Následujících 13 vypracovaných multi-otázek jsou stoprocentně z testů. Zbytek je na učení.

1. Určete napětí v ustáleném stavu (po odeznění odrazů) na vstupu koaxiálního vedení s charakteristickou impedancí $Z_0 = 50\ \Omega$ a délkou $l = 50\ m$ po připojení k výstupu napěťového zdroje s napětím naprázdno $U_0 = 9\ V$ a vnitřním odporem $R_i = 100\ \Omega$ v případě, že konec vedení je:
a) zatížen ohmickou zátěží (rezistorem) o odporu $50\ \Omega$.
b) otevřený (rozpojené vedení).
c) zkratovaný (na zem).
Vedení považujte za bezeztrátové.

Zde pozor: $R_0 = R_i = 100\ \Omega$.

a) $U_\infty = U_0 \cdot \frac{R}{R_0 + R} = 9 \cdot \frac{50}{100 + 50} = 3\ V$

b) $U_\infty = U_0 \cdot \lim_{R\to\infty} \frac{R}{R_0 + R} = 9 \cdot \lim_{R\to\infty} \frac{R}{100 + R} = 9 \cdot \lim_{R\to\infty} \frac{1}{\frac{100}{R} + 1} = 9\ V$

c) $U_\infty = U_0 \cdot \lim_{R\to 0} \frac{R}{R_0 + R} = 9 \cdot \lim_{R\to 0} \frac{R}{100 + R} = 0\ V$

Vypočítejte napětí na konci koaxiálního vedení s impedancí $Z_0 = 75\ \Omega$, délkou $l = 100\ m$ a zpožděním signálu 5 ns/m v čase $\tau = 0{,}8 \cdot 10^{-6}\ s$, je-li ke vstupu v čase $t_0 = 0\ s$ připojen stejnosměrný zdroj napětí $U_0 = 10\ V$ s vnitřní impedancí $R_0 = 75\ \Omega$, a to pro následující případy:
a) konec vedení je zakončen terminátorem s impedancí $75\ \Omega$
b) konec vedení je otevřený (nezakončený)
c) konec vedení je zkratovaný
Vedení považujte za bezeztrátové.

a) $U_a = U_0 \cdot \frac{Z}{R_0 + Z} = 10 \cdot \frac{75}{75 + 75} = 5\ V$

Zpoždění je $5\ \text{ns} / m \cdot 100\ m = 0{,}5\ \mu s$, což je menší než $0{,}8\ \mu s$, což znamená, že signál již jednou na konec došel, a tak budeme přičítat jednou U_{r_1}.

$U_{r_1} = U_a \cdot \rho_b = U_a \frac{R - Z}{R + Z} = 5 \cdot 0 = 0\ V$

$U = U_a + U_{r_1} = 5 + 0 = 5\ V$

b) $U_a = U_0 \cdot \frac{Z}{R_0 + Z} = 10 \cdot \frac{75}{75 + 75} = 5\ V$

$U_{r_1} = U_a \cdot \rho_b = U_a \lim_{R\to\infty} \frac{R - Z}{R + Z} = 5 \cdot \lim_{R\to\infty} \frac{R - 75}{R + 75} = 5 \cdot \lim_{R\to\infty} \left(1 - \frac{150}{R + 75}\right) = 5 \cdot 1 = 5\ V$

$U = U_a + U_{r_1} = 5 + 5 = 10\ V$

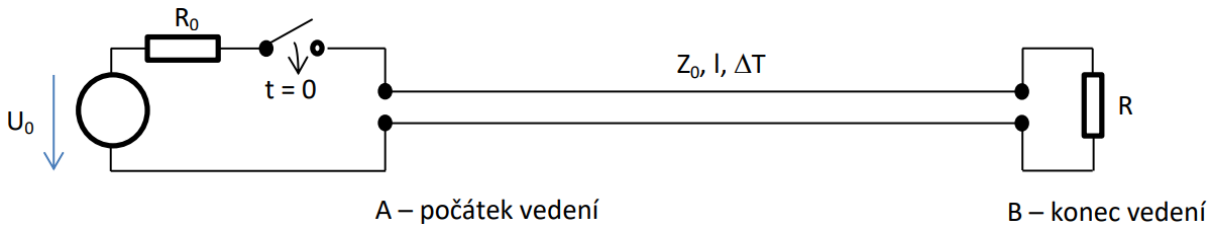
c) $U_a = U_0 \cdot \frac{Z}{R_0 + Z} = 10 \cdot \frac{75}{75+75} = 5\ V$

$U_{r_1} = U_a \cdot \rho_b = U_a \frac{R-Z}{R+Z} = 5 \cdot \frac{0-75}{0+75} = -5\ V$

$U = U_a + U_{r_1} = 5 - 5 = 0\ V$

V čase $t = 0\ s$ byl na vstup bezeztrátového vedení délky $l = 100\ m$ s charakteristickou impedancí $Z = 50\ \Omega$ a dobou šíření $\Delta T = 0,5\ \mu s$ připojen stejnosměrný zdroj napětí o velikosti $U_0 = 10\ V$ s vnitřním odporem $R_0 = 150\ \Omega$. Určete napětí na vstupu vedení v čase $t_U = 1,1\ \mu s$, je-li vedení na svém konci:

a) otevřené (rozpojené)
b) zkratované
c) zakončené zátěží $R = 50\ \Omega$
d) zakončené zátěží $R = 250\ \Omega$.



Za $1,1\ \mu s$ se signál stihne dostat na konec, zpátky, a ještě jednou se odrazit.

$$\rho_a = \frac{R_0 - Z}{R_0 + Z} = \frac{150-50}{150+50} = 0,5$$

$$U_a = U_0 \cdot \frac{Z}{R_0 + Z} = 10 \cdot \frac{50}{150+50} = 2,5\ V$$

a)

$$\rho_b = \lim_{R\to\infty} \frac{R-Z}{R+Z} = \lim_{R\to\infty} \frac{R-50}{R+50} = \lim_{R\to\infty} \frac{1-\frac{50}{R}}{1+\frac{50}{R}} = 1$$

$$U_{r_1} = U_a \cdot \rho_b = 2,5 \cdot 1 = 2,5\ V$$

$$U_{r_2} = U_{r_1} \cdot \rho_a = 2,5 \cdot 0,5 = 1,25\ V$$

$$U_{IN} = U_a + U_{r_1} + U_{r_2} = 2,5 + 2,5 + 1,25 = 6,25\ V$$

V čase $t_U = 1,1\ \mu s$ bude při $R = \infty\ \Omega$ napětí na počátku vedení napětí $6,25\ V$.

b)

$$\rho_b = \lim_{R\to 0}\frac{R-Z}{R+Z} = \lim_{R\to 0}\frac{R-50}{R+50} = \lim_{R\to 0}\left(1-\frac{100}{R+50}\right) = 1-2 = -1$$

$$U_{r_1} = U_a \cdot \rho_b = 2,5\cdot(-1) = -2,5\ V$$

$$U_{r_2} = U_{r_1} \cdot \rho_a = -2,5\cdot 0,5 = -1,25\ V$$

$$U_{IN} = U_a + U_{r_1} + U_{r_2} = 2,5-2,5-1,25 = -1,25\ V$$

V čase $t_U = 1,1\ \mu s$ bude při $R = 0\ \Omega$ napětí na počátku vedení napětí $-1,25\ V$.

c)

$$\rho_b = \frac{R-Z}{R+Z} = \frac{50-50}{50+50} = 0$$

$$U_{r_1} = U_a \cdot \rho_b = 2,5\cdot 0 = 0\ V$$

$$U_{r_2} = U_{r_1} \cdot \rho_a = 0\cdot 0,5 = 0\ V$$

$$U_{IN} = U_a + U_{r_1} + U_{r_2} = 2,5+0+0 = 2,25\ V$$

V čase $t_U = 1,1\ \mu s$ bude při $R = 50\ \Omega$ napětí na počátku vedení napětí $2,25\ V$.

d)

$$\rho_a = \frac{R_0-Z}{R_0+Z} = \frac{250-50}{250+50} = \frac{2}{3}$$

$$U_{r_1} = U_a \cdot \rho_b = 2,5\cdot\frac{2}{3} = \frac{5}{3}\ V$$

$$U_{r_2} = U_{r_1} \cdot \rho_a = \frac{5}{3}\cdot 0,5 = \frac{5}{6}\ V$$

$$U_{IN} = U_a + U_{r_1} + U_{r_2} = 2,5+\frac{5}{3}+\frac{5}{6} = 5\ V$$

V čase $t_U = 1,1\ \mu s$ bude při $R = 250\ \Omega$ napětí na počátku vedení napětí $5\ V$.

2. Definujte pojem Hammingova vzdálenost kódu d. S použitím tohoto pojmu uveďte, kdy kód opravuje t-násobné chyby, a své tvrzení dokažte.

Hammingova vzdálenost kódu d je nejnižší počet znaků, v nichž se liší libovolná dvě kódová slova.

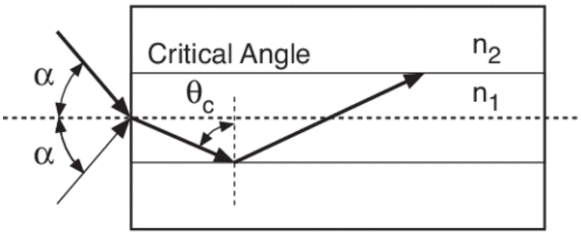
Kód opravuje t-násobné chyby, pokud je Hammingova vzdálenost kódu $d > 2t$.

Ať je vzdálenost d a chyba $t > \frac{d}{2}$. Hammingovy kódy opravují tak, že najdou nejbližší kódové slovo. V tomto případě ale může existovat zpráva s t chybami, které jsou blíž ke špatnému kódovému slovu než ke správnému.

Přesně vysvětlete, co to je a jaký praktický význam má numerická apertura (NA) mnohavidového optického vlákna.

Numerická apertura (vyjádřena sinem úhlu α_{MEZ}) je maximální velikost úhlu, který může svírat paprsek s osou optického vlákna, aby při dopadu na jeho čelní plochu byl navázán do vlákna a pokračoval jím. Při praktickém měření se NA určí z úhlu natočení vláken, kdy je

pokles přeneseného výkonu na 5 % původní hodnoty. Pro numerickou aperturu NA optického vlákna platí vztah $NA = \sqrt{n_1^2 - n_2^2}$, kde n_1 je index lomu jádra a n_2 je index lomu pláště.



Vysvětlete, co je to ICMP protokol.

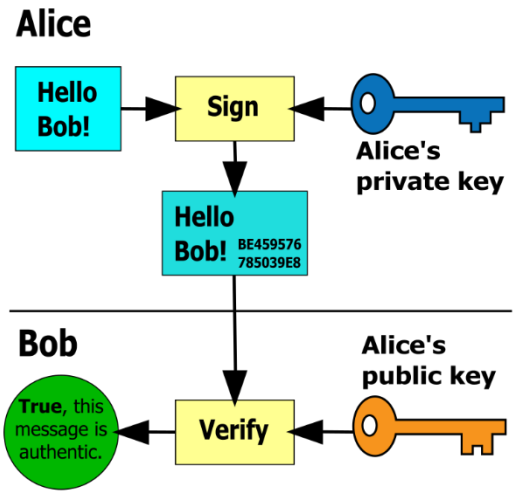
ICMP (Internet Control Message Protocol) slouží k hlášení problémů při zpracování IP paketů směrovači.
Nachází se v datovém poli IP paketu, ale neslouží k zajištění spolehlivosti přenosu. Používá se například při příkazech ping a tracert.

Jaké jsou funkce presentační vrstvy? Uveďte příklady.

Protože příchozí data mohou být v různých formátech z různých zdrojů, jsou presentační vrstvou překládána pro aplikační vrstvu do jednoho standardního formátu.
To zahrnuje šifrování, konvertování a komprimace. Příklad protokolu – SMB.

3. Vysvětlete pojem digitální podpis a popište způsob jeho vytvoření a následného ověření. Jaké základní funkce plní?

Digitální podpis je matematické schéma pro šifrování souborů, které slouží k zajištění integrity, autenticity a nepopíratelnosti (odesílatel nemůže popřít, že je jeho).



Alice přidáním zašifrované verse svým privátním klíčem zprávu „Hello, Bob!“ podepíše.
Bob dostane jak samotnou zprávu, tak podpis. Použije Alicin veřejný klíč k dešifraci zprávy a porovnáním s přijatým podpisem tak potvrdí autenticitu zprávy.

Šifrování je asymetrické, takže se Bob nemůže vydávat za Alici, dokud nebude mít její klíč. Veřejný klíč umí pouze dešifrovat, nikoliv však šifrovat. Nejpoužívanější algoritmus je DSA.

4. Uveďte všechny podstatné hashovací funkce. Kde se tento typ kódování používá?

   CRC-32: zip soubory
   MD5: ukládání hesel uživatele na unixových systémech
   SHA-2: SSL
   Hashovací funkce se používají k ověření správnosti přijatých souborů. Odesílatel odešle soubor spolu s hashem, načež si příjemce spočítá vlastní hash a porovná ho s přijatým – pokud sedí, tak soubor dorazil v pořádku.
   Dalším použitím hashovacích funkcí je v kryptografii.

   Co jsou porty a k čemu slouží? Lze použít současně jeden port pro TCP a UDP komunikaci?

   Port je číslo, které je posíláno spolu s daty a slouží k tomu, aby byla data na konci cesty přesměrována přímo do aplikace, která je bude využívat.
   Ano, lze použít jeden port pro TCP a UDP současně.

5. Uveďte Vámi známé metody pro sdílení kapacity přenosového signálu.

   Stochastické – Aloha, CSMA / CA, CSMA / CD
   Deterministické – master-slave, token-passing, delegated token

   Jaký je vztah mezi CSMA / CD s ethernetem? Co je CSMA / CD a k čemu slouží?

   CSMA (Carrier Sense Multiple Access) je protokol, ve kterém uzel ověřuje nepřítomnost dalšího provozu před vysíláním před vysíláním na sdíleném fysickém médiu (<- fancy slovo pro kabel…).
   Carrier Sense znamená, že vysílač naslouchá nosné vlně a pokud detekuje přítomnost signálu, tak čeká.

   Na rozdíl od čistého CSMA si CSMA / CD (Carrier Sense Multiple Access with Collision Detection) při vysílání kontroluje přenosové médium, zda nezachytí jiné vysílání, které koliduje s jejím. Pokud potencionální kolisi zjistí, zastaví vysílání, počká náhodnou dobu a opakuje pokus znovu. V CSMA a CSMA / CA se naproti tomu kolise nezjišťují a dochází k nim, čímž se zbytečně odvysílá celá datový rámec, který bude beztak nutno opakovat.
   Nejrozšířenějším představitelem je Ethernet.

   Popište princip architektury klient-server.

   Klient-server popisuje vztah mezi dvěma počítačovými programy, v nichž první program - klient, žádá o služby jiný program zvaný server. Na tomto modelu je založen například přístup na e-mail, web a přístup k databázi.

6. Vypočítejte CRC kód pro datové pole rámce 110111000111010011, kde je generující polynom kódu $x^3 + x + 1$. Jaké typy chyb jsou CRC detekovány?

Viz: https://asecuritysite.com/comms/crc_div a https://youtu.be/6gbkoFciryA .
Pozor: $x^3 + x + 1 \equiv 1011$.

Vypočítejte CRC kód pro datové pole rámce 111101101010101101, kde je generující polynom kódu 1011. Kdy CRC odhalí chyby liché násobnosti?

Nechť $G(x)$ je generující polynom $E(x)$ chybový polynom.
Detekovány jsou:

- všechny jednonásobné chyby, pokud má $G(x)$ alespoň dva členy
- všechny dvojnásobné chyby, pokud generující polynom nedělí $(x^m + 1)$ pro všechna $m <$ délka kódového slova a má alespoň dva členy
- všechny chyby liché násobnosti, pokud je $G(x)$ beze zbytku dělitelný $(x+1)$
- všechny shlukové chyby délky $\leq k$, kde k je stupeň $G(x)$, pokud $G(x)$ obsahuje nenulový konstantní člen

Detekovány nejsou, pokud je $E(x)$ násobkem $G(x)$.

Vysvětlete token-passing.

Jednotlivé uzly jsou rovnocenné a oprávnění má pouze držitel tokenu, který si uzly předávají v kruhu mezi sebou. Vlastnictví tokenu je obvykle časově omezeno.
Výhoda: nestane se, že by výpadek jednoho uzlu – mastera znamenal výpadek celé sítě
Nevýhoda: trvá dlouho, než se kruh zformuje

Popište adresaci uzlů a adresaci zpráv.

Při adresaci uzlů je každému uzlu přiřazena unikátní MAC adresa, která jej identifikuje v síti, zatímco při adresaci zpráv je každá jednotlivá zpráva identifikována unikátní adresou (identifikátorem). Adresace uzlů se používá v distribuovaných systémech.

K čemu slouží ARP protokol a na jaké vrstvě se nachází?

ARP (Adress Resolution Protocol) poskytuje konversi IP adresy na MAC adresu.
Slouží spojové vrstvě, která neumí s IP adresami pracovat.
Uzel sítě si udržuje tabulku převodů z IP do MAC, které se říká ARP cache.
Pokud IP nenalezne, vyžádá si ji broadcastem po spojové vrstvě a příjemci vyhodnotí, zda je dotazovaná IP jejich.
Nachází se na spojové vrstvě.

7. Jaká je maximální délka shlukové chyby t (shluková chyba délky t je definována jako $x^i \cdot \left(x^{t-1} + a_{t-2} \cdot x^{t-2} + \cdots + a_1 \cdot x^1 + 1\right)$, kde koeficienty a_1 až a_{t-2} nabývají hodnot 0 nebo 1), kterou CRC kód s jistotou odhalí? Své tvrzení dokažte.

Vysvětlete, jak funguje virtuální odposlech u Wi-Fi.

Uzel, který chce poslouchat, nejprve signálem RTS – Request To Send přes CSMA / CA vyšle

žádost o přidělení kanálu. Přístupový bod odpoví přidělením vysílacího času signálem CTS – Clear To Send. Ostatní slyší a pokládají kanál za obsazený. Tímto se výrazně sníží pravděpodobnost vzniku kolise.

8. Vysvětlete funkční rozdíly mezi rozbočovačem (hub) a přepínačem (switch) – obecně, ne pro konkrétní síťovou technologii.

   Zatímco rozbočovač je pasivní součástka, která nemá vnitřní logiku a funguje v polo-duplexním přenosu na fysické vrstvě, switch pracuje na spojové vrstvě a aktivně zabraňuje kolisím v plně duplexním přenosu.

9. Vysvětlete rozdíl mezi metodami adresace uzlů a adresace zpráv.

   Při adresaci uzlů je každému uzlu přiřazena unikátní MAC adresa, která jej identifikuje v síti, zatímco při adresaci zpráv je každá jednotlivá zpráva identifikována unikátní adresou (identifikátorem). Adresace uzlů se používá v distribuovaných systémech.

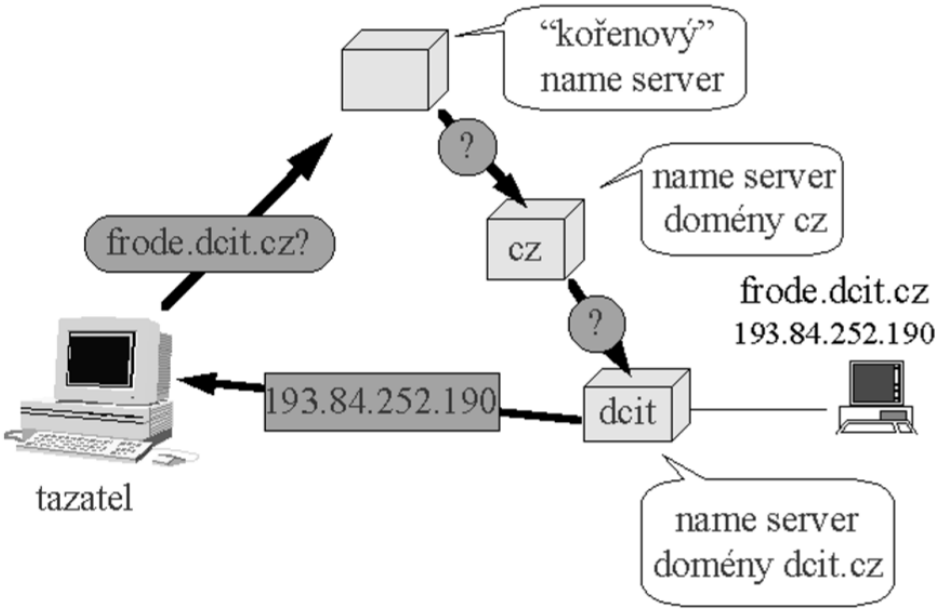
   Vysvětlete (obecně) rozdíl mezi adresací na spojové a síťové vrstvě ISO / OSI modelu a souvislost mezi nimi. Uveďte a vysvětlete konkrétní řešení pro nalezení linkové (MAC) adresy příjemce, známe-li jeho síťovou adresu, používané v IP sítích.

   Na síťové vrstvě je adresace dána IP adresami, na spojové MAC adresami.

   Jaký je rozdíl mezi synchronním a asynchronním přenosem? Kdy se který používá?

   Asynchronní přenos posílá na rozdíl od synchronního data s náhodnými rozestupy – nesynchronisovaně.
   Asynchronní se používá v emailech, synchronní na příklad u videochatu.

10. Popište funkční principy mechanismu DNS v IP sítích. Jaký je rozdíl mezi rekursivním a iterativním algoritmem vyhledávání?



Moje vlastní slova:
DNS je název serverů a stejnojmenného protokolu pro překlad doménových jmen na IP adresy. Tazatel odešle na správce domén (v Česku myslím CZNIC), a ten jej odkáže na správce DNS nižšího řádu, který jej pak odkáže případně ještě níž. Takže při připojení k www.fel.cvut.cz se nejdřív ptáme správce domény .cz, ta nás odkáže na správce poddomény cvut, který nás odkáže na samotné fel, odkud dostaneme IP.

Rekursivní vyhledávání: na dotaz DNS udělá všechnu potřebnou práci pro nalezení odpovědi – může se za odesílatele ptát i dalších DNS serverů

Iterativní vyhledávání: na dotaz DNS může vrátit referenci na další DNS server, který by mohl míz odpověď na zadaný dotaz

Přesně vysvětlete smysl a funkci mechanismů NAT a NAPT v IP sítích.

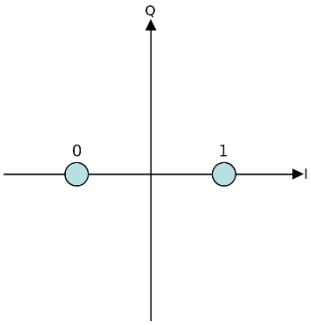
NAT (Network Address Translation) se používá pro přístup více počítačů z lokální sítě do internetu prostřednictvím jediné veřejné IP adresy. Hlavním důvodem k použití NAT je omezení potřebných IP adres, které musí organisace či společnost používat.
U NAPT (Network Address Port Translation) se kromě IP adresy překládá i číslo portu, čímž je celá privátní síť z pohledu veřejné sítě vnímána jako jeden uzel.

Jaký je princip fragmentace na síťové vrstvě? Je nějaký rozdíl mezi fragmentací u IPv4 a IPv6?

Fragmentace je rozdělování IP datagramů na menší části, aby mohly být přeneseny další částí počítačové sítě. Každá část přenosové trasy v počítačové síti má totiž definovanou svoji maximální MTU (anglicky Maximum Transmission Unit), která určuje maximální velikost IP datagramu, který je možné přenést.
Rozdíl mezi fragmentací v IPv4 a IPv6 je ten, že v IPv6 smí fragmentovat pouze odesílatel.

Popište princip BPSK, nakreslete jeho konstelační diagram a vyjmenujte další typy fásové modulace.

BPSK je digitální modulace založená na posunutí fáse harmonické nosné o 0° nebo 180° v závislosti na hodnotě binárního modulačního signálu.
Konstelační diagram:

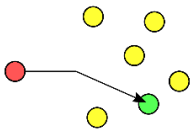
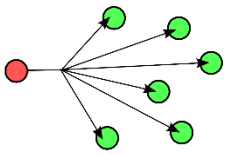
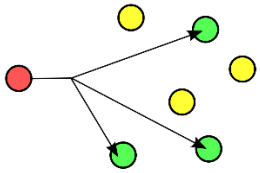


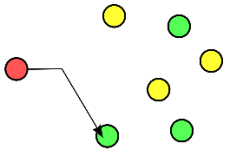
Další typy fásové modulace: PSK, BPSK, QPSK, 8-PSK, QAM

11. Co nejpodrobněji vysvětlete, jakým způsobem zajišťuje protokol TCP spolehlivou službu.

Využívá spojovaného přenosu – před odesíláním dat navazuje spojení mezi klientem a serverem, které je realizováno trojcestným hanshakingem:
Při navazování spojení si každá strana náhodně zvolí pořadové číslo, od kterého bude číslovat odesílané byty, ta si navzájem pošlou a drží tak po celou dobu přenosu správná pořadí bytů.
Každý paket obsahuje „checksum“, což je číslo spočítané určitým algoritmem a slouží k ověřování správnosti přijatých dat. Odesílatel tak za data vloží checksum a příjemce jej pak porovnává s vlastním výpočtem.
Dalším bezpečnostním prvkem je timer. Odesílatel si odpočítává čas od odeslaného paketu a pokud překročí určitou dobu, odešle paket znovu. Provádí se to pro případ, že by se paket ztratil někde na cestě a příjemce by pak nemohl odeslat acknowledgement.

Jaký je rozdíl mezi unicast, anycast, broadcast a multicast?

Typ	Asociace	Dosah	Příklad použití
Unicast	 1 : 1	Celá síť	HTTP
Broadcast	1:N 	Podsíť	ARP
Multicast	1:N nebo M:N 	Předem definovaný	SLP

Anycast	N:M, ke N > M 	Celá síť	BGP

12. Uveďte základní rozdíly mezi protokoly UDP a TCP.

- TCP je spolehlivý přenos, kde je zaručeno, že data dojdou nepozměněná, zatímco UDP nic takového nezaručuje
- TCP je kvůli svojí spolehlivosti pomalejší
- TCP používá řízení toku, aby nedošlo k přehlcení příjemce, což UDP neřeší

Díky výše zmíněným rozdílům je TCP vhodné tam, kde je důležité, aby data byla přijata bez chyb. Využívají jej protokoly HTTP, SSH, FTP, SMTP.
UDP se uplatňuje tam, kde je na prvním místě rychlost. To může být například při online hrách nebo live streamech.

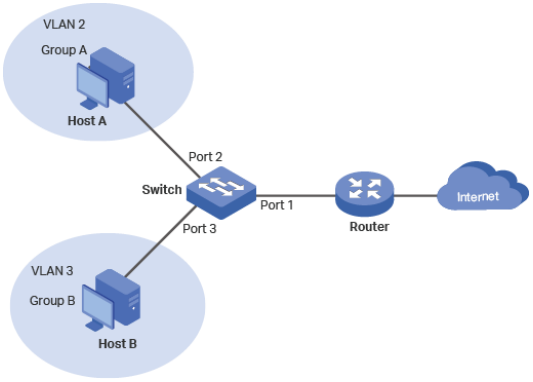
Zapište uvedené adresy do kanonického tvaru (nemáme v k disposici přímo tu jednu z testu, tak sem dávám příklady, kde by to šlo teoreticky pokonit).

Zadání	Kanonický tvar
2001:0001:0002:0003:0004:0005:0006:0007	2001:1:2:3:4:5:6:7
2041:0000:140F::875B:131B	2041:0:140f::875b:131b
2001:0000:0dea:C1AB:0000:00D0:ABCD:004E	2001:0:0eab:dead::a0:abcd:4e
2001:0:0:0dea:0:0:131B:875B	2001::dea:0:0:131b:875b

Pro další příklady si zkuste: https://www.ultratools.com/tools/ipv6Compress
Pravidla jsou:

- Můžete zkrátit několik po sobě jdoucích polí nul na jedno:
  2001:0:0:0:0:0:0:0 -> 2001::
- Akci výše můžete provést pouze jednou a musí to být pro ten nejdelší sled polí nul.
- Pokud jsou dvě stejně dlouhá pole nul – vždy zkraťte to první.
- Musíte zkrátit zápis jednotlivých polí, pokud to jde – pokud dávají v HEX stejná čísla. Na příklad 0001 na 1, 0000 na 0 apod., což se nepočítá jako zkrácení z prvního bodu.

13. Vysvětlete smysl a způsob implementace technologie VLAN v sítích Ethernet.
Virtuální LAN slouží k logickému rozdělení sítě nezávisle na fyzickém uspořádání.
VLAN (Virtual Local Area Network) je logicky nezávislá síť v rámci jednoho nebo několika zařízení. Je vytvářena s cílem učinit logickou organizaci sítě nezávislou na fyzické vrstvě, čímž lze usnadnit správu sítě, zvýšit její výkon a podpořit bezpečnost.
Příklad:
V jedné budově jsou všechny počítače ze všech pater připojené na jedné síti, a tak všichni vidí všechno od ostatních. VLAN je vlastně způsob isolace. Na přepínači nastavíme broadcastové domény pro každé patro zvlášť a podle toho patra zapojíme.



Výhody: Zjednodušení sítě, zvýšení bezpečnosti, omezení broadcastů

Jak se chová hub, když v ethernetu dojde ke kolisi?

Vyšle do všech portů jam signál.

Otázky dle zveřejněných okruhů v letním semestru roku 2019 / 2020

1. otázka na OSI model, funkce vrstev a komunikaci mezi nimi

2. výpočet odrazů na bezeztrátovém vedení

3. výpočet CRC jednou z přednášených metod

4. jeden z důkazů detekčních schopností CRC (pro ty co chtějí lepší známku :)

5. otázky o protokolech rodiny TCP/IP

6. otázka na téma metod řízení přístupu k médiu

7. otázka na téma reakce na výskyt chyb v komunikaci (ARQ metody, ale nejen ty)

8. otázka na typy a vlastnosti propojovacích prvků

- o modulacích ve fyzické vrstvě chceme znalost základních principů jednotlivých typů modulací (definiční vztahy, pouze AM podrobně pro harmonický modulační signál)
- je třeba rozumět šíření paprsku v optickém vlákně a umět odvodit numerickou aperturu vlákna (viz laboratorní úloha, kde jste ji i měřili)
- obecně u všech dalších témat

1. učte se principy a algoritmy
2. neučte se zpaměti detaily, které k tomu nejsou třeba (např. strukturu hlaviček jednotlivých protokolů)

- takže při otázce na rozdíl mezi lokálně a globálně definovanou MAC adresou mne nezajímá, jestli lokálně definovaná má nějaký konkrétní bit roven 1 a globálně definovaná nule, ale co z toho vyplývá pro vás jako uživatele či administrátory, když adresu sami definujete či používáte
- při otázce na smysl portů v TCP/UDP mne až tak nezajímá, že porty jsou v hlavičce hned na začátku, ale k čemu slouží, zda a případně jak jsou přidělovány a proč ...
- při otázce na implementaci napájení po Ethernetu se neučte číselné rozsahy měřeného odporu pro detekci, zda zařízení chce či nechce napájení ze síťového prvku, ale obecně algoritmus, kterým to přepínač zjišťuje
- atd.

V otázkách písemného testu samozřejmě nebude nic, co nebylo odpřednášeno (naštěstí jsme zvládli všechna témata).

5.

Uveďte, jaké vrstvy definuje sada protokolů TCP / IP a pro každou vyjmenujte nějaký protokol.

Aplikační vrstva – SMTP, Telnet
Transportní vrstva – TCP / UDP
Síťová vrstva – IP
Vrstva síťového rozhraní – Ethernet, Token-Ring

Popište typy doručení dat v IP protokolu.

Unicast – jeden příjemce
Broadcast – směrován do cílové sítě
Multicast – doručení vybrané skupině uživatelů
Anycast – nejbližší příjemce ze skupiny možných poskytovatelů služby (IPv6)

Jak vypadají IPv4 a IPv6 adresy protokolu IP?

IPv4: xxx:xxx:xxx:xxx, neboli čtyři dekadická čísla v rozsahu od 0 do 255.

IPv6: 2001:0db8:85a3:0000:0000:8a2e:0370:7334, neboli 16 bytů

K čemu slouží ARP protokol?

ARP (Adress Resolution Protocol) poskytuje konversi IP adresy na MAC adresu.
Slouží spojové vrstvě, která neumí s IP adresami pracovat.
Uzel sítě si udržuje tabulku převodů z IP do MAC, které se říká ARP cache.
Pokud IP nenalezne, vyžádá si ji broadcastem po spojové vrstvě a příjemci vyhodnotí, zda je dotazovaná IP jejich.

K čemu slouží ICMP protokol?

ICMP (Internet Control Message Protocol) slouží k hlášení problémů při zpracování IP paketů směrovači.
Nachází se v datovém poli IP paketu, ale neslouží k zajištění spolehlivosti přenosu. Používá se například při příkazech ping a tracert.

K čemu slouží NDP protokol?

NDP (Neighbor Discovery Protocol) ověřuje dosažitelnost sousedů, detekuje duplicitní adresy a přesměrovává.

Co jsou porty a k čemu slouží?

Síťový port je speciální číslo, které slouží k rozlišení aplikace v rámci počítače při komunikaci v sítích.
Porty jsou rozděleny do tří skupin:
- dobře známé porty (0 – 1023) jsou vyhrazené pro nejběžnější služby
- registrované porty (1024 – 49151) jsou přidělované ICANN
- dynamické a soukromé porty (49151 – 65535) nejsou pevně přidělené žádné aplikaci
Známá čísla: 20 – FTP, 22 – SSH, 25 – SMTP, 80 – http

K čemu slouží DHCP protokol?

DHCP protokol umožňuje prostřednictvím DHCP serveru nastavovat stanicím v počítačové síti sadu parametrů – IP adresu, masku podsítě, default gateway, adresu DNS serveru atd. – nutných pro komunikaci pomocí IP protokolu.

K čemu slouží DNS?

DNS (Domain Name System) je systém doménových jmen realisovaný DNS servery a protokolem stejného jména. Jeho hlavním úkolem a příčinou vzniku jsou vzájemné převody doménových jmen a IP adres.

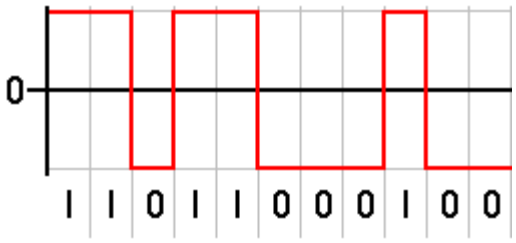
Jaké jsou typy DNS serverů?

Primární –probíhá na něm editace záznamů
Sekundární – přebírá data od primárního serveru
Caching only – slouží k omezení zátěže

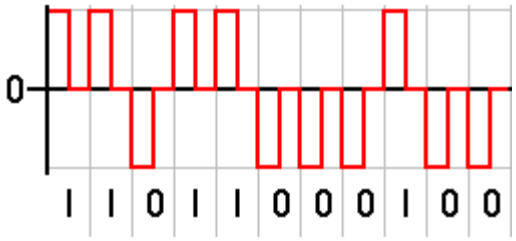
6.

Vyjmenujte několik typů kódování signálu a uveďte, jaké mají výhody a nevýhody.

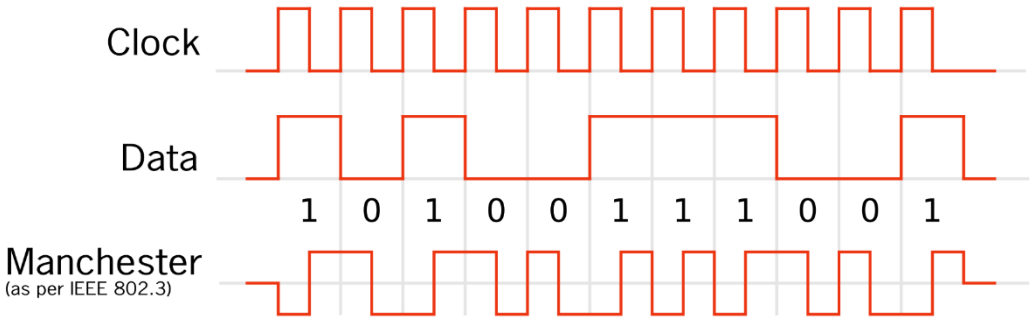
NRZ (Non Return To Zero) – úroveň signálu přímo odpovídá 1 nebo 0.
Výhody: na rozdíl od RZ postačí poloviční šířka pásma



RZ (Return To Zero) – třístavový, polovina intervalu +1 při bitu 1, při bitu 0 zase -1, druhá polovina intervalu je nenulová.
Výhody: jednodušší a levnější čipy než NRZ.
Nevýhody: Vyžaduje dvojnásobnou šířku pásma vzhledem k NRZ.

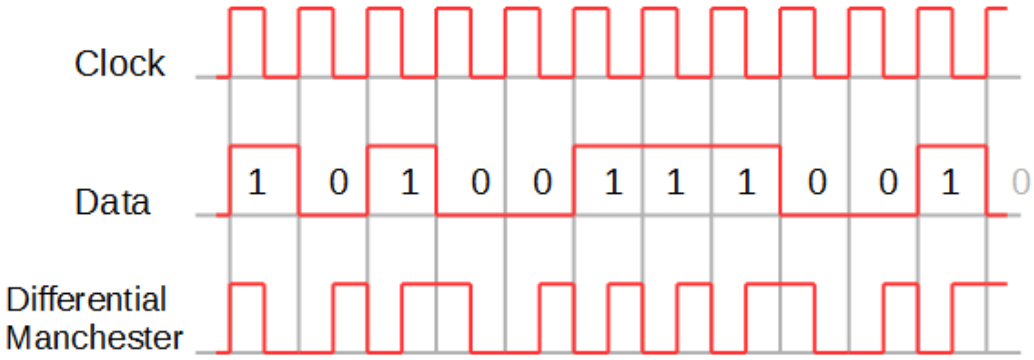


PSK (Manchester) – Pro vyjádření hodnoty bitu se do poloviny bitového intervalu původního signálu vloží hrana – změna signálu. Pokud signál v této hraně přechází z vysoké úrovně na nízkou úroveň, pak vyjadřuje hrana hodnotu bitu 0. Pokud signál přechází z nízké úrovně na vysokou úroveň, hodnota bitu bude 1. Protože se hrana vždy nachází uprostřed každého bitového intervalu, může snadno sloužit k synchronisaci.

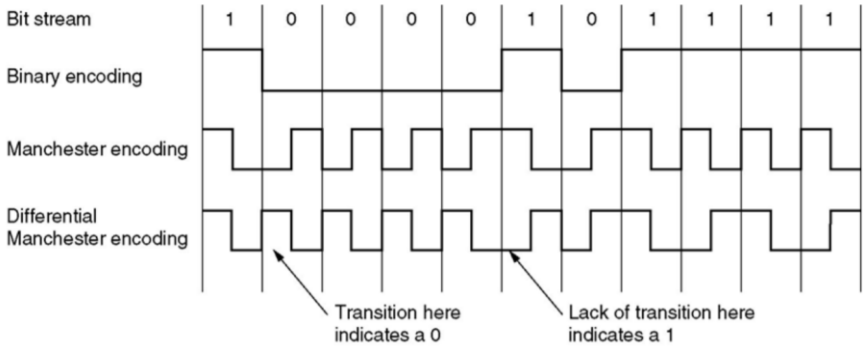


Výhody: Hodiny jsou vnořeny v samotném signálu, což zjednodušuje synchronisaci.
Nevýhody: Vyžaduje dvojnásobnou šířku pásma vzhledem k NRZ.

DPSK (Diferenciální Manchester) - Hodinový signál potřebný pro synchronní přenos je, stejně jako u klasického Manchester kódování, začleněn přímo do přenášených dat. Tím pádem dochází k průběžné synchronizaci odesílatele a příjemce a zároveň není potřeba vést hodinový signál po samostatné lince. V názvu je použito slovo diferenciální, neboť na rozdíl od klasického manchesterského kódování jsou jednotlivé bity (0 nebo 1) kódovány přítomností nebo absencí přechodu.



Přímé porovnání Manchesteru s diferenciální versí:



7.

Vyjmenujte typy modulací a jejich rozdělení.

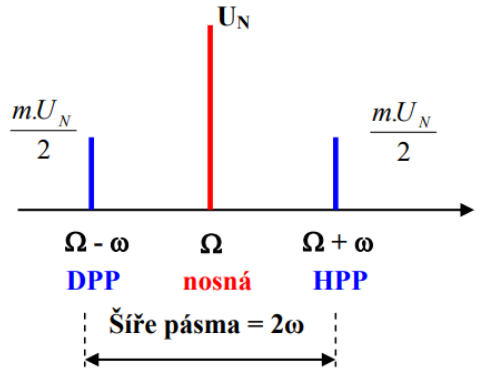
Z hlediska modulované veličiny – amplitudová, frekvenční, fásová, šířková

Z hlediska nosného signálu – s harmonickým nosným signálem nebo s impulsním

Dle modulačního signálu – analogový nebo číslicový, který může být binární či vícestavový

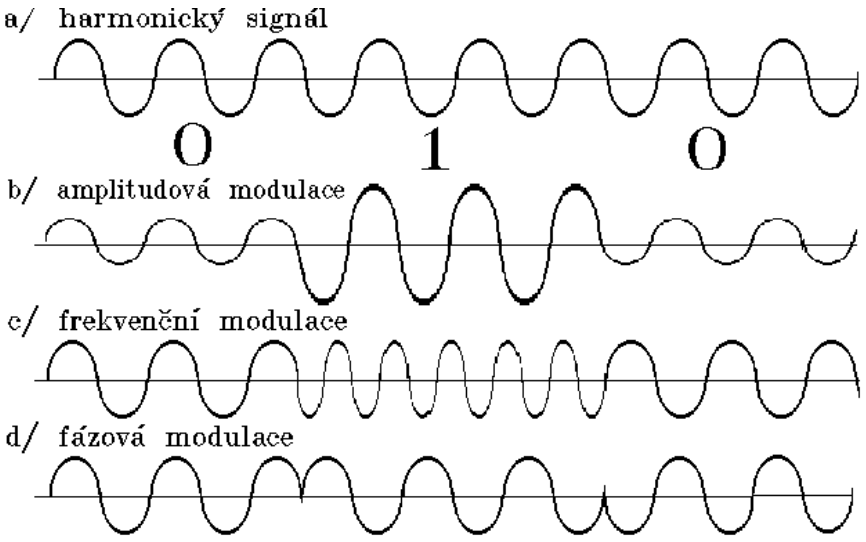
Nakreslete kmitočtové spektrum AM modulovaného signálu.

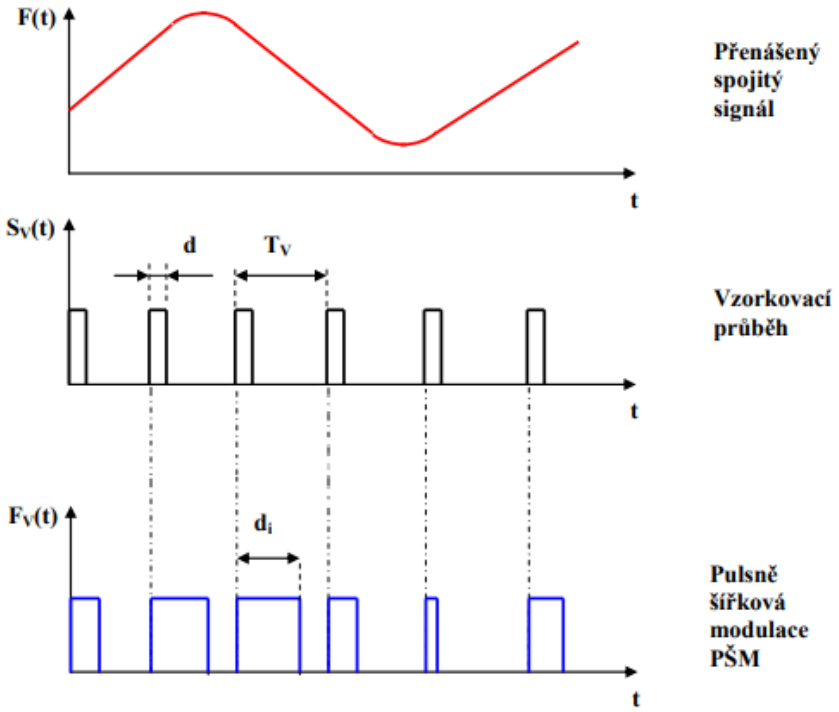
DPP a HPP jsou dolní postranní pásmo a horní postranní pásmo.



Nakreslete principy funkcí amplitudové, frekvenční, fásové a šířkové modulace.

(Nejspíš to nebude potřeba, ale je na tom moc hezky vidět, jak to má fungovat)





Popište základní typy datových přenosů.

- Podle směru přenosu – simplex, half-duplex, duplex
- Podle počtu současně využitých kanálů – sériový, paralelní
- Podle způsobu synchronisace – synchronní, asynchronní

Jaký je rozdíl mezi synchronním a asynchronním přenosem? Kdy se který používá?

Asynchronní přenos posílá data s náhodnými rozestupy – nesynchronisovaně. Používá se v emailech. Synchronní se používá například u videochatu.

Jaký je rozdíl mezi lokálně a globálně definovanou MAC adresou? (vyskytlo se ve výčtu otázek)

Podle odpovědí na Quoře nic jako lokálně definované MAC adresy neexistují, neboť, jak je jasné ze slova „globálně“, jsou ty globálně definované naprosto unikátní.
Pokud tomu rozumím dobře, tak lokální MAC adresy jsou adresy, které si můžeme vytvořit ve vlastní sítí a které musí být v rámci této sítě unikátní. ¯_(ツ)_/¯

Co je to FDM a jak funguje?

FDM (Frequency Division Multiplex) je princip přenosu více signálů jedním společným širokopásmovým přenosovým médiem, při kterém každý z přenášených signálů používá jinou část kmitočtového pásma.
Kmitočtové spektrum každého signálu je posunuto do jiného kmitočtového pásma; přenáší se sloučené signály, které se na přijímací straně pomocí pásmových propustí posunou do původního kmitočtového pásma.

Co je to TDM a jak funguje?

TDM (Time-Division Multiplex) je princip přenosu více signálů společným přenosovým médiem, při kterém jsou jednotlivé signály odděleny tím, že je každý vysílán pouze v krátkých pevně definovaných časových intervalech nazývaných časové sloty. Laicky řečeno „každý chvilku tahá pilkuů.

Co je to STDM a jak funguje?

STDM (Statistical Time-Division Multiplex) je princip přenosu společným přenosovým médiem, při kterém je komunikační kanál rozdělen do náhodného počtu datových toků. Celkový datový tok je pak řízen v závislosti na používánosti jednotlivých dílčích datových toků.

Vyjmenujte metody řízení přístupu k médiu

Deterministické:

Master-Slave:

Master se pravidelně dotazuje všech potenciálních zájemců – slavů o vysílání.
Výhoda: jednoduchá implementace
Nevýhoda: pokud vypadne master, tak je všechno v pytli
Využití: systémy s nižší datovou propustností

Token Passing (vyskytlo se v testu):

Jednotlivé uzly jsou rovnocenné a oprávnění má pouze držitel tokenu, který si uzly předávají v kruhu mezi sebou. Vlastnictví tokenu je obvykle časově omezeno.
Výhoda: nestane se, že by výpadek jednoho uzlu – mastera znamenal výpadek celé sítě
Nevýhoda: trvá dlouho, než se kruh zformuje

Delegated Token: v podstatě totéž, co Master-Slave, jen je zde použita adresace zpráv a místo master se říká arbitr.

Stochastické:

Jedním z nejstarších byl protokol ALOHA. Dnes se využívají varianty CSMA.

CSMA

CSMA (Carrier Sense Multiple Access) je protokol, ve kterém uzel ověřuje nepřítomnost dalšího provozu před vysíláním před vysíláním na sdíleném fysickém médiu (<- fancy slovo pro kabel…).
Carrier Sense znamená, že vysílač naslouchá nosné vlně a pokud detekuje přítomnost signálu, tak čeká.
Multiple Access znamená, že na médiu vysílá a přijímá více uzlů. Vysílání jednoho uzlu je obecně přijímáno všemi ostatními uzly.

CSMA / CA

V CSMA / CA (Carrier Sense Multiple Access with Collision Avoidance) vysílající uzel oznamuje, že bude vysílat ještě před vysíláním. Na rozdíl od CSMA / CD nedetekuje kolise, ale snaží se jim rovnou předejít.

CSMA / CD (bylo v testu):

Na rozdíl od čistého CSMA si CSMA / CD (Carrier Sense Multiple Access with Collision Detection) při vysílání kontroluje přenosové médium, zda nezachytí jiné vysílání, které koliduje s jejím.

Pokud potencionální kolisi zjistí, zastaví vysílání, počká náhodnou dobu a opakuje pokus znovu. V CSMA a CSMA / CA se naproti tomu kolise nezjišťují a dochází k nim, čímž se zbytečně odvysílá celá datový rámec, který bude beztak nutno opakovat. Nejrozšířenějším představitelem je Ethernet.

CSMA / CR

CSMA / CR (Carrier Sense Multiple Access with Collision Resolution) následuje klasické CSMA / CA. Pokud ale jeden uzel detekuje kolisi, vyšle signál, který zastaví přenosy z dalších stanic a dostane prioritní přístup, čímž zabrání další kolisi, která by mohla nastat.

Jaký je rozdíl mezi přepínáním okruhů a přepínáním paketů?

Při přepínání okruhů vzniká mezi příjemcem a odesílatelem přímá, souvislá cesta a komunikace probíhá v reálném čase. Je to vhodné pro kontinuální datové přenosy, přenosy zvuku, obrazu. Příjemce nemusí být přímo adresován – je to prostě „ten na konci roury“.

Při přepínání paketů žádná souvislá vyhrazená cesta nevzniká. Na cestě k odesílateli jsou přestupní bodu, které si zásilku předávají. Není to v reálném čase – jednotlivé přestupní uzly nejprve paket přijmou a teprve pak jej předají dál. Je to vhodné pro počítačové sítě a tam, kde jsou náhodné požadavky – např. přenos souborů.

Jaký je rozdíl mezi spojovanou a nespojovanou službou?

Nespojovaná služba – před vysíláním dat není nutno budovat spojení s druhou stranou a jednotlivé pakety jsou odesílány a zpracovávány sítí nezávisle.

Spojovaná služba – před započetím vysílání je nutné navázat komunikační relaci. Zajišťuje doručení dat v nezměněném pořadí.

7.

Popište funkci ARQ (údajně se vyskytlo v testu)

ARQ (Automatic Repeat Query) je metoda, která za pomocí acknowledgementů a timerů zajišťuje spolehlivý přenos.

1. Každý odeslaný datový paket obsahuje kontrolní součet (např. CRC), aby příjemce mohl

detekovat chyby v přijatých datech.

2. Každý odeslaný datový paket obsahuje pořadové číslo, aby příjemce mohl jednoznačně

detekovat tentýž datový paket, přijatý dvakrát (a nepřijal tedy duplikát jako další blok dat).

3. Každé potvrzení odeslané příjemcem odesilateli (ACK – Acknowledgement) obsahuje pořadové

číslo potvrzovaného datového paketu.

4. Po každém odeslání paketu se odpočítává timer. V případě, že timer doběhne a odesílatel nedostal acknowledgement, odesílá paket znovu.

Jaké jsou implementace ARQ?

Repeat request – V případě, že nesedí kontrolní součet, opakuj přenos.

Stop & Wait – Po odeslání dat je očekáván acknowledgement. Pokud není do určité doby přijat, přenos se opakuje.

Go Back N – Vysílající uzel smí odeslat až N paketů, aniž by obdržel potvrzení, kde N je velikost vysílacího okénka. Potvrzení obsahuje pořadové číslo posledního správně přijatého paketu.
Po odeslání N paketů vysílač vyhodnotí pořadové číslo posledního přijatého potvrzení a pokračuje ve vysílání následujícího paketu.

Selective Repeat – Vysílací uzel smí odeslat až N rámců, aniž by obdrzžel potvrzení, kde N je velikost vysílacího okénka. Přijímač přijímá všechny bezchybně doručené pakety i po výskytu chyby až do počtu M, kde M je velikost přijímacího okénka. Potvrzení obsahuje pořadové číslo chybného paketu nebo dalšího v pořadí. Vysílač vyhodnotí pořadové číslo v posledním přijatém potvrzení a pokračuje vysíláním paketu s tímto číslem a následujících. Bezchybné se neopakují.

8.

Popište propojovací zařízení na jednotlivých vrstvách a vysvětlete jejich funkci.

Fysická vrstva: opakovač, rozbočovač
Spojová vrstva: most, přepínač
Síťová vrstva: směrovač
Aplikační vrstva: brána

Opakovač (Repeater):
Jedná se o digitální zesilovač přenášeného signálu. Je hloupý, neboť nemá žádnou logiku pro řízení toku či informaci co propustit a co poslat dál. Je to prostě zesilovač, nic víc.

Most (Bridge) a přepínač (Switch):
Jsou to aktivní prvky, které propojují jednotlivé uzly do hvězdicové topologie.
Přepínač přeposílá síťový provoz jenom do těch směrů, do kterých je to potřeba, čímž se odlišuje od jednoduššího hubu, který je hloupý a posílá všechno do všeho.
Aby přepínač dokázal reagovat na adresy příjemce a odesílatele, nemůže pracovat v reálném čase.
Musí nějakým způsobem ukládat data, díky čemuž je schopen propojovat segmenty s různými rychlostmi.
Most spojuje 2 segmenty, přepínač více.

Směrovač (Router):
Analysuje obsah paketu a odešle ho na správnou adresu.
Musí mít povědomí o topologii celé sítě – ukládá si údaje ve směrovací tabulce.
Může spojovat podsítě se zcela odlišnými fysickými a linkovými technologiemi.

Brána (Gateway):
Propojuje dvě sítě pracující odlišnými komunikačními protokoly.
Vykonává i funkci směrovače.
Příkladem brány je počítač, který pomocí webové stránky přijme z internetu zprávu, kterou odešle do mobilní GSM sítě v podobě SMS zprávy.
Default gateway označuje směrovač, přes který se stanice dostanou do vnější sítě.

Vyjmenujte a popište základní modely přenosu dat.

Klient server – uzel v roli serveru poskytuje službu uzlu v roli klienta.
Producent – Konsument – role se mohou měnit.

Algoritmy propojování v Ethernetu. (explicitně ve výčtu)

Popište STP protokol.

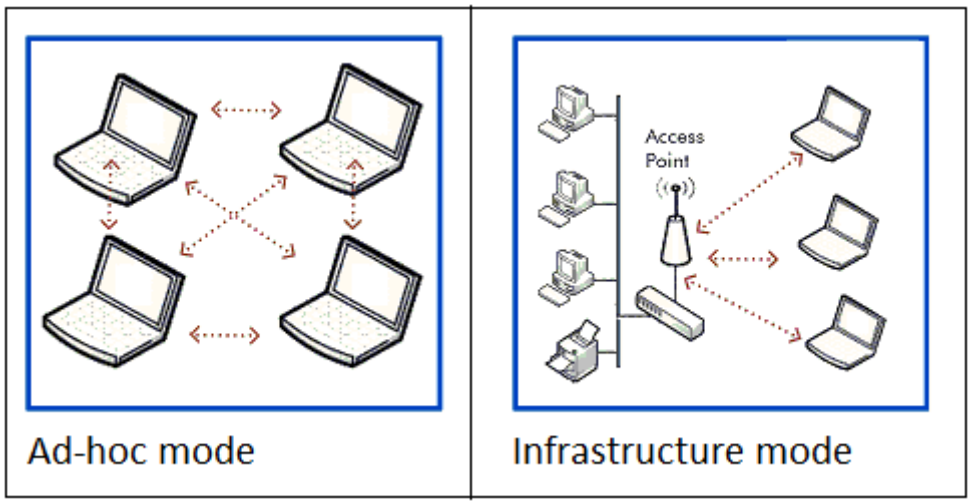
STP (Spanning Tree Protocol) je síťový protokol, který v ethernetových LAN sítích odstraňuje smyčky. STP vytvoří kostru stromu, která je propojená mosty a odpojí části, které nejsou její součástí, čímž vznikne právě jedna aktivní cesta mezi každými dvěma uzly.
Informace výše je vlastně důsledkem implementace stromem, jehož vlastností, jak již víme z logiky a grafů, je právě absence kruhů. Tím, že je právě jedna aktivní cest mezi každými dvěma uzly se výrazně omezí situace, kdy odeslaný paket putuje zbytečně do dalších uzlů, pro něž zpráva není určena – omezí se matematicky vzato na minimum.
Výhody: rychlost
Nevýhody: problematické sdílení kabeláže pro komunikaci a napájení

9.

Popište dva typy struktur bezdrátové sítě standardu IEEE802.11.

Ad-hoc sítě
- uzly komunikují přímo mezi sebou
- někdy se jim říká peer-to-peer sítě
- hodí se jen na krátkodobější připojení
- je rychle a lehce nastavitelný

Stacionární sítě
- uzly spolu komunikují přes jeden přístupový bod (access point)



Jaké jsou typy zabezpečení Wi-Fi sítě?

WEP (Wired Equivalent Privacy) – lze prolomit v řádu minut
WPA (Wi-Fi Protected Access) – dynamická změna klíče