

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

LAN - lokální síť. 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) – sběrnice s předáváním pověření
- Token ring (IEEE 802.5) – kruhová síť
- Bezdrátové sítě (Wi-Fi, IEEE 802.11)

MAN - Metropolitní síť. 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 síť. 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, ujití 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

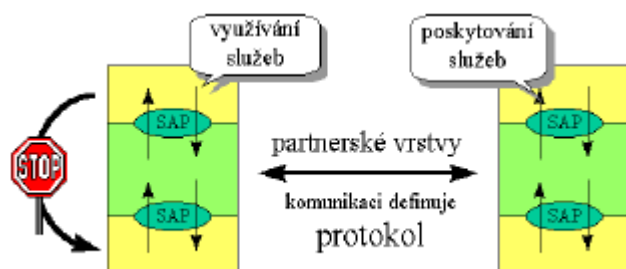
přepínání kanálů – existuje kanál mezi 2 body → data jdou tímto kanálem; kanál je virtuální; kanál se vytvoří před navázáním spojení nastavením přepínačů v bodech sítě → kanál se dále chová jako přímý spoj

- + 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 standardizovány

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*

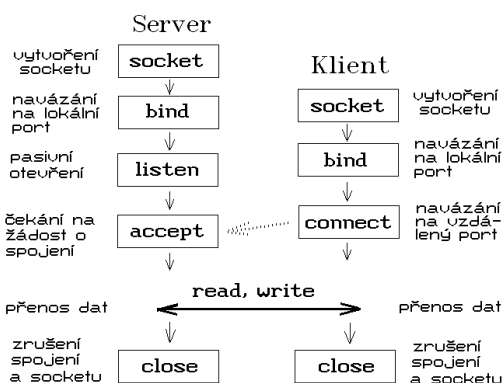
Otevření portu – *listen* – socket pasivně čeká na příchozí žádosti o navázání spojení, jako parametr délka fronty; když přijde žádost → OS žádost přijme a vytvoří nový socket,

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

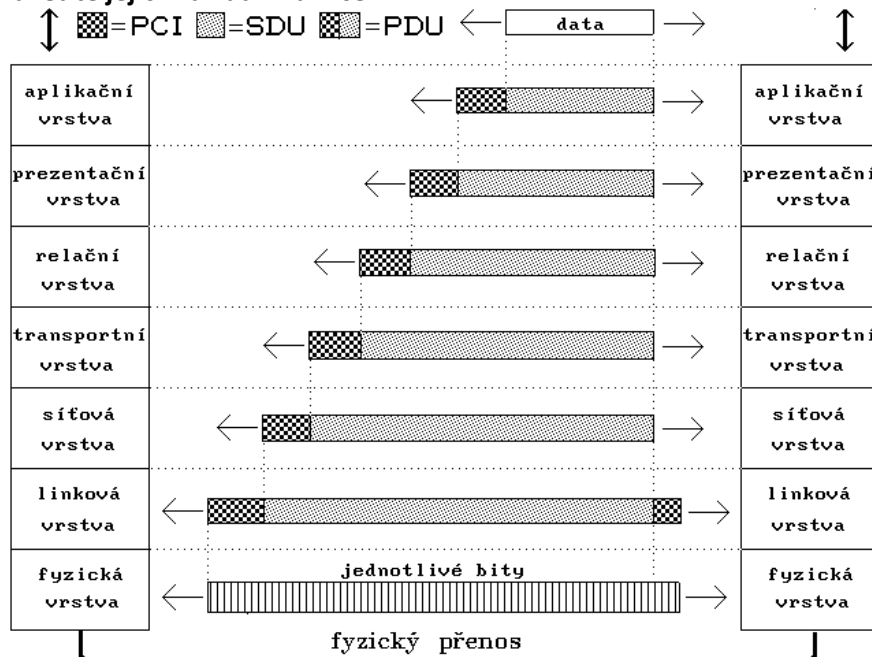
Klient:

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.



Fyzická vrstva - úkolem zajistit přenos jednotlivých bitů mezi příjemcem a odesílatelem 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 zajistit 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.

TCP/IP	ISO/OSI
Aplikační vrstva	Aplikační vrstva
Transportní vrstva	Prezentační vrstva
Síťová (IP) vrstva	Relační vrstva
Vrstva síťového rozhraní	Transportní vrstva
	Síťová vrstva
	Linková vrstva
	Fyzická vrstva

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 síť 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 odesílatele až ke svému skutečnému příjemci, přes případné směrovače resp. brány. Vzhledem k nespojovému 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.

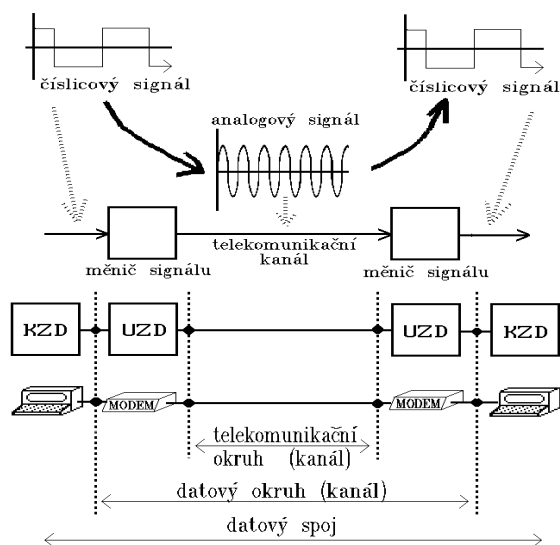
Vrstva aplikační - jejími entitami jsou jednotlivé aplikační programy, které na rozdíl od referenčního modelu ISO/OSI komunikují přímo s transportní vrstvou.

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).

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.



Obr. 8.1.: Datový spoj a okruh

(nevím <http://www.earchiv.cz/a91/a146c110.php3>)

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

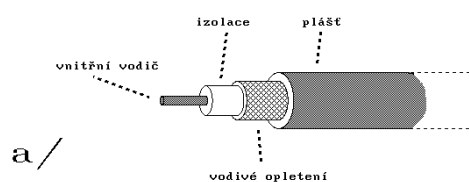
Koaxiální kabel (a) - Tvoří jej vnitřní vodič, kolem kterého je nanесena izolující vrstva dielektrika. Koaxiální kabely se používají např. v lokálních sítích Ethernet.

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

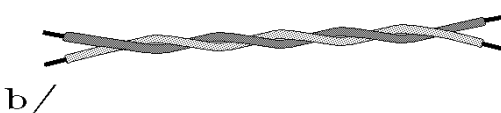
tenký - tloušťka kabelu je 0,25 palců, přenáší signál do vzdál necelých 200m

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

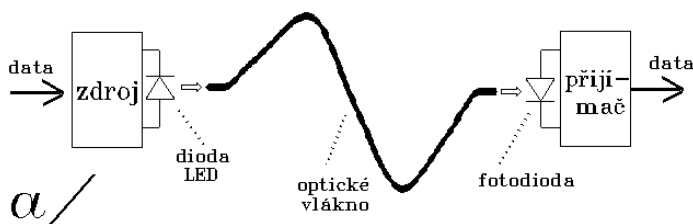
Optické kabely - přenos číslicových dat pomocí světelných impulsů, optické, s tenkým jádrem obaleným vhodným pláštěm



a/



b/

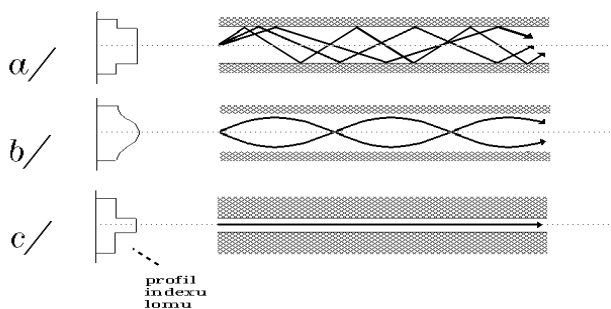


9. Jaké druhy optických vláken znáte? Čím se od sebe liší?

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, snazší spojování, velká numerická apertura a možnost buzení luminiscenční diodou

Jednovydové (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.

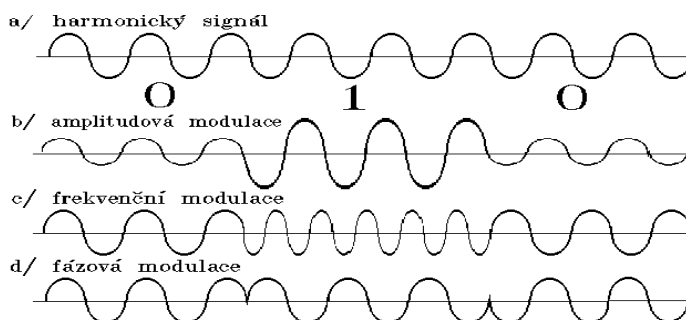
Zajímavým důsledkem rozdílů mezi přenosem v základním a přeloženém pásmu je i jejich typický dosah - u přenosů v základním pásmu bývá menší, a u přenosů v přeloženém pásmu naopak větší, často i dosti výrazně. Důvodem je fakt, že v tomto druhém případě je skrz příslušnou přenosovou cestu fakticky přenášen 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

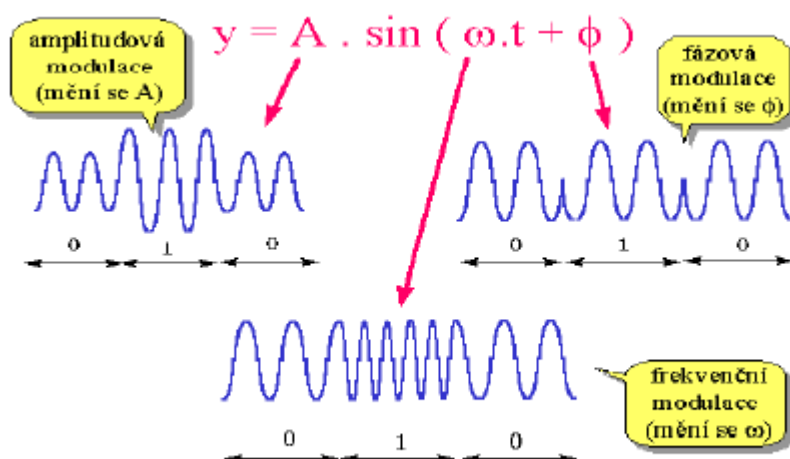
Frekvenční – při které jsou jednotlivé logické hodnoty vyjádřeny různými frekvencemi (kmitočty) harmonického signálu (FM), analogové televizní soustavy

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

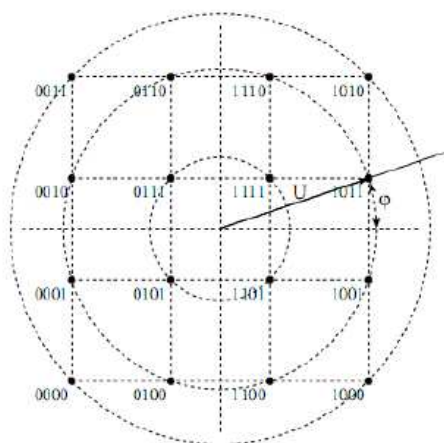


Obr. 4.2.: Modulace při přenosu v přeloženém pásmu

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.

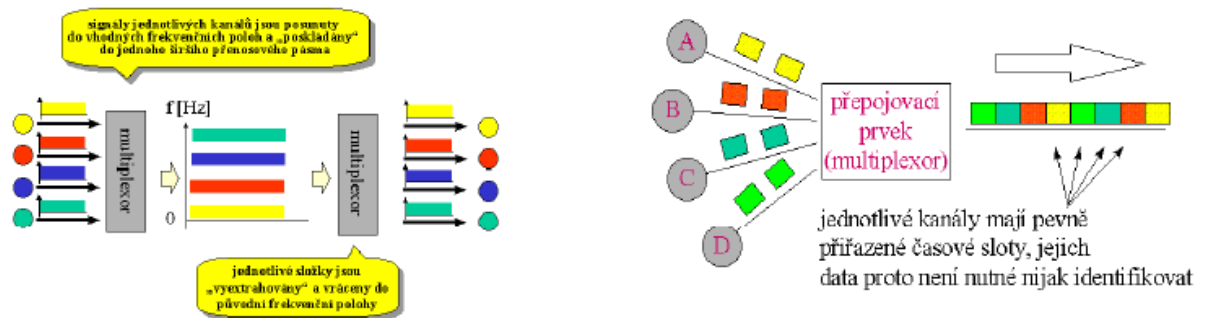


16. Jaký je rozdíl mezi frekvenčním a časovým multiplexem. Zakreslete jednoduchý obrázek.

frekvenční multiplex (analog) – 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

časový multiplex (digital) – 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“.

Modulace – přenášen signál, který se šíří médiem nejlépe → často sinusové signály → informace se přenáší prostřednictvím změn → měníme charakter nosného signálu modulačním (např. sin)

Kódování signálu – zabezpečení signálu např. proti chybám

Bez návratu k nule – NRZ – 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?

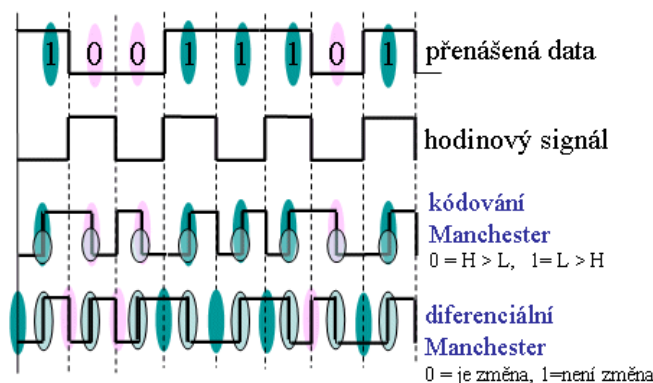
Diferenciální a nediferenciální variantu má např. kódování Manchester.

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.



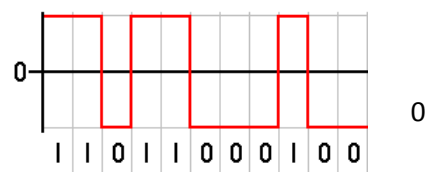
20. Popište metody NRZ-L, NRZ-M (NRZ-S). Uveďte jejich výhody a nevýhody.

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.

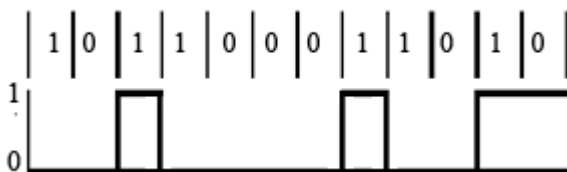
Nevýhody: nelze použít pro synchronní přenosy

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

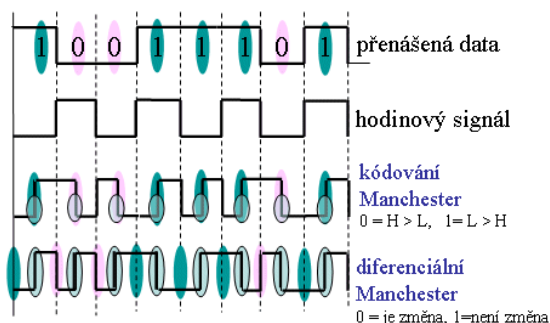


21. Popište metody kódování s dvojí fází (Manchester, diferenciální Manchester) a uveďte kde se používají.

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 spojořově orientovaným a nespořovaným modelem komunikace. Pro každý z nich uveďte jejich výhody a nevýhody.

UDP (nespořový), na rozdíl od TCP (spořový) nezajiřtuje mj. spoleřlivost přenosu.

Spořový model: př. TCP, nejprve se stanice domluví na spoleřné komunikaci, spoří se a teprve poté přenos dat, na konci poté dojde k ukončení spoření; zajiřtěno:

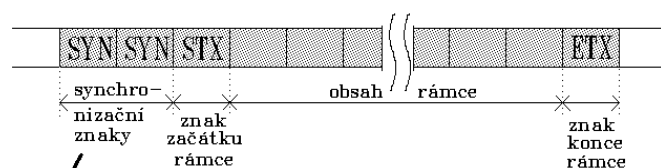
- proudový přenos dat – není potvrzován každý paket, ale skupina (window)
- spoleřlivost – zajiřtěna potvrzováním přijmu skupiny paketů; ztracené nebo opožděné pakety příjemce nepotvrdí a odesílatel je pošle znovu
- plně duplexní operaci – TCP umořňuje přijímat i odesílat data současně

výhodné pro větřší přenosy dat

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

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

Znakově orientovaný

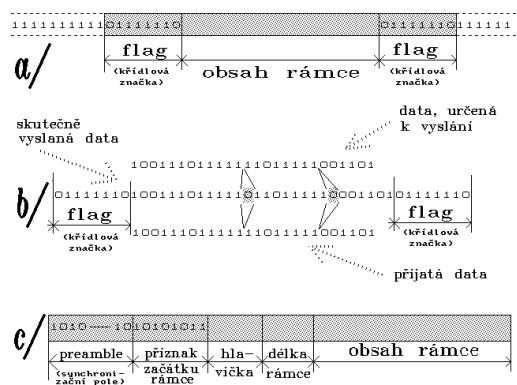


Potřebujeme-li pak přenášet data, tvořená posloupnostmi běžných ASCII znaků, vloříme blok znaků mezi dvojicí speciálních: STX a ETX - řídící znaky přenosu.

Když potřebujeme přenést (jako data) i některé řídící znaky, nebo v případě, kdy místo znaků přenášíme obecná binární data - *ukládání znaků*, kdy je před řídící znaky STX a ETX vlořen 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 zalořen na myřlenice 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.

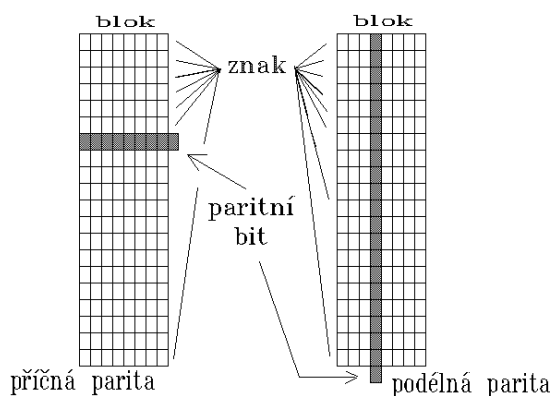
Hammingova vzdálenost je počet pozic, na kterých se řetězce stejné délky liší, neboli počet změn, které je potřeba provést pro změnu jednoho z řetězců na druhý

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; $K = 0,5 * (d_0 - 2)$ - 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



Obr. 3.1.: Zabezpečení paritou

ale jen jednou k celému bloku dat (a přenesou se spolu s ním). Je-li pak chyba detekována,

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).

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,

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 stejnohlých 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. Odesílatel aplikuje na odesílaná data algoritmus, který vyplývá z povahy detekčního kódu. Výsledkem je pak zabezpečovací údaj, který odesílatel „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 odesílatele. Dostatečnou spolehlivost nabízí cyklické kódy (CRC).

$T(x)$... výsledná zpráva

$G(x)$... generující polynom

$M(x)$ = ... původní zpráva

$R(x) = M(x) \bmod G(x)$... 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 řídicí znaky, které přenos nesmí interpretovat, nýbrž zacházet s nimi právě pouze jako s daty. Transparentní přenos tedy vyžaduje, aby se řídicí znaky v datech buď "obalily" nějakými metaznaky, anebo aby se řídicí znaky přenosové cesty úplně oddělily od přenášených dat.

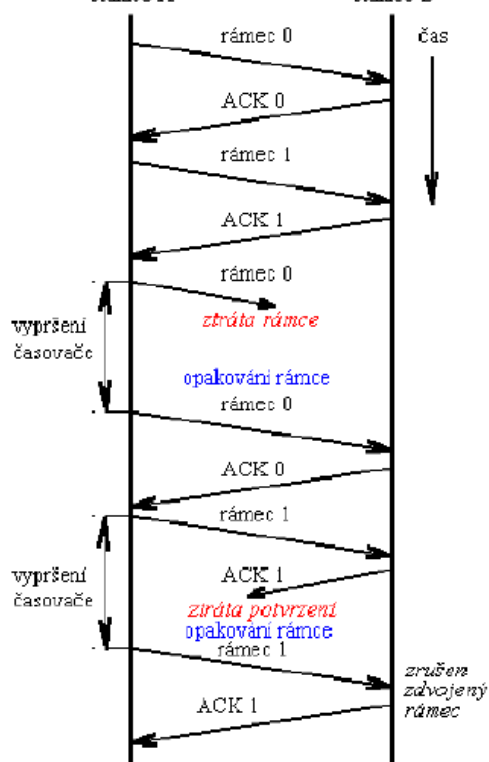
Bitově - potřebná transparence dat se zajišťuje vkládáním bitů (bit stuffing), při kterém je za každých pět po sobě jdoucích jedničkových datových bitů automaticky vložen jeden nulový bit (který příjemce zase automaticky odstraňuje)

Znakově – Vložíme blok znaků mezi dvojici speciálních: STX a ETX - řídicí znaky přenosu. Když potřebujeme přenést (jako data) i některé řídicí znaky, nebo v případě, kdy místo znaků přenášíme obecná binární data - *vkládání znaků*, kdy je před řídicí znaky STX a ETX vložen ještě jiný řídicí 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.

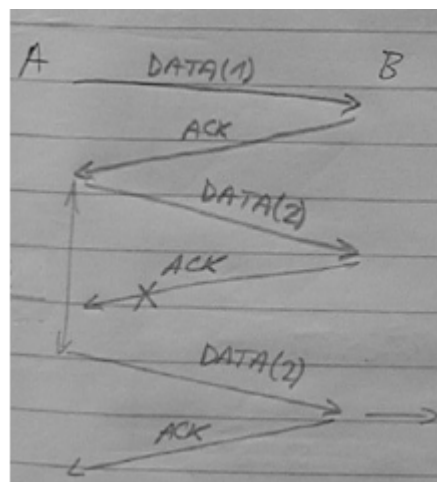
Odesílatel si po odeslání každého bloku dat nejprve počká na jeho explicitní potvrzení (nebo na vypršení časového limitu, do kterého by měl potvrzení dostat), a teprve pak podnikne další akci - podle přijatého potvrzení buď odešle další blok, nebo opakuje přenos již jednou odeslaného bloku. Je vhodné jen pro takové sítě, ve kterých je doba přenosu zanedbatelná -

stanice A stanice B



tedy například pro lokální síť. 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.

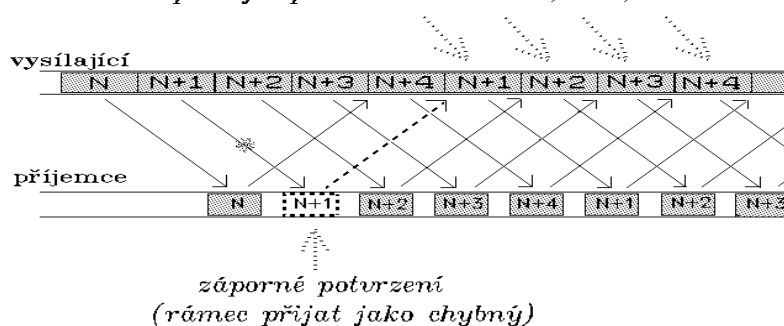
Metody klouzajícího okénka – stanice smí vysílat více rámců (dle šířky vysílacího okna), při odeslání se pro každý rámec nastartuje časovač, po přijetí rámce se vysílá ACK, v případě chyby nic nebo NACK, obě okénka kloužou po sekvenčních číslech.

Vysílací okno – buffer s vysílanými rámcí, 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.

vysílající v důsledku
záporného potvrzení rámce $N+1$
opakuje přenos rámců $N+1$, $N+2$, $N+3$...

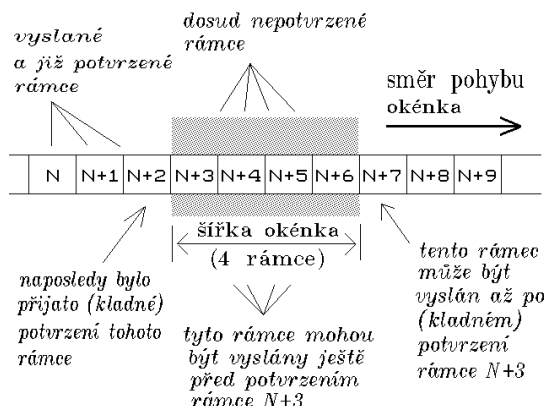


tzv. Go-Back-N; 1
vyrovnávací paměť
- ztratí-li se a1 => bez
ohledu na to, co dál
došlo, se vše zahodí a
přenos znovu od a1
- Velikost okénka: $W = N - 1$, N je císle pro ozn.
ramce, W vel. Okna

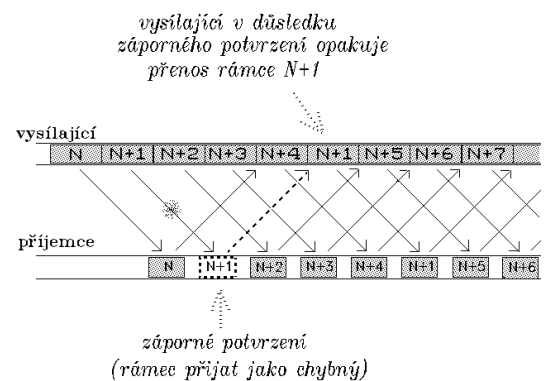
33. Zakreslete průběh přenosu dat protokolem s klouzajícím okénkem a s nesequenčním příjmem. Jaký musí platit vztah mezi velikostí vysílacího a přijímacího okénka a proč.

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

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



Velikost okénka



Selective repeat

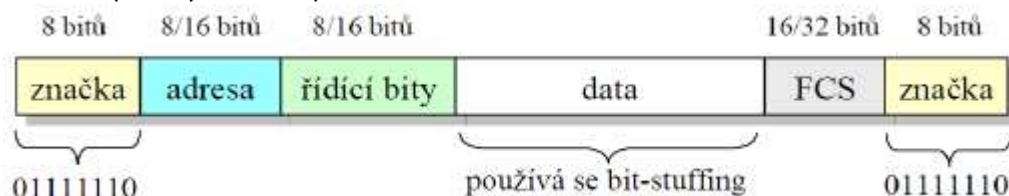
34. Co je to Petriho síť. Zakreslete Petriho síť pro simplexní protokol Stop a Wait s kladným potvrzováním.

Petriho síť je matematická reprezentace diskretních 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.

Řídící pole

Řídící pole je u U-rámců osmibitové. U I-rámců a S-rámců může být buď osmibitové nebo šestnáctibitové. Řídící 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 médium 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 chvíli posečkat (odmíčet 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 naléhavý CSMA od nenaléhavý CSMA a co je to p-naléhavý 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:)

- **Naléhavý 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.
- **Nenaléhavý 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-naléhavý CSMA** - kompromis mezi dvěma výše uvedenými metodami. S pravděpodobností p se chová jako naléhavý, s pravděpodobností (1-p) jako nenaléhavý 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 režii, 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“. $adg^{**}a \Rightarrow adga + 111001$

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

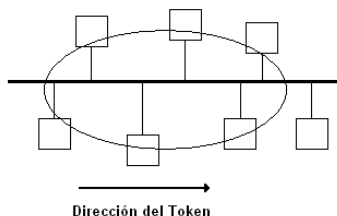
Předávání pověření – malý paket s nezaměnitelným obsahem. Kdo ho má, vysílá. V síti jen 1x. Stanice tvoří kruh a předávají si pověření. Jedna stanice je monitorovací – stará se o to, aby předávání fungovalo OK, aby se pověření neztratilo. Nezahlučuje se.

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 převeze úlohu monitoru bez rekonstrukce

Vždy musí být jeden uzel ve funkci aktivního monitoru, který řeší nestandardní situace, má řídicí 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 takového 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 sběrníkovou topologií.

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



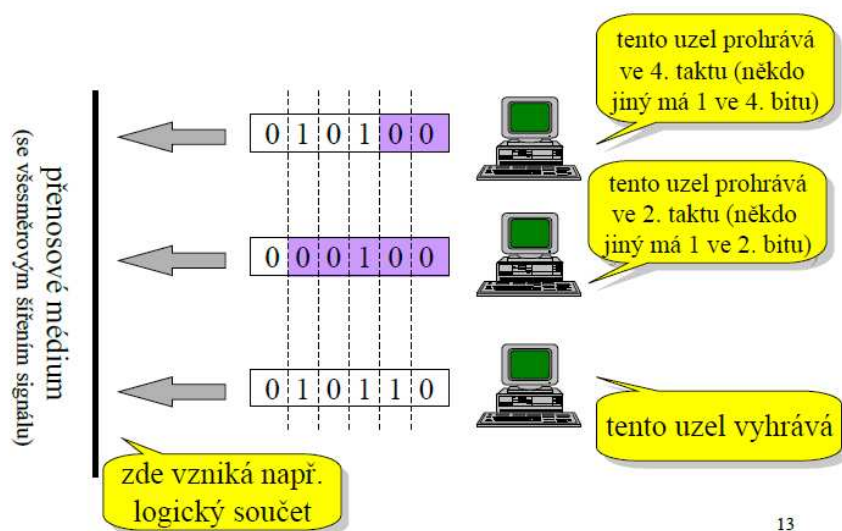
logického kruhu a proč se musí řešit. Jak se postupuje při rozpadu kruhu?

Pověření se předává na stejném principu jako u Token Ringu, jde prostě o logický kruh. Zbytek – fyzická topologie – je sběrnice.

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.



13

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 $n \dots$ to se ale může zdát hodně
- doba obsluhy max. N

2. jednobitová dynam. priorita

- doba obsluhy 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. (nevím 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 EtherType 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 nekompatibilitu. Níže uvedená tabulka popisuje rámec Ethernet II a 802.3, které se liší využitím jednoho pole pro typ nebo pro délku.

Ethernetový rámec

Preamble	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		

Preamble – 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

o pro Ethernet II je to pole určující typ vyššího protokolu

o 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

50. Které protokoly popisují standardy IEEE 802.11, IEEE 802.15 a IEEE 802.16

IEEE 802.11 – WiFi, 802.11b a 802.11g pásmo 2,4GHz, 802.11a pásmo 5GHz

IEEE 802.15 – ZigBee – bezdrátová komunikační technologie, pro sítě PAN, dosah 75 metrů, rychlost až 250 kbit/s

IEEE 802.16 – WiMAX – bezdrátová komunikace pro venkovní sítě, stále se vyvíjí

51. Co jsou to virtuální lokální počítačové sítě? Jak se tvoří a v čem spočívají jejich výhody?

Logicky nezávislá síť v rámci jednoho nebo několika zařízení.

Clem je učinit logickou organizaci sítě nezávislou na fyzické vrstvě, čímž lze usnadnit správu sítě, zvýšit její výkon a podpořit bezpečnost.

52. Co je to most, jak se liší od opakovacího? Jaké jsou základní funkce mostu?

Opakovač – digitální zesilovač, pracuje na fyzické vrstvě. Nechápe význam jednotlivých bitů. Bez něj například dostah 10Gb Ethernetu, při užití kroucenné dvoulinky jen 100m, tenký koaxiál 185m.

Most – Má inteligenci, dokáže rozhodnout, zda data zůstanou jen v lokální segmentu, či je nutné je poslat dál. Most tedy ke své funkci potřebuje znát formát přenášených dat, a to alespoň natolik, aby si z nich dokázal odvodit, kdo je jejich příjemcem a kdo odesílatelem. Kromě toho pak potřebuje i informaci o tom, které uzly se nachází ve kterých segmentech.

Tuto druhou skupinu informací může most získat různými způsoby:

1, Jednou z možností je apriorní "vyplnění tabulky", kterou most ve vhodné formě dostane při svém spuštění a podle které pak pracuje, aniž by ji sám jakkoli měnil. To je jistě velmi robustní řešení, vhodné pro takové sítě, jejichž konfigurace se mění jen zcela výjimečně. V praxi je ale toto řešení používáno jen velmi málo, protože existují jiná, ještě výhodnější řešení.

2, Další možností je nechat most se takhle informace naučit, dá si je do souvislosti adresu se segmentem. Postupně se naučí vše potřebné, používá se u Ethernetu.

53. Vysvětlete jak funguje Spanning Tree algoritmus a kdy se používá.

Most se dokáže sám učit, když mu přijde datový rámec ze směru A, od odesílatele X, odvozí, že uzel X leží v tomto směru. Pokud je ale spojení redundantní (existují cykly v grafu popisujícím síť), přijde mu taková informace z více směrů a nemůže se rozhodnout.

Ovšem existence redundantního spojení je žádoucí, zvyšuje se tím spolehlivost sítě. Je tedy nutné, aby se mosty domluvily a vybraly takovou cestu, která nebude obsahovat žádné cykly. Mosty se tedy pomocí speciálního protokolu domluví na nejvhodnější acyklické topologii. Z této vzájemné domluvy vychází jeden most v roli tzv. kořenového mostu (root bridge), a všechny ostatní mosty vybírají ze všech svých směrů právě jeden, který prohlásí za "kořenový" (ve smyslu: vedoucí ke kořenovému mostu). Tím vzniká přísně stromovitá (a tudíž acyklická) struktura, v jejímž kořeni je kořenový most. Celý algoritmus je navíc řešen tak, aby při výpadku některého mostu či spojení dokázal využít existenci redundantních spojení a zajistil automatické zotavení celé sítě.

54. Vysvětlete jak funguje algoritmus Source Routing a kdy se používá?

A nyní již k samotné pointě: source routing není způsobem směrování, jak by slovíčko "routing" napovídalo. Místo toho jde o jeden konkrétní druh "mostění" (bridging), neboli o jeden konkrétní způsob fungování mostu. Samotný "source routing" vyvinula firma IBM pro své síť **Token Ring**. Vše je založeno na myšlence, že způsob průchodu datových rámců skrz jednotlivé mosty se určí předem a potřebné pokyny k průchodu takto zvolenou trasou se vloží do každého jednotlivého rámce. Tyto pokyny přitom mají formu lineárního seznamu mostů, přes které má datový rámec postupně projít. Podstatná je na celé věci skutečnost, že o celé trase přenosu datových rámců rozhoduje již jejich odesílatel - odsud přívlastek "source" (doslova: od zdroje).

Zajímavé je na celé věci i to, podle čeho vlastně odesílatel volí nejvhodnější trasu, kterou pak zakóduje do každého odesílaného rámce: na všechny strany vyšle speciální "průzkumný" rámec, který se sám následně šíří do všech existujících směrů, dokud nedojde k hledanému cíli. Od něj se rámec vrací zpět ke svému původnímu odesílateli a nese v sobě informaci o trase, kterou přitom prošel.

55. Jaké problémy řeší síťová úroveň?

Chtějí-li spolu komunikovat dva uzly počítačové sítě, mezi kterými neexistuje přímé spojení, je nutné pro ně najít alespoň spojení nepřímé - tedy vhodnou cestu, vedoucí přes mezilehlé uzly od jednoho koncového uzlu ke druhému. Možných cest může být samozřejmě více, někdo je však musí najít, jednu z nich vybrat, a pak také zajistit správné předávání dat po této cestě. Všechny tyto úkoly má v referenčním modelu ISO/OSI na starosti síťová vrstva.

Úkoly síťové vrstvy:

1, Nejdůležitějším úkolem síťové vrstvy je tedy tzv. **směrování (routing)**, které představuje právě ono zmíněné rozhodování o směru odesílání jednotlivých paketů. Není jistě třeba zdůrazňovat, že k tomu síťová vrstva potřebuje alespoň základní informace o topologii celé sítě.

2, S tím dosti úzce souvisí i další úkol síťové vrstvy - předcházet přetížení či dokonce zahlcení částí sítě, řídit tok dat a dbát o co možná nejrovnoměrnější využití všech přenosových prostředků a kapacit.

3, Při vzájemném propojení dvou či více sítí pak přibývá síťové vrstvě ještě jeden důležitý úkol - zajišťovat nezbytné předávání paketů mezi jednotlivými sítěmi.

56. Co je to záplavové směrování, kde se používá, jaké má výhody a nevýhody?

Extrémní formou směrování je tzv. **záplavové směrování (flooding)**. Předpokládá, že přijatý paket je znovu odeslán všemi směry kromě toho, odkud sám přišel.

Zřejmou výhodou je maximální robustnost, díky které se záplavové směrování dokáže vyrovnat prakticky s jakýmkoli výpadkem. Zaručuje také, že každý paket je vždy doručen tou nejkratší možnou cestou. Nevýhodou je ale vznik velkého množství duplicitních paketů, které výrazně zvyšují zátěž existujících přenosových cest, a které je třeba následně rušit.

V praxi se proto používá spíše tzv. **selektivní záplavové směrování (selective flooding)**, při kterém není každý paket znovu vyslán všemi směry, ale pouze těmi, které jsou alespoň přibližně orientovány ke konečnému příjemci paketu.

57. Co je to směrování podle vektoru vzdáleností? Který směrovací protokol tuto metodu podporuje?

DVA – používá Bellman-Fordův Algoritmus. Je to směrování nejkratší cestou v počtu skoků k cíli. Maximální délka je 15, 16 je již bráno jako nekonečná vzdálenost. Používá to protokol RIP.

Vektor vzdáleností pro uzel X: minimální vzdálenost z uzlu X do všech ostatních uzlů

Každý uzel provádí následující 3 operace souběžně:

- 1,** Posílá vektor vzdáleností svým sousedům
- 2,** Přijímá vektor vzdáleností od svých sousedů
- 3,** Počítá nové vzdálenosti na základě přijatých vektorů

Problém „čítání do nekonečna“:

- 1, Omezení horní meze pro čítání (maximální vzdálenost)**
- 2, Split horizon (rozštěpený obzor):**

X nesmí poslat do uzlu Y svou vzdálenost k uzlu Z, je-li uzel Y ve směru z X do Z.

3, Split horizon with poisoned reverse (rozštěpený obzor s otráveným zpětným směrem):

X posílá do uzlu Y jeho vzdálenost k uzlu Z je ∞ , je-li uzel Y ve směru z X do Z.

Bohužel, žádné z těchto řešení nezabrání cyklům

Možné řešení: Před generováním a posíláním vektoru vzdáleností, který upravuje konektivitu k jinému uzlu, počkat nějakou dobu na informace o konektivitě k tomuto uzlu od jiných uzlů

Může významně prodloužit dobu konvergence.

Urychlení konvergence: triggered update (okamžité spuštění opravy)

58. Co je to směrování podle stavu linek? Který směrovací protokol tuto metodu podporuje?

LSA, používá se v **OSPF**, prostě to vytvoří graf sítě a lokálně to Dijkstrem spočte nejkratší cestu. Nezátěžuje síť oproti **DVA**, ale zase vyžaduje větší výpočetní výkon

Link State Algorithm (LSA) – směrování podle stavu linek

- Každý uzel ví jak dosáhnout přímo spojené sousedy: lokální link-state (stav linek)
- Přerušené linky nebo nefungující sousední směrovače jsou detekovány periodickou výměnou „hellou“ zpráv
- Každý směrovač šíří vlastní stav linek do všech ostatních uzlů sítě pomocí spolehlivého záplavového doručování
- Znalost stavu linek ze všech uzlů je dostatečná pro konstrukci grafu propojení celé sítě
- Každý uzel vypočte minimální vzdálenost k ostatním uzlům pomocí Dijkstrova algoritmu

Každý uzel generuje periodicky nebo při změně stavu lokální linky **Link State** pakety (**LSP**)

Uzel, který **LSP** přijme, pošle jej všem svým sousedům, kromě toho, od kterého ji obdržel

Sekvenční číslo **LSP** musí být větší, než posledně uloženého **LSP** od tohoto uzlu

- Před posláním **LSP** sousedům snižuje hodnotu TTL
- Jestliže TTL **LSP** dosáhlo nuly, posílá je uzel dál s tím, že je to signál pro vyřazení tohoto **LSP** ze všech uzlů
- Pomocí TTL se měří stáří lokálně uložených **LSP**
- Co se stane, když sekvenční číslo **LSP** dosáhne maxima?
- Co se stane když se uzel rychle vypne a zase zapne bez toho, že sousedé detekují výpadek?
- Uzel si může od souseda vyžádat poslední uložené **LSP**

Výhody a nevýhody:

- + Rychlé ustálení po změně topologie
- + Více robustní než RIP
- + Předchází problému čítání do nekonečna
- Vyžaduje ukládání **LPS** v každém uzlu (týká se rozšiřitelnosti)
- OSPF se proto používá pouze pro interní směrování (omezení z důvodu škálovatelnosti – rozšiřitelnosti)

59. Co je to skupinové směrování a čím se liší od směrování podle individuální adresy?

Přeposílání IP datagramů z jednoho zdroje skupině více koncových stanic.

Odešle se jeden datagram, ale přijde každému cíli.

60. Co je to Dijkstrův algoritmus a jak funguje?

Nalezení nejkratší cesty v grafu. Při každém průchodu cyklu se do množiny navštívených uzlů přidá právě 1 uzel. Průchodů cyklem je tolik, kolik má graf vrcholů.

Algoritmus:

Celý algoritmus se dá shrnout do tří kroků (ohodnocení cesty do vrcholu X budeme značit $|X|$):

- nalezení vrcholu s minimálním dočasným ohodnocením (nazvěme ho V)
- prohlášení vrcholu V za trvalý
- změna ohodnocení sousedů tak, že $|S| = \min(|S|, |V| + \text{ohodnocení hrany z V do S})$, kde S je soused V.

<http://www.kiv.zcu.cz/~konopik/sem/cech/index.html>

(Příklad)

61. Co je to Bellman-Fordův algoritmus a jak funguje?

V případě grafů se záporně ohodnocenými hranami není Dijkstrův algoritmus použitelný. Proto nasazujeme Bellman-Fordův algoritmus, který také jako v Dijkstrovu algoritmu využívá metodu relaxace hran, která zjišťuje aktuálně nastavenou hodnotu nejkratší vzdálenosti od uzlu S. Jestliže je zjištěno

, že hodnota v uzlu je vyšší než hodnota z nynějšího uzlu plus ohodnocení hrany z nynějšího uzlu do uzlu, v kterém bychom chtěli změnit jeho hodnotu, tak tuto hodnotu změníme, respektive snížíme. Hlavní rozdíl oproti Dijkstrovu algoritmu spočívá v průchodu grafu. Jelikož Dijkstrův algoritmus jestliže projdeme všechny následníky jednoho uzlu tak tento uzel "uzavře" a poté ho už neupravuje. Toto se v Bellman-Fordovu algoritmu neděje jelikož on tyto uzly neuzavírá takto ihned ale projíždí několikrát všechny uzly a upravuje postupně hodnoty vzdáleností nejkratších cest.

62. Popište funkci protokolu RIP. Kde se používá, jaké má výhody a nevýhody. Uveďte algoritmy, které byly vyvinuté aby kompenzovaly nevýhody protokolu.

Je typu **distance vector** – uzly si vyměňují aktualizace tvořené směrovým vektorem a jeho ohodnocením.

Všechny ohodnocení linek jsou nastaveny na 1 (počet mezilehlých uzlů).

Princip fungování:

Aktualizace se posílají každých 30 sekund. Pokud do 180 sekund nepřijde update od konkrétního(sousedního) routeru, jsou všechny cesty přes ně považovány jako nekonečné. Po dalších 120 sekundách jsou odstraněny z tabulky.

Výpočet cest je distribuovaný, každý počítá kousek, takže chyba jednoho ovlivní ostatní.

Aktualizace se posílají jen přímým sousedům(routerům), takže router nevidí dál, než ke svým sousedům, nezná celou topologii.

Neudržuje alternativní cesty, cesty se stejným ohodnocením ignoruje.

Zatěžuje hodně síť, ale nezatěžuje moc CPU.

Algoritmus opravy směrovací tabulky:

Pokud je nově vypočtená vzdálenost

1, Menší – opravit

2, Stejná – nic neměnit

3, Horší:

Na základě zprávy ze směrovače, který je sousední pro původní směrování – opravit (**zhoršení ocenění**)

Na základě zprávy z jiného směrovače – **nic neměnit**

63. Popište funkci protokolu OSPF. Kde se používá, jaké má výhody a nevýhody. Uveďte topologii sítě, typy směrovačů a jakou mají funkci.

Je typu link-state, každý uzel testuje dostupnost svých sousedů, každý uzek sestavuje link-state paker, ve kterém jsou údaje o dostupnosti sousedů(stav linky a ohodnocení).

Tyto pakety jsou rozesílány všem uzlům v síti, ale jne při nějaké změně, jinak každých 30 minut. Všechny uzly tedy mají úplnou informaci o jednotlivých spojích a mohou si vypočítat optimální cesty → chyby ovlivní jen sama sebe.

OSPF podporuje alternativní cesty, různé cesty pro různé druhy provozu. Také dovoluje rozdělit síť na menší oblasti, kdy topologie není šířena mimo tuto oblast.

Směrovače v oblastech se rozdělí takto:

- interní – zajišťují směrování v rámci oblasti
- páteřní – zajišťují směrování v páteřní oblasti
- na rozhraní – patří do oblasti o do páteře, vyměňují info mezi nimi
- hraniční – vyměňují informace s jinými oblastmi

Směrovač monitoruje dostupnost sousedů hello paketem každých 10 sekund, pokud do 40 sekund soused neodpoví, zruší se sousedství, když do 30 minut není změna, opakuje vše.

Určení vah cest:

- Nejjednodušší (často používané)

Všechny linky mají stejnou cenu – směrování s minimálním ohodnocením

- Cena linky – převrácená hodnota kapacity

10Mb linka má 100 krát vyšší cenu než 1Gb linka

- Cena linky – zpoždění linky

250ms satelitní spojení má 10 krát větší cenu než 25ms pozemní linka

- Cena linky – využití linky

Linka s 90% využitím má 10 krát vyšší cenu než linka s 9% využitím, způsobuje oscilace.

64. Co jsou to protokoly externího směrování a kde se používají?

Používají se pro směrování mezi sítěmi, jsou to protokoly pro směrování mezi autonomními oblastmi.

- BGP udržuje směrovací tabulky, šíří opravy směrování a rozhodnutí o směrování zakládá na směrovací metrice
- Vyměňuje informaci o dosažitelnosti sítě (reachability)
- Vytváří graf propojitelnosti AS (AS connectivity)
- Odstraňuje směrovací smyčky a prosazuje rozhodnutí o strategii
- BGP používá jednu metriku k určení nejlepší cesty

Linková metrika je hodnota preference přiřazená administrátorem

Je to multikriteriální funkce: počet procházených AS, strategie směrování, stability, rychlosti, zpoždění, ceny, ...

- Vybírá nejlepší cestu a instaluje IP forwardovací tabulku

Path Vector protocol:

- Podobný Distance Vector Protocol
- Každý BGP směrovač posílá pomocí broadcastu sousedům celou cestu (posloupnost AS) do cíle

Dá seručně nastavit, kudy to má jít, aby síť obsluhovala jen své zákazníky a ne všechny jenom proto, že má nejvyšší rychlost; „aby to ten s dobrým připojením neodsral“.

65. Co je to zahlcení v sítích, čím vzniká a jak se mu bráníme.

Přepojovací uzel nestačí přepojovat přenášená data v reálném čase → hromadí se ve frontě → zvyšuje se čas obrátky → překročí se kapacita front → nové bloky jsou zahazovány → mechanismy potvrzování snaží se zajistit spolehlivost posílají data znova → zvýšení provozu v síti → zhoršuje ještě více stav → zahlcení sítě

Ošetření: uzly mají možnost upozornit na hrozící nebezpečí; „disciplína“ odesílatelů; AIMD - pomalu posílám a čekám co se stane → pomalu tím zvyšuju rychlost → jakmile zjistím ztrátu tak spadnu dolů - v nejhorším případě na 0 a zase pokračuju

66. Co je to tunelování a kde se používá. Uveďte příklady.

Používá se pro zapouzdření jednoho, či více síťových spojení do jiného. Například budu komunikovat pomocí Ipv6, ale půjde to přes síť, který umí jen IPv4, takže Ipv6 pakety obalím IPv4 a pošlu je.

Jiným běžným využitím je tunelování přes [SSH](#) spojení - pokud jím protunelujete jiné síťové spojení, zaručíte, že internetem budou data procházet zašifrovaně, i když protokol tunelovaného spojení šifrování nepodporuje.

67. Co je to mobilní IP a jak funguje.

Mobilní IP adresa umožňuje stanicím s IP adresou ze sítě o daném rozsahu IP adres být připojeny a komunikovat v sítích o jiném rozsahu IP adres.

Technologie Mobile IP udržuje stejnou IP adresu mobilního zařízení a podporuje jeho komunikaci, zatímco se přemísťuje z jedné sítě do druhé. IP zařízení komunikuje v síti, i když jeho trvalá IP adresa může být odlišná od adresy sítě.

68. Popište formát IPv4 adresy. Co jsou to podsítě a proč se zavádí?

délka adresy – 32 bitů;

5 tříd – A 0

B 10

C 110

D 1110

E 1111

Adresa rozdělena na 4 úseky po 8 bitech. Např. u A –první úsek značí síť, zbytek určuje PC v síti → státní organizace; běžný uživatel má C; E - speciální

Podsítě - nejdřív začali s třídami (A,B,C,D). Třeba u A bylo první číslo síť a ostatní čísla stanice atd. Začaly ale nedostačovat adresy, tak se přešlo na CIDR. Tam může být třeba IP/21, kde zleva překreješ IP adresu 21 jedničkama a zbytek IP adresy je pro stanice.

69. Co je to maska sítě a implicitní adresa směrovače?

Maska sítě:

Rozděluje adresu na část síťovou a část pro hostitelský systém

Např. 255.255.255.0

147.228.67.0 * 255.255.255.0 dává stejný výsledek pro všechny adresy začínající 147.228.67

Důvodem rozdělení na dvě části je minimalizace počtu položek ve směrovačích (jedna položka zahrnuje více adres počítačů)

CIDR (ClassLess InterDomain Routing)

Umožňuje použít pro adresování v podsíti takový počet bitů, který není na hranici 8.

Adresa se udává ve tvaru adresa/počet bitů síťové části

Implicitní směrování (Default Routing) se používá tehdy, když je zdrojová síť připojená na IP intersíť přes jediný směrovač, takže přes něj musí procházet všechny pakety nepřímého směrování. V tomto případě není potřeba směrovačí tabulka a stačí znalost IP adresy **implicitního směrovače**.

70. Jak se v lokální (mnohobodové) síti převede síťová adresa na fyzickou adresu počítače?

Pomocí ARP; pošle se ARP paket se zdrojovou síťovou i fyz. adr. a cílovou síťovou => cíl odpoví doplněním své fyzické adresy. Když je cíl mimo LAN, tak by směrovač doplnil svou fyz., protože to stejně půjde přes něj.

71. K čemu slouží protokol ICMP? Znáte programy, které jej využívají? Znáte princip?

Protokol IP, který je hlavním přenosovým protokolem na úrovni síťové vrstvy, funguje tzv. nespolehlivě - když zjistí, že se něco při přenosu poškodilo, nepovažuje za svou povinnost postarat se o nápravu (ale počítá s tím, že o ev. nápravu se postará někdo jiný, a to vyšší vrstvy). Protokol IP tedy má právo zahodit taková data, u kterých zjistí, že jsou nějakým způsobem poškozena (samozřejmě je nezahazuje bezdůvodně). I když nemá povinnost postarat se o nápravu, přesto se snaží alespoň informovat o tom, že se něco špatného stalo. Právě k tomuto účelu pak využívá další z "doprovodných" protokolů, protokol ICMP. Ten je jakýmsi "poslem špatných zpráv" - sám nenapravuje žádné chyby či závady nebo jiné nestandardní situace, ale pouze přenáší zprávy o tom, že něco je v nepořádku.

ICMP se posílá v IPpaketu, IPpaket - hlavička, IPpaketdata a v ní ICMP paket

Využívá ho **PING**.

72. Co je to Network Address Translation (nebo Network Address and Port Translation)? Kde se používá a jaké má výhody a nevýhody?

[Způsob úpravy síťového provozu přes router přepisem výchozí nebo cílové IP adresy. Adresy](#)

lokální síť se přeloží na jedinečnou adresu, která slouží pro vstup do jiné sítě (www...), překládanou adresu uloží do tabulky pod náhodným portem, při odpovědi vyhledá port a pošle pakety na přiřazenou IP. Používá se v Internetu.

Výhody – připojení více PC na jedné veřejné IP; vyšší bezpečnost

Nevýhody – ztráta rychlosti připojení

73. Kde se používá a jak funguje protokol ARP?

Mechanismus dynamického budování a udržování převodních tabulek mezi IP a fyzickou adresou.

Využívá broadcast → vyšle info o tom, koho hledá → hledaný mu odpoví infem o sobě.

V sítích Ethernet.

74. Vysvětlete postup doručení paketu v síti internet mezi dvěma počítači, připojenými do lokálních počítačových sítí různého typu, propojených internetem (směrovači).

Pakety odeslány na server (poskytovatele připojení), server určí ideální trasu → Každý paket může putovat internetem zcela jinou trasou, a proto je jeho součástí informace o adrese odesílatele a příjemce, dále údaje označující bezchybnost data a pořadové číslo paketu, díky němuž se dá ve finále původní soubor znovu poskládat do výchozí podoby, protože jednotlivé pakety jsou doručovány v různém pořadí. → cíl odpoví a celý proces běží od cíle ke mě

75. K čemu slouží protokol BOOTP? Jak funguje?

Přiděluje stanicím parametry jako IP adresa, maska sítě, brána...-> tyto informace jsou na BOOTP serveru.

Startující stanice vyšle dotaz „kdo jsem?“ broadcastem, BOOTP server najde v tabulce podle MAC adresy příslušné údaje a odpoví

Protokol BOOTP slouží právě tomuto účelu, a vychází vstříc dokonce i bezdiskovým stanicím, kterým umožňuje tzv. počáteční zavedení jejich operačního systému (tzv. bootstrap, odsud také jeho název) - protokol BOOTP poskytne startující (tzv. bootující) stanici přesný odkaz na místo, odkud si může vyzvednout svůj operační systém a vše, co potřebuje ke svému startu (tzv. boot image).

76. K čemu slouží protokol DHCP? Jak funguje?

Dovoluje dynamické přidělování parametrů (IP, maska sítě, brány...); parametry jsou vztaženy k segmentu počítačové sítě;

přidělování IP – statické - máme ji doopravdy zaregistrovanou; dynamické - napořád nebo na dobu určitou (pronájem)

Protokol DHCP (stejně jako BOOTP) přitom vychází z architektury klient/server a počítá s existencí konfiguračního serveru (DHCP serveru), který poskytuje potřebné konfigurační informace uzlům, které vůči němu vystupují jako jeho klienti. Jednou z jeho odlišností oproti protokolu BOOTP je například to, že dokáže "propůjčovat" svým klientům IP adresy pouze dočasně, jen na dobu jejich skutečné potřeby, a pak je zase odebírat a využívat jinak.

77. Co je to protokol IPv6, jaké má základní vlastnosti, kde se používá? Jak se liší od Ipv4?

- je síťová vrstva pro mezisíťový přenos paketů
- 128bitů dlouhé adresy => spooooooooousty adres
- bezstavová autokonfigurace adres
- lepší podpora multicastu
- adresy místní linky
- lépe řeší fragmentaci a defragmentaci
- jumbogramy – pakety větší než 64KiB, velikost až 4GB
- rozdíly: velikost paketu, počet možných adres...

- anycast – jedna IP adresa přidělená více uzlům současně

78. Vysvětlete princip DVA, jakým způsobem se konstruuje směrovací tabulky, co je to čítání do nekonečna a jaké algoritmy se používají pro urychlení konvergence.
Viz. 57

79. Vysvětlete, jak fungují jmenné servery, proč je systém doménových jmen decentralizovaný a jak se převádí jméno počítače na adresu a naopak. Účastní se také jmenné servery doručování elektronické pošty? Pokud ano, pak jak.

Jmenné servery (DNS) – převádí jméno (www.pepa.cz) na IP adresu (123.123.12.45)

Domény:

Je potřeba zajistit, aby se nesesli stejné adresy (pepa.cz).

Zavádí se hierarchie, kdy v rámci cz domény smí být

pepa.cz jenom 1x (v rámci com domény opět 1x apod).

pepa se následně dále může dělit na subdomény, ale každá opět pouze 1x (honza.pepa.cz; franta.pepa.cz)

Použití pro el. poštu – určuje kam a jakým zp. má být doručena pošta; *pet@dcit.cz* → na tento server chodí pošta pro adresata pet, ten ji ovšem chce přijímat na *pet@frode.dcit.cz* → není vhodné mít ovšem takovou adresu, např. pokud by se změnila subdoména frode, byla by pošta v klu → proto se posílá na globalní doménu dcit.cz → DNS má info o tom, že pro uživatele pet se má pošta přijímat na frode. Pokud se změní frode za xy, pouze se prepíše DNS záznam, ale jinak vše jede pořád stejně.

80. Vysvětlete, jak se podílí ARP na komunikaci mezi dvěma vzdálenými počítači, připojenými do Internetu prostřednictvím rozhraní Ethernet.

ARP – zabezpečuje přiřazení IP adresy fyzickým adresám linkové vrstvy → vlastní komunikace v síti pomocí fyzických adres;

2 funkce – získání MAC adres; udržování tabulek přiřazených MAC adres k IP adresám

Když IP protokol získá z vyšší vrstvy adresu → prohledá tabulku → nenajde-li cílovou adresu → vyšle požadavek → odpoví mu vlastník IP adresy → aktualizace tabulky

81. Co víte o náhodných metodách sdílení komunikačního kanálu?

Aloha – stanice nezjistuje, jestli se něco přenáší, či ne, prostě začne vysílat. Pokud nedostane potvrzení, pošle zprávu znovu. Dá se aplikovat pouze do 20% zatížení sítě.

Taktovaná Aloha – zahájit vysílání lze pouze v pevně stanovených časových okamžicích.

CSMA – viz. předchozí otázka.

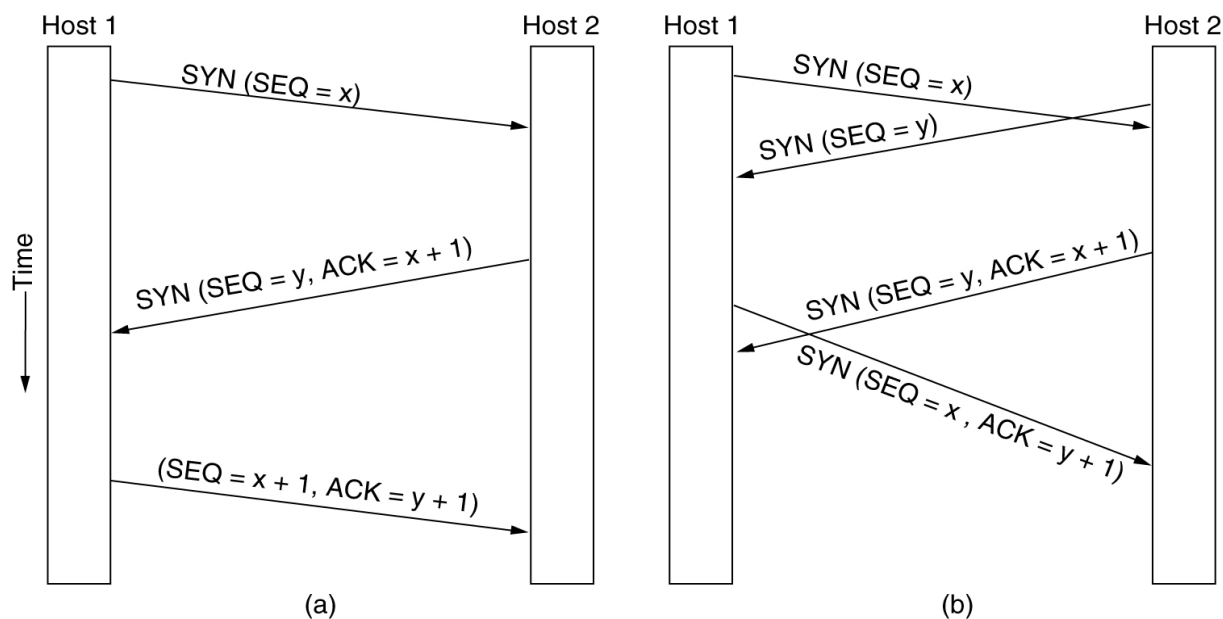
82. Co víte o standardech 802.11 (WiFi) a 802.15 (Bluetooth)?

IEEE 802.11 – WiFi, 802.11b a 802.11g pásmo 2,4GHz, 802.11a pásmo 5GHz

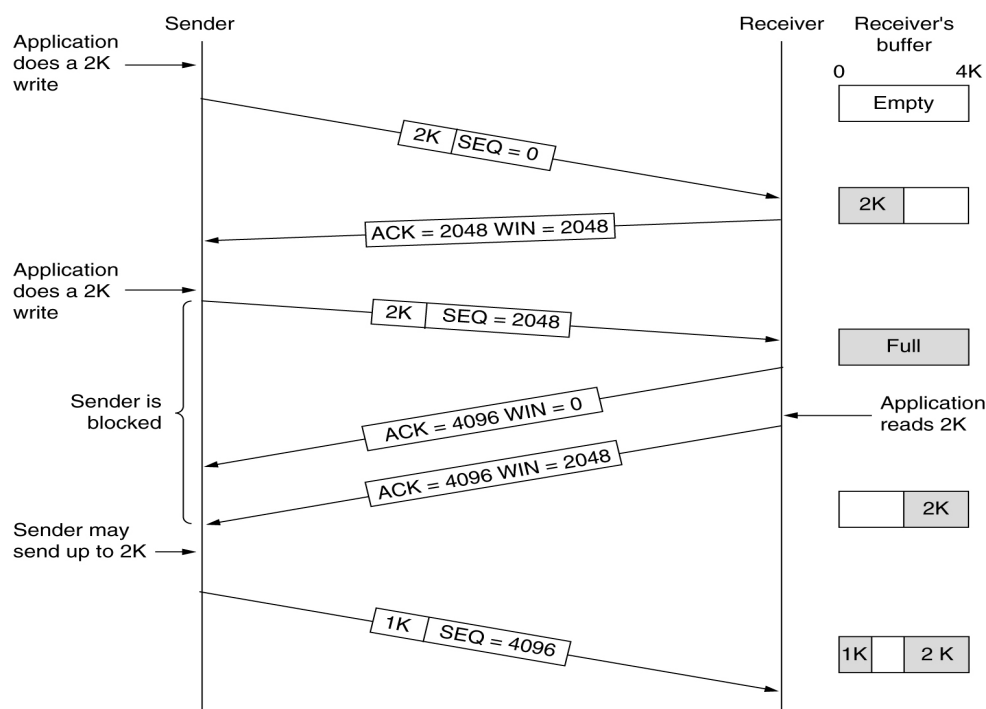
IEEE 802.11 – Bluetooth, bezdrátová síť pro propojení například mobilů, pda atd. Max. Dosah 100 metrů (teoretický), rychlost 2Mbit/s, v pásmu 2,4GHz

83. Popište, jak se navazuje spojení, ruší spojení a přenáší data v protokolu TCP.

Vytváření spojení:



Přenos dat:



84. Co je to BOOTP protokol, k čemu slouží, jaký je rozdíl mezi BOOTP (bootstrap protokol) a DHCP (Dynamic Host Configuration Protocol). Viz. Předchozí otázky.

85. Jakou funkci má relační úroveň.

Smyslem vrstvy je organizovat a synchronizovat dialog mezi spolupracujícími relačními vrstvami obou systémů a řídit výměnu dat mezi nimi. Umožňuje vytvoření a ukončení relačního spojení, synchronizaci a obnovení spojení, oznamování výjimečných stavů. Do této vrstvy se řadí: NetBIOS, AppleTalk, RPC, SSL. K paketům přiřazuje synchronizační značky které využije v případě vrácení paket (např. z důvodu, že se během přenosu dat poškodí síť) k poskládání původního pořadí.

1. Spočítat CRC pro: zpráva "0" a zpráva "1", polynom x^4+x+1 . Uvést obecné vzorce.

CRC

zpráva / polynom

$R(x) = M(x) / G(x)$ x^4+x+1

$T(x) = M(x) + R(x)$ ZSTEK

$T(x) / G(x) \Rightarrow 0$ JE TO DOBRĚ
1 CHYBA

ODESLANÁ ZPRÁVA

"0" $T(x) = 0 / 0000$

"1" $T(x) = 1 / 0011$

00000 }
10011 } 3

$\frac{N-1}{2}$ DETEKUJE
 $\frac{N}{2}$ OPRAVUJE

2. Zařízení DTE a DCE, jak propojí dvě zařízení DTE. Null modem.

DTE / DCE

DTE: POČ. KONCOVÉ ZAŘÍZENÍ DATOVÉHO OKRUHU

DCE: MODEM UKONČOVACÍ ZAŘÍZENÍ DATOVÉHO OKRUHU

KOMUNIKAČNÍ SÍŤ

MODEM - MODULÁTOR/DEMODULÁTOR
- UPRAVUJE ČÍSLICOVÝ SIGNÁL DO PODOBY SHODNÉ PRO PŘENOS KOMUNIKAČNÍ SÍTÍ

NULL MODEM - PROPOJOVACÍ KABEL

PŘÍPOJENÍ DTE/DCE
SIGNÁLY: VYSÍLANÁ DATA - TxD
PŘÍJMANÁ DATA - RxD
DSR
DTR
CTS

PROPOJENÍ DVOU PC

P_1 P_2

TxD RxD DSR CTS

3. Co je to OPAKOVAČ, HUB, MOST, SMĚROVAČ, BRÁNÁ.

OPAKOVAČ - Opakovač je obousměrný číslicový zesilovač. Používáme jej pouze jako prostředek pro zvětšení vzdálenosti, již jsme schopni lokální sítě obsáhnout. Nejedná se tedy v pravém smyslu slova o propojení dvou různých lokálních sítí, ale o tvorbu jedné větší lokální sítě z menších částí. Další možnou funkcí opakovače je propojení dvou částí lokální sítě, pracujících s různými kabely.

HUB - je aktivní prvek počítačové sítě, který umožňuje její větvení. Chová se jako opakovač. To znamená, že veškerá data, která přijdou na jeden z portů (zásuvek), zkopíruje na všechny ostatní porty, bez ohledu na to, kterému portu (počítači a IP adrese) data náleží. To má za následek, že všechny počítače v síti „vidí“ všechna síťová data a u větších sítí to znamená zbytečné přetěžování těch segmentů, kterým data ve skutečnosti nejsou určena.

MOST – spojuje dvě části sítě na druhé (linkové) vrstvě referenčního modelu ISO/OSI. Most je pro protokoly vyšších vrstev transparentní (neviditelný), odděluje provoz různých segmentů sítě a tím zmenšuje i zatížení sítě. Most odděluje provoz dvou segmentů sítě tak, že si ve své paměti RAM sám sestaví tabulku MAC (fyzických) adres a portů, za kterými se dané adresy nacházejí. Leží-li příjemce ve stejném segmentu jako odesílatel, most rámce do jiných částí sítě neodešle. V opačném případě je odešle do příslušného segmentu v nezměněném stavu.

PŘEPÍNAČ - je aktivní síťový prvek, propojující jednotlivé prvky sítě. Switch obsahuje větší či menší množství portů (až několik stovek), na něž se připojují síťová zařízení nebo části sítě. Na rozdíl od HUBu neposílá přijatá data na všechny porty, ale pouze na ty, kterým data patří.

SMĚROVAČ - je v počítačových sítích aktivní síťové zařízení, které procesem zvaným routování přeposílá datagramy směrem k jejich cíli. Routování probíhá na třetí vrstvě referenčního modelu ISO/OSI (síťová vrstva). Netechnicky řečeno, router spojuje dvě sítě a přenáší mezi nimi data. Router se podstatně liší od switche (přepínače), který spojuje počítače v místní síti. Rozdílné funkce routerů a switchů si lze představit jako switche coby silnice spojující všechna města ve státě a routery coby hraniční přechody spojující různé země.

BRÁNÁ - je obvykle kombinací softwaru a hardwaru, který propojuje dvě různé sítě pracující pod různými protokoly. Brány pracují zpravidla na síťové vrstvě nebo ještě výše. Některé brány kromě vlastního přenosu dat z jedné sítě do jiné zabezpečují současně s přenosem také převod do jiného protokolu; takovými branám se říká aplikační brány. Někdy se pojem brána používá i v situacích, kdy se neprovádí žádný převod mezi protokoly, ale kdy se data pouze přenesou z jedné sítě do jiné. Takovouto bránu tvoří software a hardware, který propojuje dvě různé sítě.

4. Vysvětlit syndrom hloupého okénka

Při výměně segmentů nestejné velikosti může dojít k syndromu hloupého okna způsobeného odesílatelem, či příjemcem. V případě odesílatele tento problém nastává tehdy, když posílá malé segmenty dat, i když je možno počkat a následně odeslat větší objem dat v jednom segmentu. U příjemce syndrom hloupého okna nastává v případech, když v potvrzovacích segmentech ohlašuje malé velikosti svého dostupného okna, i když by bylo možno počkat a ohlásit větší velikost. Samotné zpoždění doručování potvrzování a Naglův algoritmus tomuto problému přímo nezabrání, ale specifikace protokolu TCP obsahuje posloupnost kroků, jak řešit odesílání dat a potvrzení tak, aby problému s „hloupým oknem“ nedocházelo. Zasílání krátkých segmentů dat vede k velmi neefektivnímu využití přenosového pásma, kde se navíc velká část spotřebuje pouze na režii samotného protokolu.

5. Co jsou sítě Personal Space Communication IEEE 802.15.8 Napojení na 3G síť.

Hlavní vlastnosti:

čisté řešení, není třeba kombinované řešení
dynamické školování velkého rozsahu (100Kb/s až 50Mb/s, dosah do 30m)
rychlá synchronizace a připojování (rychlé vyhledávání sousedů a odpojování)
asymetrické připojení

PSC aplikace:

přizpůsobení pro smartphone (lokalizační služby, načítání dat přístupových bodů, ...)
bezdrátová interakce se všemi zařízeními v osobním prostoru (zvuk/video, Voip, web camera, ...)
zajišťuje pomalou i rychlou komunikaci (ovládání a řízení + prohlížení videa

6. Co je to reverse path forwarding? Nakreslit strom.

REVERSE PATH FORWARDING (RPF)

- POSÍLÁM POLE ZPĚTNÉ CESTY

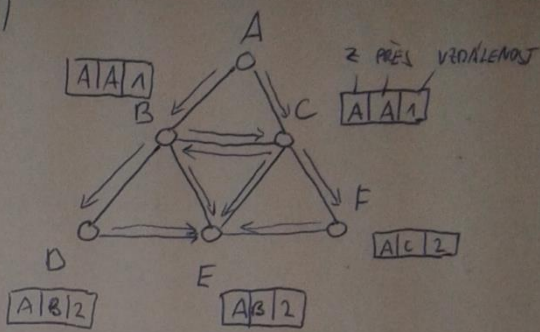
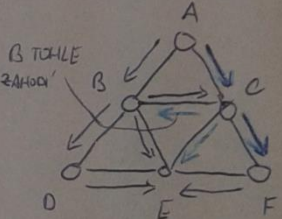
HUSTÁ SÍŤ

- ZPRÁVU POSÍLÁM VŠEM
- SMĚROVACÍ ODMÍTAVÍ PŘENOS
- ZAPLAVOVÉ SMĚROVÁNÍ
⇒ DOSTRANĚNÍ SMYČEK

RPF

- ZAPLAVOVÉ - POSÍLÁM VŠEM (DO VŠECH SMĚRŮ), KROM TOHO, ODKUD JSEM PŘIŠEL

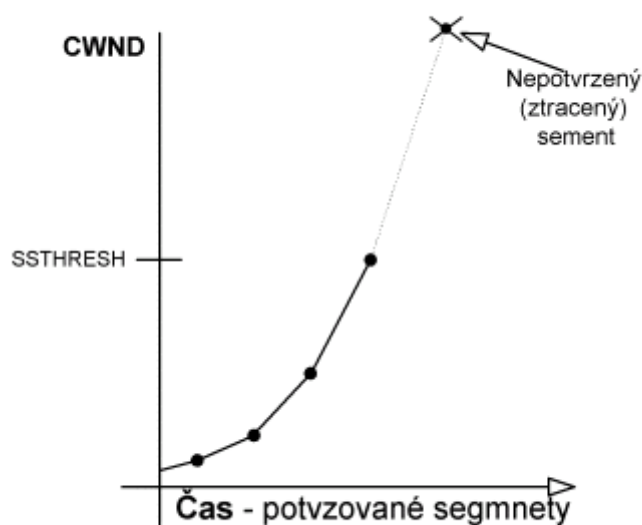
- TECHNIKA SKUP. VYSÍLÁNÍ, PŘI KTERÉ JE DATAGRAM SMĚROVÁN NA VŠECHNA VÝSTUPNÍ ROZHRANÍ MIMO ROZHRANÍ, KTERÝM BÝL PŘIJAT JE POUŽITO K VYSÍLÁNÍ UNICAST DATAGRAMU PRO ZDROJ SMĚROVÉHO VYSÍLÁNÍ

7. Pomalý start

- při zřizování nového TCP spojení možnost skokového nárůstu zátěže, zahlcení sítě a zneprůchodnění všech (i již navázaných) spojení.
- principem je přizpůsobení rychlosti vysílání segmentů do sítě rychlosti přicházejících ACK
- používá se jen pro spojení mimo LAN

Vysílač upravuje šířku vysílacího okna (CWND, "Congestion Window"), ta se udržuje v bajtech. Také udržuje hodnotu SSTHRESH, což je hodnota velikosti CWND, od které již začíná hrozit zahlcení. Cílem je udržovat CWND blízko nad hodnotou SSTHRESH, kde však ještě nedochází k zahlcení.



8. Protokol HTTP, GET, POST, COOKIES

Protokol HTTP

URL

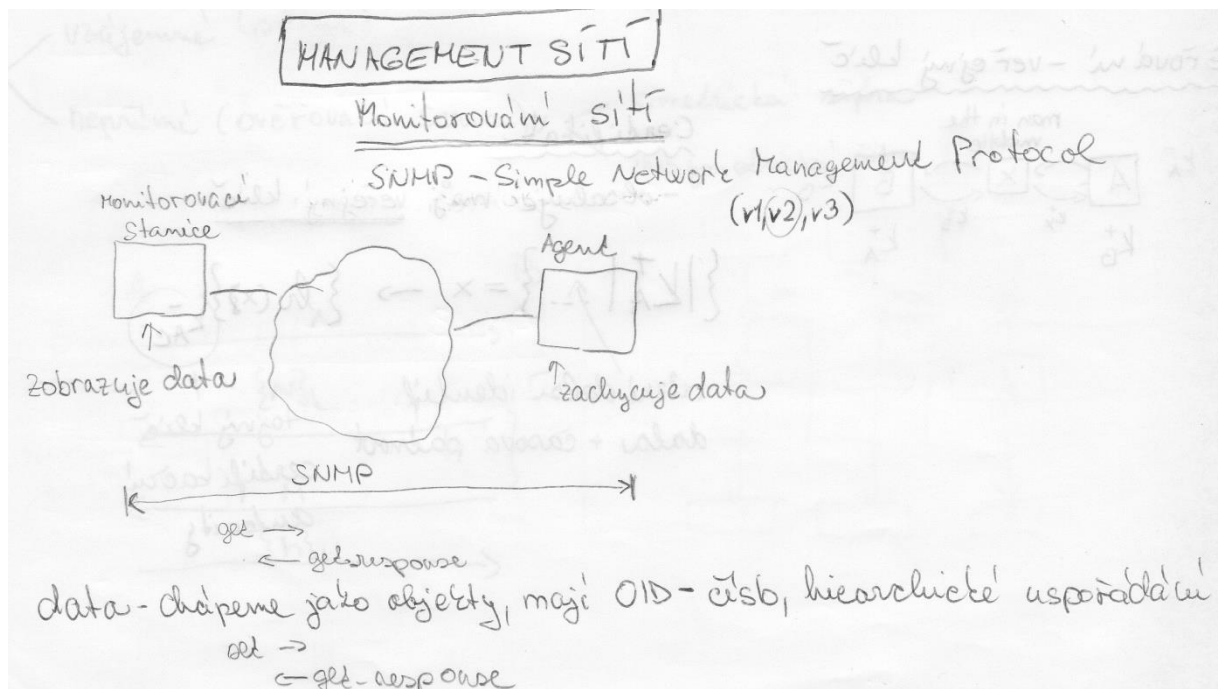
$\langle \text{schema} \rangle : // \langle \text{jmeno} \rangle : \langle \text{heslo} \rangle @ \langle \text{stroj} \rangle : \langle \text{port} \rangle // \langle \text{cesta_k_souboru} \rangle ? \langle \text{parametry} \rangle$

- PŘI POUŽITÍ GET SE VEŠKERÁ FORM. DATA PŘEDAJÍ JAKO SOUČÁST URL ZA OTAZNÍKEM
- PŘI POUŽITÍ POST SE PŘEDAJÍ V TĚLE DOTAZU, TAKŽE V URL NEJSOU VIDĚT
- POKUD SE PŘEDANÁ DATA MAJÍ CHÁPAT JAKO PARAMETRY STRÁNKY (PŘ. ID ČLÁNKU) POUŽIJU GET JINAK POST

COOKIES - JSOU MALÉ TEXTOVÉ SOUBORY VYTVAŘENÉ WEB. SERVEREM A UKLÁDANÉ VE VAŠEM PC PROSTŘEDNICTVÍM PROHLÍŽEČE. KOTŘ SE POŘEDÍ VRÁTÍTE NA STEJNOU STRÁNKU, PROHLÍŽEČ PŘEČ ULOŽENOU COOKIE ZPĚT A SERVER ZÍSKÁ VŠECHNY INFO, KTERÉ SI U VÁS PŘEDTÍM ULOŽIL, TAKTO COOKIES UMOŽŇUJÍ OZNAČIT JEDNOTLIVÉ UŽIVATELE.

9. Co je to SNMP? Jaký je rozdíl mezi jednoduchými objekty a sloupci tabulky

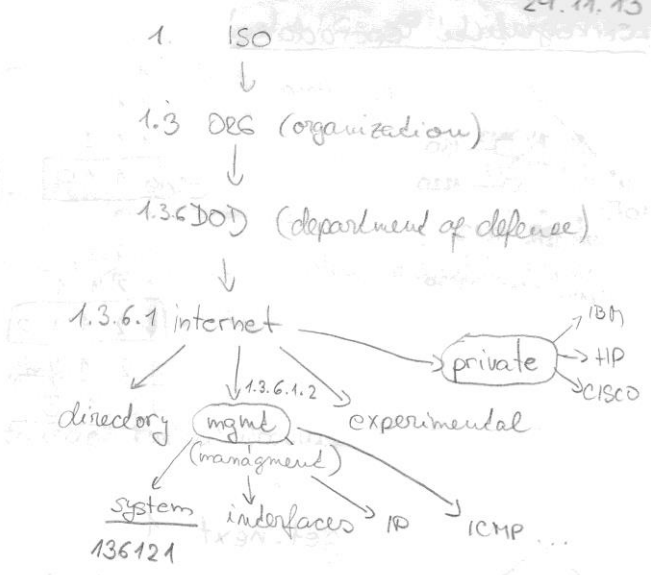
Je součástí sady internetových protokolů. Slouží potřebám správy sítí. Umožňuje průběžný sběr nejrůznějších dat pro potřeby správy sítí, a jejich následné vyhodnocování. Na tomto protokolu je dnes založena většina prostředků a nástrojů pro správu sítí. Má tři verze: druhá obsahuje navíc autentizaci a třetí šifrování. Nejvíce zařízení podporuje druhou verzi.



ISO } strom identifikatori
CCITT/ITU }
- pro management slouží ISO

Protokol

get - čtení hodnoty
set - zápis hodnoty
get_response - odpověď
get_next
trep - asynchroni zpráva



PE.

get 136.1.2.1.1.0, (jmeno systému)
get_response 13.6.1.2.1.1.0 | router u401
OID hodnota

identifikator objektu - instance OID
OID OID.0

Práce s tabulkami

ARP tabulka

fyzická adr.	síťová adr.	interface
CD:AB:CD:01:02:03	147.228.67.1	1

SQL: select ... where <MENO>='JAN'

SNMP: OID.index1.index2... OID.147.228.67.1.1

Práce s protokolem SNMP

- monit. stanice periodicky čte specifikované proměnné

- zpracování asynchronické zprávy (trap)

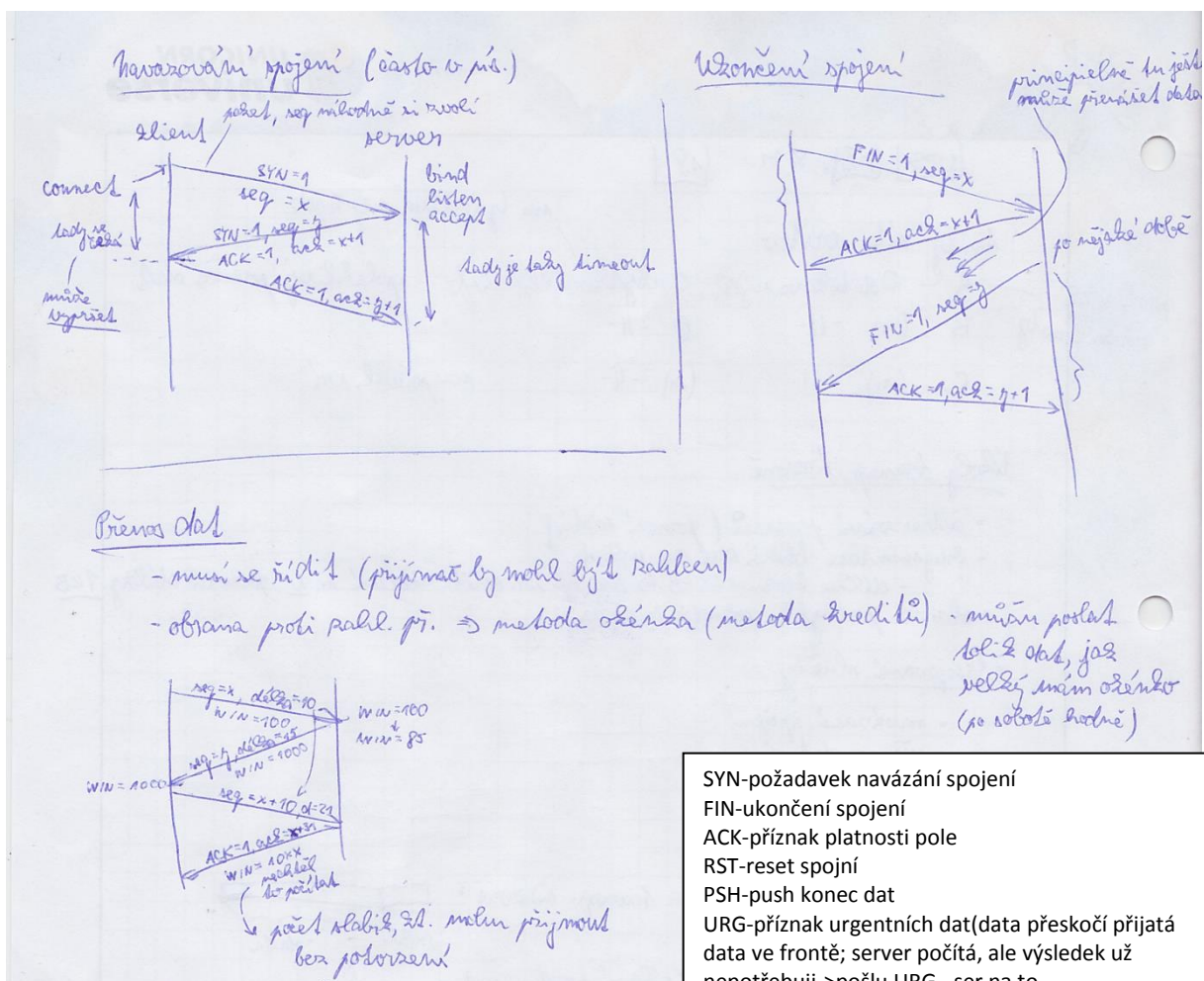
Lageus zjistí - studený start

- teplý start

- nahrazení / složení rozhraní, ...

} sám pošle monit.
stanici zprávu

10. TCP navázání spojení, ukončení spojení, přenos dat, nakreslit komunikace. Co jsou to urgentní data, kde se používají a jak se přenáší? Jak se řeší v TCP data přicházející z klávesnice a myši.



Nejdřív pošleš jednu klávesu, s nějakým bitem, který zajistí, aby tam nebyla taková režie a než ti dojde potvrzení o doručení, tak se naplní buffer se zbývajícími klávesy a ty se pak pošlou v jedné zprávě.

Obrana proti záhlcení

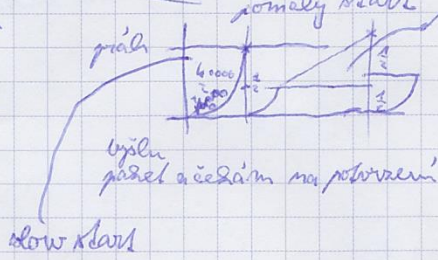
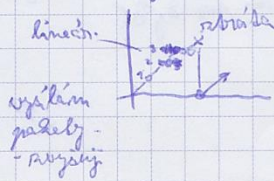
explicitní - přenáší se příznaky o záhlcení sítě

(zařadí směrovací má fronty a jistěže dojde k záhl. - požadavky fronty záhl.

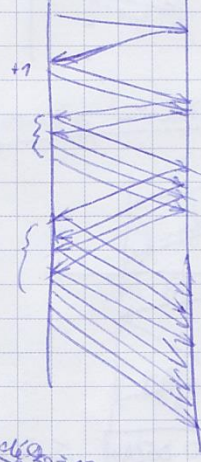
implicitní metody - provádí se testováním přichodnosti sítě

- detekce záhlcení = ztráta paketů

Metody řešení záhlcení sítě



contention avoidance (přetěžování sítě)



detekce záhlcení sítě

timeout

retransmission

T.O. preložen ACK

duplicitní potvrzení

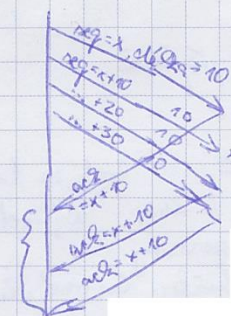
z obou stran toho odnesli:

→ běží po z úrovních

→ řízení mezi z úrovních

→ řízení možností dat přenášených

konverzí (záhlcení)



11. Chceme poslat zprávu prostřednictvím symetrického šifrování a ověřit nepopíratelnost zprávy. Popište, jak bude vypadat komunikace s využitím symetrického, asymetrického šifrování a kryptografického kontrolního součtu (hash funkce). Určete jaký klíč, je jaký. man-in-the-middle, certifikát

9.

22.11.

Šifrování a bezpečnost

Simon Singh: Kniha kóde a šifer

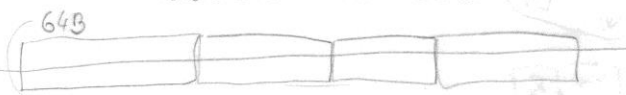
Šifra

/ symetrická / bloková
/ asymetrická / proudová

Šifrování = převod otevřeného textu na šifrovaný text s použitím funkce a klíče

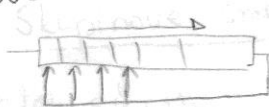
- funkce je veřejně známá
- klíč je utajovaný

Symetrické blokové šifrování

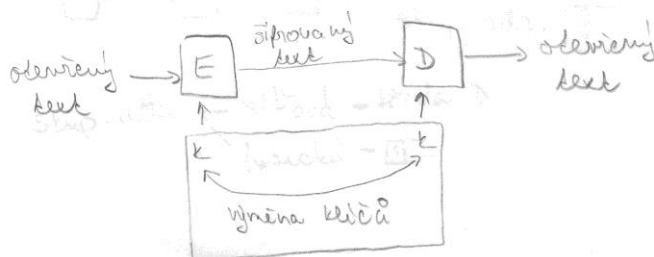


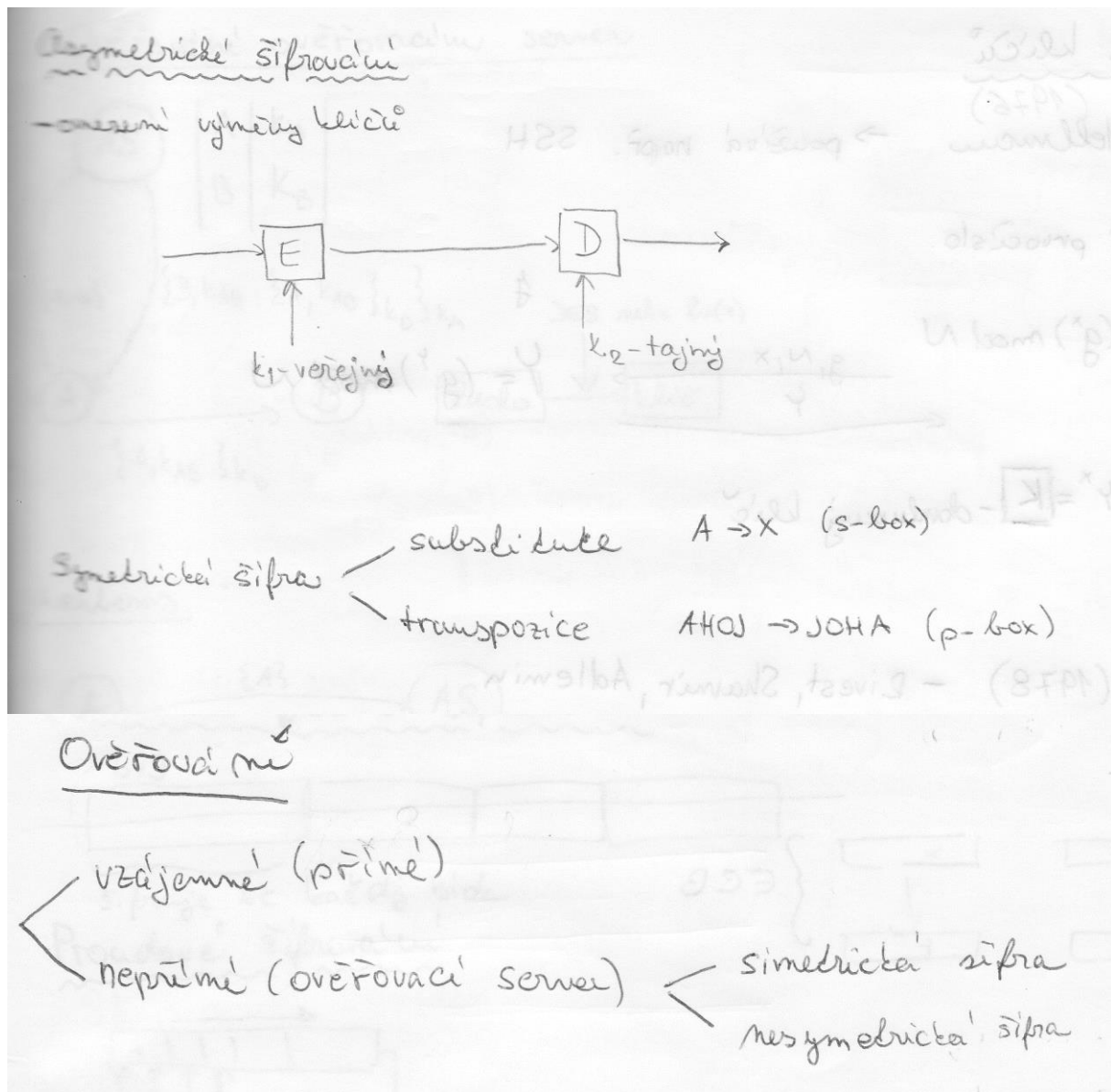
šifruje se každý blok

Proudové šifrování



Symetrické šifrování



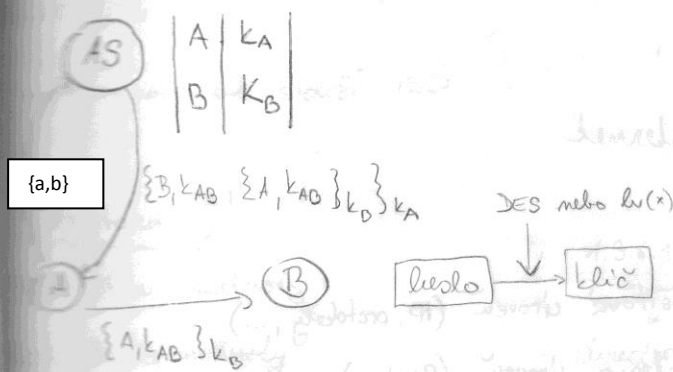


Kryptografická hašovací funkce je v kryptografii hašovací funkce s takovými vlastnostmi, které umožňují její použití v aplikacích zabezpečení informací, jako například autentizace nebo zaručení integrity zprávy. Kryptografická hašovací funkce je používána pro ochranu proti úmyslnému poškození dat a v dalších kryptografických aplikacích.

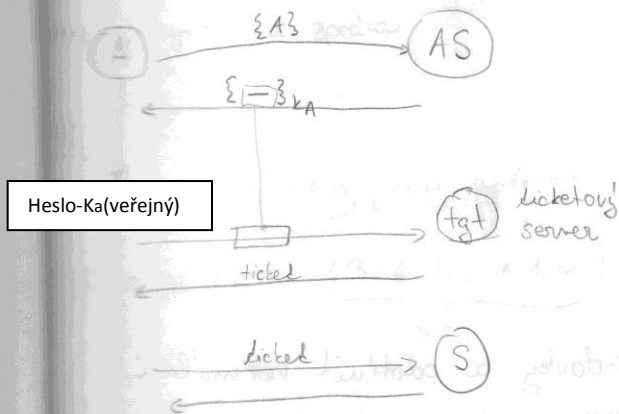
Známé hashovací funkce: SHA-1 a SHA-2

Certifikát je datová struktura (řetězec bitů) pomocí které se zveřejňují údaje o uživateli a zejména uživatelův veřejný šifrovací klíč (v případě RSA šifer). Certifikát je elektronicky podepsán (ověřen) certifikační autoritou. Z certifikátu je možné získat veřejný šifrovací klíč uživatele, který je možné použít k prokazování totožnosti uživatele. V případě, že certifikát obsahuje šifrovací klíč určený také k šifrování dat, pak je možné i tento klíč z certifikátu použít k šifrování dat odesílaných uživateli. Certifikát se často přirovnává k občanskému průkazu.

Overovani overovacni server

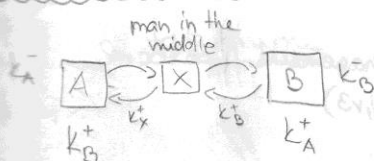


Overovani



Heslo-Ka(verejný)

Overovani - verejny klíč



Certifikát

- obsahuje můj veřejný klíč

$$\{K_A^+\}_{K_{AC}^-} = x \rightarrow \{hv(x)\}_{K_{AC}^-}$$

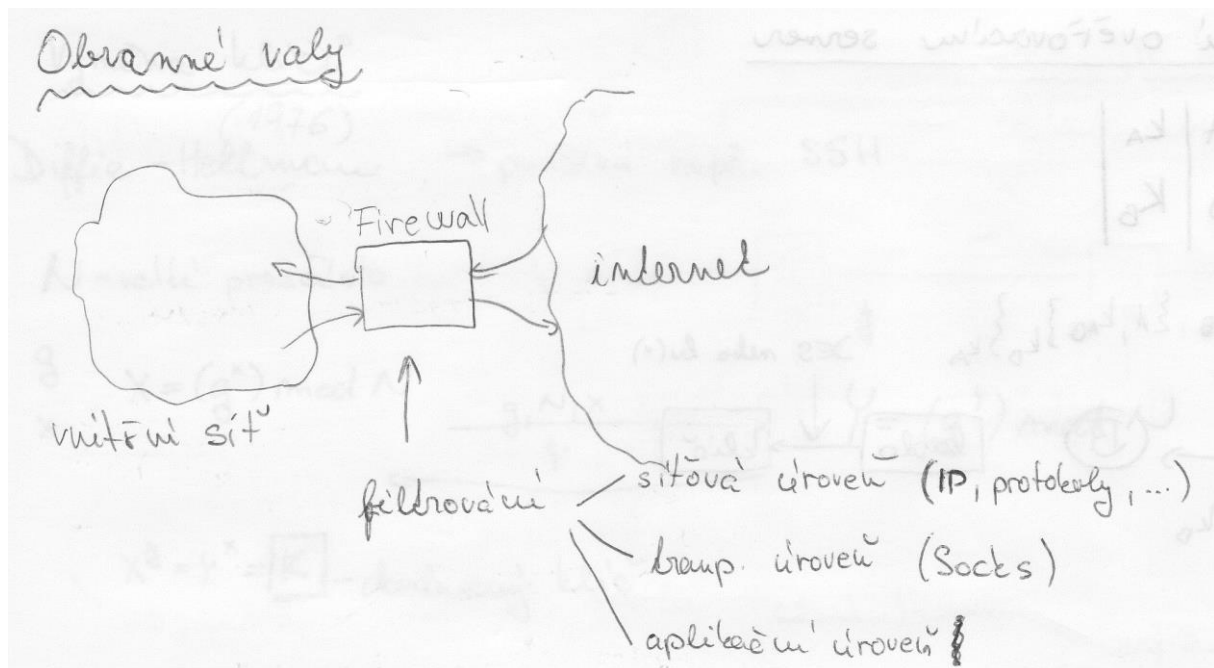
ruční dalsi identifik.

dalsi + časová podmínka

točný klíč

certifikační

autorita



12. Nakreslete TCP/IP zásobník a zařaďte protokoly a ve stručnosti je popište.

1. TCP/IP zásobník

Aplikační vrstva

- DNS, BOOTP, DHCP, FTP, Telnet, SMTP, SSH

Transportní vrstva

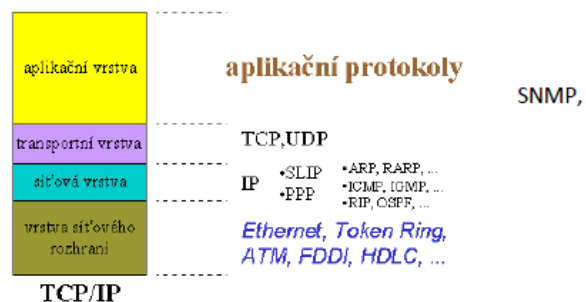
- TCP, UDP

Síťová vrstva

- IP, ARP, ICMP, IGMP

Přenosová vrstva

- Ethernet, HDLC



DHCP (Dynamic Host Configuration Protocol) – obdoba BOOTP, modernější, nepoužívá statické konfigurace (při každém připojení do sítě může uzel obdržet jinou adresu), umožňuje dynamickou změnu nastavení uzlu

BOOTP (Bootstrap Protocol) – pracuje nad UDP, slouží k získání IP adresy a dalších parametrů potřebných pro zapojení uzlu do sítě; získání síťového nastavení pro provoz uzlu

Telnet (Telecommunication Network) - pomocí stejnojmenné aplikace umožňuje uživateli připojení ke vzdálenému počítači, spojení typu klient-server protokolem TCP (duplexní spojení)

Ethernet – metoda náhodného přístupu, sběrníková nebo hvězdicová topologie, rozlehlost stovky metrů až několik km, nejrozšířenější lokální síť, distribuovaná a neřízená metoda přístupu

FTP (File Transport Protocol) – přenos souborů, přístup ke vzdálenému serveru

DNS (Domain Name System) – převod jména na adresu a opačně, poskytuje i další informace

UDP (User Datagram Protocol) – nespojované služby, nepotvrzované

TCP (Transport Control Protocol) – spojované služby, potvrzované, obnova po chybě

ICMP (Internet Control Message Protocol) – přenos zpráv o chybách, test dosažitelnosti vzdáleného uzlu, přenos parametrů, synchronizace času

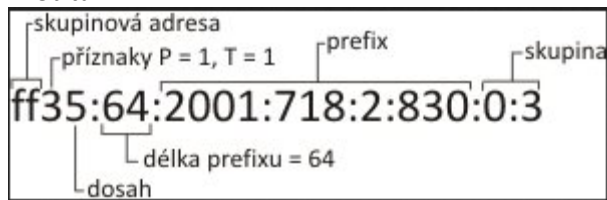
IGMP (Internet Group Management Protocol) – je protokol, který rozšiřuje požadavky na implementaci protokolu IP (IPv4) o podporu IP multicastu. Využívá se pro dynamické přihlašování a odhlašování ze skupiny u multicastového routeru ve své lokální síti. IGMP protokol řeší i situaci, kdy jsou v síti připojeny dva a více multicastových routerů, protože pak by mohlo dojít v síti k šíření nadbytečných informací.

ARP (Address Resolution protocol) – převod síťové adresy na fyzickou

IP (Internet Protocol) – nespojovaný protokol, nepotvrzované služby, přenáší pakety a směřuje je podle cílové adresy

13. IPv6 - jak vypadá záhlaví IPv6

128bitů



Základní záhlaví IPv6 protokolu

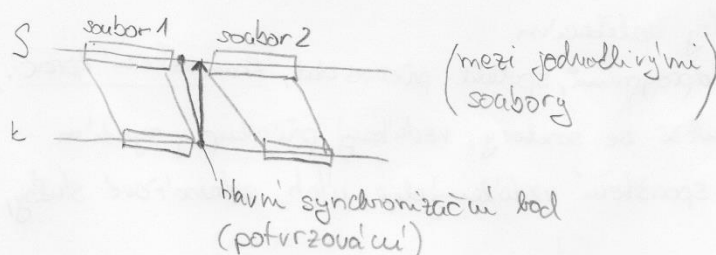
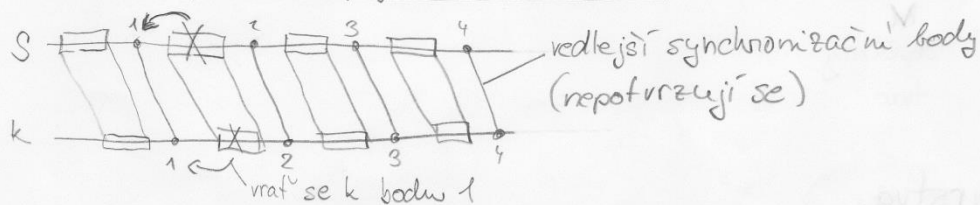


14. Relační úroveň, hlavní a vedlejší synchronizační body.

Relační vrstva

- řeš se problém: co s výpadkem transportního spojení?
- \exists transportní spojení
- \exists relační spojení
- vztahy 1:1 (T:R) - např. přenos 1 HTML stránky v rámci HTTP protokolu
- 1:N (T:R) - navázání 1 transp. spojení a realizaci více relací
- N:1 (T:R) - stahování souborů (dojde-li k výpadku \Rightarrow může stahování obnovit)

Obnova transp. ~~relace~~ spojení během relace



15. FTP - aktivni/pasivni

Přenos souborů

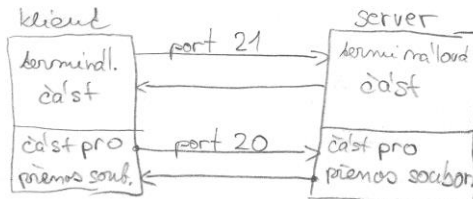
- FTP (File Transfer Protocol)

- Spolehlivý, TCP

- vyžaduje přihlášení

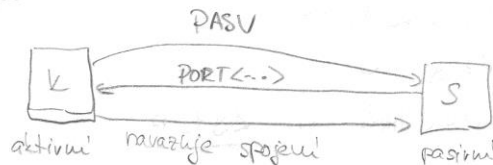
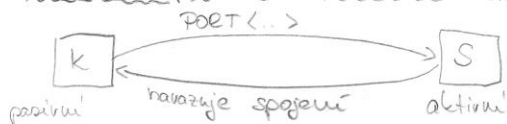
- sestává ze dvou částí

terminálový provoz
vlastní přenos souborů (GET, PUT)



oslaďdání klienta: ! před přibaz

Aktivní a pasivní navazání spojení



Anonymní uživatelé

- ftp, anonymous - heslo: e-mailová adresa

Bezpečnost

- řeší scp (secure copy) naváže šifrované spojení
přeneší data

- SSH protokol

- navazování spojení



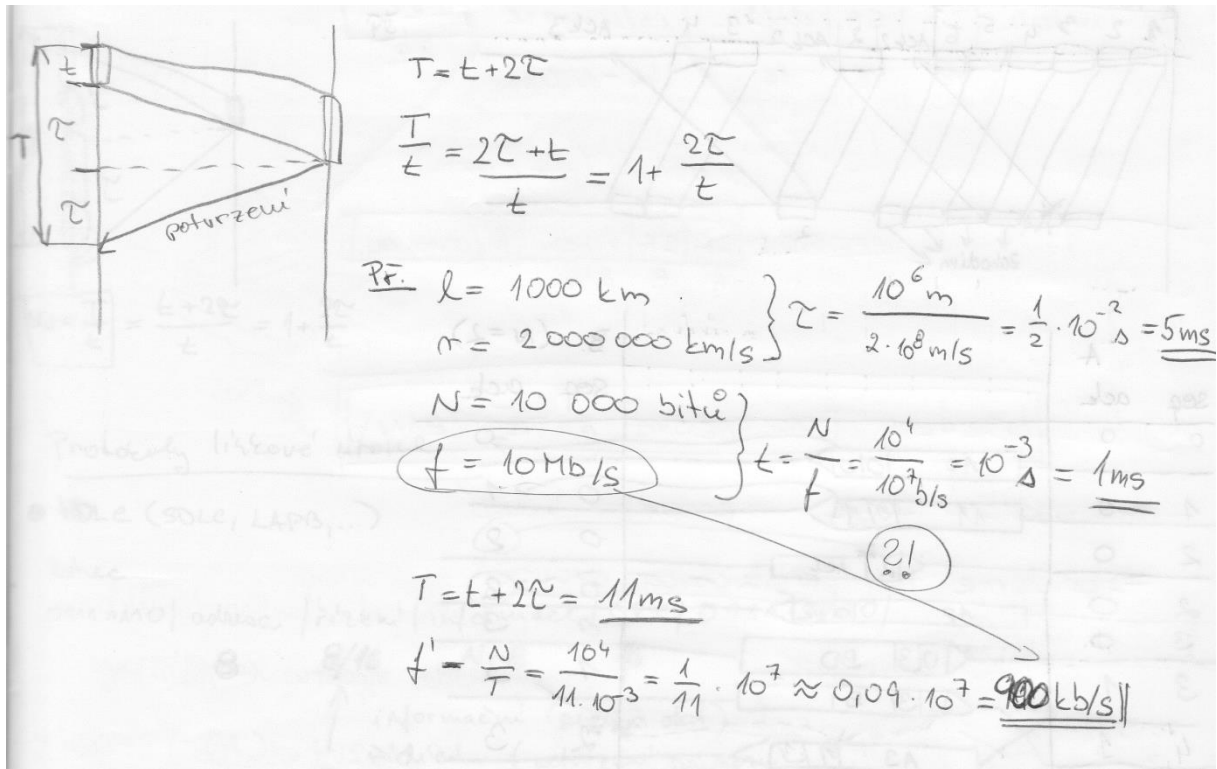
Diffie-Hellman schéma

$$\begin{aligned}
 &g \quad \quad \quad g - \text{tajemství} \\
 &N - \text{velikost prvocísla} \quad \leftarrow Y = (g^x) \bmod N \\
 &x - \text{tajemství} \\
 &X = g^x \bmod N \quad \rightarrow \\
 &\quad \quad \quad X, g, N
 \end{aligned}$$

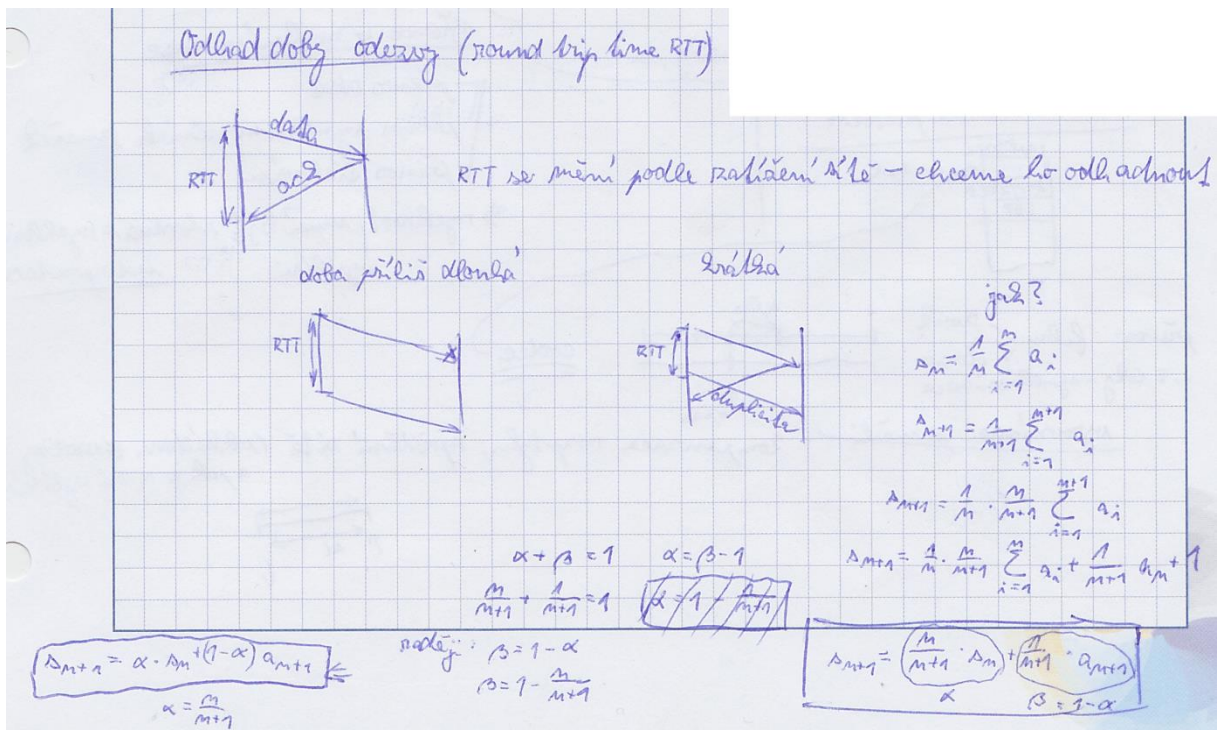
$$(X^Y) \bmod N = (Y^X) \bmod N = K$$

Klíč používaný pro komunikaci

16. Určit průměrnou přenosovou rychlost u Stop and Wait. Doba vysílání je 1ms, délka zprávy 10000 bitů a doba odezvy je 5ms. Nakreslit obrázek vysílání.



17. Jak se zjišťuje (odhaduje) doba odezvy RTT při přenosu TCP.

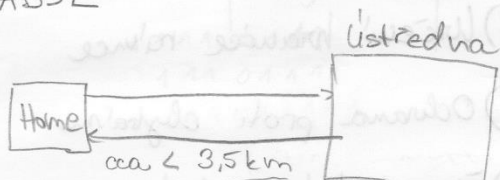


18. Co je ADSL, co je to splitter, díky čemu ADSL dosahuje vysokých rychlostí.

- AD převodník

ISDN - 2 kanály (64 kb/s) - volání + internet
1 kanál (16 kb/s)

ADSL

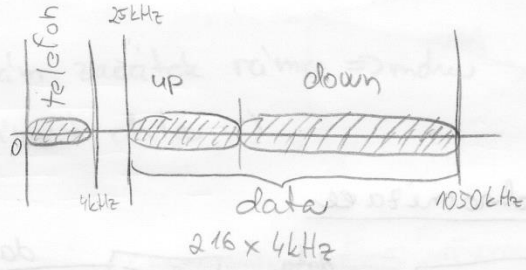


0 - 4 kHz

telefon

25 kHz - 1050 kHz

data



Kabelové síť

- kabelové televize

- telefon

- kabelový modem

downlink

! uplink - sdílení

Splitter

