na stejném místě) má rámec Ethernet_II údaj o typu svého obsahu (tzv. EtherType). Naštěstí rozlišení obou typů rámců je vždy možné, protože zmíněný EtherTyp je vždy číselně větší než maximální možná délka Ethernetového rámce (1500 bytů).

Typy:

- *DIX Ethernet*
- *Ethernet II*
- *10Base5* (10 rychlost v megabitech za sekundu, base přenos v základním pásmu, 5 rozlehlost sítě ve stovkách metrů)
- *10BaseT* (na pouhých 100 metrů, rychlost 10 v megabitech za sekundu)
- *Fast Ethernet* – 100megabitový Ethernet, je k dispozici pro kroucenou dvojlinku a optická vlákna
- *Gigabitový Ethernet* - zvýšil přenosovou rychlost na 1 Gbit/s. Opět recykloval co nejvíce prvků z původního Ethernetu, teoreticky i algoritmus CSMA/CD. V praxi je ale gigabitový Ethernet provozován pouze přepínaně s plným duplexem. Důležité je především použití stejného formátu rámce. Původně byl definován pouze pro optická vlákna (IEEE 802.3z), později byla doplněna i varianta pro kroucenou dvojlinku (IEEE 802.3ab).
- *Desetigigabitový Ethernet* - představuje zatím poslední standardizovanou verzi. Jeho definice byla jako IEEE 802.3ae přijata v roce 2003. Přenosová rychlost činí 10 Gbit/s, jako médium zatím slouží hlavně optická vlákna a opět používá stejný formát rámce. Algoritmus CSMA/CD byl definitivně opuštěn, tato verze pracuje vždy plně duplexně. V současnosti (2008) byla vyvinuta jeho specifikace pro kroucenou dvojlinku s označení IEEE 802.3an. Začíná se zavádět.

Formát rámce se popisuje pomocí oktetů, což je osmice bitů. Důvodem je přesnost definice, protože některé počítače mohou pracovat s jinou základní délkou bajtu (např. 4 nebo 10 bitů), což by v počítačových sítích způsobovalo nekompatibility. Níže uvedená tabulka popisuje rámec Ethernet II a 802.3, které se liší využitím jednoho pole pro typ nebo pro délku.

Ethernetový rámec

Preambule	SFD	MAC cíle	MAC zdroje	Typ/délka	Data a výplň	CRC32	Mezera mezi rámci
7× oktet 10101010	1× oktet 10101011	6 oktetů	6 oktetů	2 oktety	46-1500 oktetů	4 oktety	12 oktetů
		64-1518 oktetů					
72-1526 oktetů							

Preambule – 7 oktetů, střídavě binární 0 a 1; slouží k synchronizaci hodin příjemce
SFD – označení začátku rámce (Start of Frame delimiter), oktet 10101011
MAC cíle – MAC adresa cílového síťového rozhraní o délce 48 bitů
MAC zdroje – MAC adresa zdrojového síťového rozhraní
Typ/délka

- pro Ethernet II je to pole určující typ vyššího protokolu
- pro IEEE 802.3 udává délku pole dat

Data – pole dlouhé minimálně 46 a maximálně 1500 oktetů (46—1500 B); minimální délka je nutná pro správnou detekci kolizí v rámci segmentu
Výplň – vyplní zbytek datové části rámce, pokud je přepravovaných dat méně než 46 B
CRC32 – kontrolní součet

49. Jak vzniká kolize při použití metody CSMA/CD a proč jí nelze zabránit? Nakreslete obrázek.

Díky příposlechu (detekci nosné) nedochází k tomu, že by jeden uzel zahájil vysílání v době, když již nějakou dobu probíhá vysílání jiného uzlu. Může však dojít k tomu, že v této době projeví zájem o vysílání více uzlů. Všechny sice spořádaně počkají, až právě probíhající vysílání skončí, ale pak se doslova "utrhnou ze řetězu" a začnou vysílat všechny najednou. Pak dochází k tzv. kolizi (collision), která je ale jednoznačně rozpoznatelná. Každý uzel, který začal vysílat, může kolizi rozpoznat a z ní si pak odvodit, že nezačal vysílat sám. Dokonce je povinen to dělat, jak mu přikazují poslední dvě písmena v názvu přístupové metody CSMA/CD - CD neboli Collision Detect (detekce kolizí).

Pravidlo je takové, že každý uzel, který detektuje kolizi, se na určitou dobu odmlčí, a teprve pak může znovu usilovat o své vysílání.

Kolizím nelze zabránit, protože neexistuje žádný centrální rozhodčí, který by to řídil.

Obrázek nemam