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

BAN – sítě pro dálkové monitorování pacienta

* použití: lékařství – senzory na těle propojeny s PC a posílají info (např. o stavu srdce, ujité vzdálenosti)

PAN – osobní bezdrátová síť (Bluetooth, IrDA, ZigBee)

* použití: propojení elektrotechnických zařízení (mobilní telefon, PDA, NTB)
* topologie: hvězdice
* přenosová rychlost: několik Mbs
* rozlehlost: několik metrů
* příklady:
* WPAN-LR nízká přenosová rychlost – domácí spotřebiče
* WPAN-HR vysoká přenosová rychlost – stovky metrů

LAN – lokální síť

* použití: spojení uzlů (PC) v jedné místnosti či budově k připojení k internetu
* topologie: stromová
* přenosová rychlost: řádově Gbs
* rozlehlost:
* příklady:
	+ Ethernet – hvězdice
	+ Token Bus – sběrnice
	+ Token Ring – kruhová
	+ Bezdrátové – wifi

MAN – metropolitní síť

* použití: propojení lokálních sítí ve městech (Wi-fi, optické vlákno)
* topologie: sběrnice
* přenosová rychlost: řádově Gbs
* rozlehlost: desítky km
* příklady: protokol DQDB (Distributed Queue Dual Bus) – na koncepci ATM

WAN – rozsáhlé sítě

* použití: propojení LAN a MAN mezi státy či po celé zemi, často optika nebo satelit přes družice
* topologie: kruhová
* přenosová rychlost: kbs – Gbs
* rozlehlost: velké vzdálenosti
* příklady: internet
1. Uveďte rozdíl mezi sítěmi s přepínáním paketů, přepínáním zpráv a přepínáním kanálů. Jaké jsou jejich výhody a nevýhody?

přepínání paketů – neexistuje pevná cesta

- zpráva je rozdělena na části, v době vysílání se souběžně přijímá další zpráva

- o cestě každého paketu se rozhoduje zvlášť na přepínačích (linková – přepínání rámců, síťová – přepínání paketů)

* + urychlení přenosu, – možná ztráta, duplicita

přepínání zpráv – speciální případ přepínání paketů, přepínání mezi 2 body naráz, Store & Forward

* + lze použít jeden kanál vícekrát, – doba čekání při vícenásobném přenosu

přepínání kanálů – virtuální kanál mezi 2 body, přes který tečou všechna data, kanál se vytvoří před navázáním spojení nastavením přepínačů v bodech sítě (telefonní hovory, ATM, FrameRelay)

* + spolehlivost, – zabere kanál (po dobu přenosu nikdo jiný nemůže použít), čas
1. 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.

Protokol = horizontální komunikace mezi stejnými vrstvami

- standard, podle kterého probíhá [elektronická komunikace](http://cs.wikipedia.org/wiki/Komunikace) a přenos [dat](http://cs.wikipedia.org/wiki/Data) mezi dvěma koncovými body

**Služba** = týká se vertikální komunikace mezi vrstvami skrze rozhraní (Request, Response, Confirm, Indication)

1. Vyjmenujte a popište základní služby pro navázání spojení, přenos dat a ukončení spojení u spojově orientovaného protokolu (např. BSD sockety).

TCP/IP: Klient Server

 socket (typ) socket (typ)

 bind (ip, port)

 listen

 connect (ip, port) accept (socket)

 send receive

 close close

1. Nakreslete protokolový zásobník, vyjmenujte 7 základních úrovní referenčního modelu ISO/OSI a uveďte jejich základní funkce.

Protokolový zásobník: 4. Aplikační, 3. Transportní, 2. Síťová, 1. Vrstva síťového rozhraní (přenosová)

Model ISO/OSI

7. Aplikační – obecné a speciální služby pro aplikace (přenos souborů, terminál – adresářové služby, volání vzdál. podprogramů

6. Prezentační – převod aplikačních dat na data vhodná pro přenos nižšími vrstvami (komprese, šifrování, kódování)

5. Relační – řešení problému chyb nad přenosovými protokoly, řízení a synchronizace výměny dat mezi rel. vr. obou systémů

4. Transportní – přenos dat mezi koncovými uzly v kvalitě, jakou požadují vyšší vrstvy (řešení chyb, modifikace, ztráta dat)

3. Síťová – přenos dat mezi koncovými uzly, které spolu přímo nesousedí (směrování, síťové adresování, řízení toku dat)

2. Linková – přenos dat mezi sousedními uzly sítě, řadí rámce, oznamuje neopravitelné chyby, nastavuje parametry

1. Fyzická – zajišťuje převod proudu bitů na signál a opačně, aktivuje, udržuje a ruší fyzikální spoje (kabely, huby, Bluetooth)

1. Zakreslete protokolový zásobník TCP/IP, uveďte základní protokoly, jejich funkci a význam

4. Aplikační

* Telnet – připojení ke vzdálenému počítači
* HTTP – výměna hypertextových dokumentů ve formátu HTML
* DNS – výměna informací, převody doménových jmen a IP adres uzlů sítě
* SMTP – přenos zpráv elektronické pošty

3. Transportní

* TCP – vytvoření spojení, přes které se přenášejí data – zajišťuje spolehlivost při ztrátě paketu a správné pořadí
* UDP – netvoří trvalé spojení, nezaručuje, že se datagram neztratí, nezmění, či doručí vícekrát

2. Síťová

* IP – poskytuje datagramovou službu celé rodině protokolů TCP/IP
* ARP – IP na MAC, získání ethernetové MAC adresy sousedního stroje z jeho IP adresy
* ICMP – odesílání chybových zpráv, např. oznámení, že požadovaná služba není dostupná nebo počítač není dosažitelný

1. Vrstva síťového rozhraní (přenosová)

* PPP – autentizace, šifrování a kompresi přenášených dat
* IEEE – zabezpečení fyzického přístupu do počítačové sítě
* ADSL, Ethernet
1. Uveďte, čím je limitována frekvence změn číslicového signálu a čím je limitován počet úrovní tohoto signálu při přenosu komunikačním kanálem.
2. Uveďte základní typy komunikačních médií, jejich vlastnosti, zjednodušený náčrtek a kde se používají.
3. drátová (vodičová)
* Koaxiální kabel – sběrnicová topologie, elektrický kabel s jedním válcovým vnějším vodičem a jedním trubkovým vodičem vnitřním (kabelová televize, sluchátka a mikrofony, antény)
* Kroucená dvojlinka – hvězdicová topologie, páry vodičů, které jsou po své délce pravidelným způsobem zkrouceny (Ethernet, token ring, ATM)
* Optické vlákno – prostřednictvím světla přenáší signály ve směru své podélné osy, nepůsobí rušení, nelze odposlouchávat (přenos dat na dlouhé či krátké vzdálenosti, vysokorychlostní přenosy v internetu, telekomunikace)
	+ jednovidová (průměr 5 mikrometrů) – 100 Mbs, kilometry
	+ mnohavidová (průměr 5 nanometrů) – 100 Mbs - 10Gbs , do 1 km
1. bezdrátová
* zvukové vlny
* světelné vlny – krátké vzdálenosti, problémy teplo a nečistota ovzduší
* rádiové vlny – pozemní x družicové (vysoké 36000 km), rádiové přenosy
1. Jaké druhy optických vláken znáte? Čím se od sebe liší?
* jednovidová (průměr 5 mikrometrů) – komunikace na dlouhé vzdálenosti (mezi městy, kontinenty), 100 Mbs, kilometry
* mnohavidová (průměr 5 nanometrů) – komunikace na krátké vzdálenosti (v budově), 100 Mbs – 10 Gbs, do 1 km
	+ s konstantním indexem lomu
	+ s proměnným indexem lomu
1. Co je to přenos dat v základním pásmu a v přeneseném pásmu?

Základní pásmo (úzké) = nemodulovaný signál

- kmitočtové pásmo 0-200 MHz, na malé vzdálenosti, plně obsazují přenosový kanál

Přenesené pásmo = modulovaný signál = rozprostřené pásmo

- pokud chceme vysílat v konkrétním rozsahu (např. telefon 300 Hz – 3,5 kHz) – TV, rádio, bezdrátové systémy

1. Základní typy modulací, jejich vlastnosti a použití.

- účelem je změna vhodného nosného signálu pomocí modulujícího signálu, aby věrně reprezentoval binární data

- použití: spotřební elektrotechnika (TV přijímač, mobil, ...)

Frekvenční = mění se úhlová frekvence ω, (bit 1 více "nahuštěný) – přenos zvuku analogové TV

Fázová = mění se fáze nosné vlny Φ, (změna bitu = zlom ve směru) – v elektronických hudebních nástrojích

Amplitudová = mění se amplituda A, (bit 1 protáhlý do výšky) – rádia

1.
2. Do fázové roviny zakreslete příklad amplitudo-fázové modulace pro kódování 4 bitů.
3. Jaký je rozdíl mezi časovým a frekvenčním multiplexem. Zakreslete jednoduchý obrázek.
* Multiplex je na fyzické vrstvě

Frekvenční

* kmitočtové dělení, přenos více signálů jedním širokopásmovým přenosovým médiem (mezi jsou ochranná pásma)
* každý signál je na různých frekvencích (jiném kmitočtovém pásmu)
* využití: rádio, TV

Časový

* časové dělení
* každý signál má časový rámec (slot)
* využití: telefonní hovory
1. synchronní – kanály jsou pevně přidělené
2. asynchronní – kanály se dynamicky přiřazují
3. Přenosový systém T1 používá rámec, který vznikne jako časový multiplex jednoho řídícího 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.
4. Jak se liší kódování modulace od kódování signálu? Co to znamená, že signál je kódován „bez návratu k nule“

Kódování = proces, který binárně kóduje signál, tj. přiřazuje se hladinám 0 a 1

Modulace = proces, kterým se mění charakter vhodného nosného signálu na modulující signál (většinou sinusové)

1. Jaký je rozdíl mezi diferenciálním kódováním a kódováním, které není diferenciální?

- použití – synchronní přenosy

Diferenciální – hodinový signál je začleněn přímo do přenášených dat

- jednotlivé bity kódovány přítomností nebo absencí přechodu (1. jako nedif., 0 je změna posunutého hodinového signálu)

Nediferenciání – jednotlivé bity mají vždy přechod (0 směrem dolu, 1 směrem nahoru)

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

NRZ = NRZ-L – non return to zero (0 dole, 1 nahoře)

NRZI = NRZ-M – non return to zero inverted (změna z 0 na 1 na hraně hodinového signálu) – použití – USB

Výhody: v nezašuměném kanálu hodnoty pouze 0 a 1

Nevýhody: nelze použít na synchronní přenosy

1. Popište metody kódování dvojí fází a uveďte použití

Manchester = 1. jako nediferenciální, 0 je změna posunutého hodinového signálu

Diferenciální manchester = 0 směrem dolu, 1 směrem nahoru posunutého hodinového signálu

- použití: synchronní přenosy, Ethernet, Token Ring

1. Vysvětlete rozdíl mezi spojově orientovaným a nespojovaným modelem komunikace. Uveďte výhody a nevýhody.

TCP – protokol vytvářející spojení, přes které se přenášejí data (navázání spojení, odesílání/přijímání,kontrola, ukončení)

+ spolehlivý proti ztrátě paketu, zachovává pořadí

- vysoké režie

UDP – protokol, kde neexistuje trvalé spojení, jen přestane posílat, nezaručuje, že se datagram neztratí, nezmění pořadí

+ jednodušší, nízké režie

- bez záruky, nezachovává pořadí (spolehlivost musí být řešena na aplikační úrovni)

1. Načrtněte obecnou strukturu rámce na linkové úrovni pro délkově, znakově a bitově orientovaný protokol.

Bitově |FLAG|data|FLAG| nebo |Preambule|SDF|DA|SA|délka\_dat|data|FCS|Prodloužení|

SDF = příznak začátku rámce, DA+SA+délka dat = hlavička, FLAG = 0 po 5 jedničkách

Bytově (znakově) |STX|data|data|data|ETX|

Rámcově (délkově) 

1. Jaký je rozdíl mezi rámcem a paketem.

Rámec – jednotka přenosu na linkové úrovni ISO/OSI (větší obálka, L2)

Paket – jednotka přenosu na síťové úrovni ISO/OSI (menší obálka, L3)

1. Jak se určuje Hammingova vzdálenost a jak se dá určit, kdy je kód detekční a samoopravný.

Hammingova vzdálenost – počet míst, v němž se kódová slova liší

- charakterizuje odolnost kódu vůči poruchám a schopnost identifikovat či opravit chyby

HV = vzdálenostmin

DETEKCE = n <= dmin – 1

KOREKCE = n <= (dmin – 1):2

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

Paritní bit je přidaný redundantní bit ke kódovému slovu

- je speciální případ 1bitového CRC (polynom x+1)

- detekce lichého počtu chybových bitů ve slově

- příklad použití: - sudá = sudý počet 1

 - lichá = lichý počet 1

1. Co jsou to cyklické kódy, kde se používají. Uveďte vztahy pro výpočet zabezpečení zprávy a kontrolu jejího zabezpečení.

Cyklický kód = lineární kódy používané k zabezpečení dat při jejich přenosu

- úkol: umožnit detekci případných chyb v těchto datech

G(x) = zabezpečující (generující) polynom = délka zabezpečení

R(x) = M(x)/G(x) = zbytek po dělení = zabezpečovací pole

T(x) = M(x) | R(x) = odeslání

T(x)/G(x) po přijetí, pokud 0, přenos OK

1. Co je to transparentnost přenosu. Jak dosáhnout transparentnosti přenosu u bitově a znakově orientovaných protokolů?

Transparentnost = přenos dat, který žádná data neztratí ani nezkreslí, problémem jsou hlavně řídící znaky, které nesmí přenos interpretovat, nýbrž zacházet s nimi právě pouze jako s daty

- problém: Pokud určíme kódy 0 – 31 a 255 jako řídící znaky, co s daty s kódy 0 – 31?

Bitově – řídicí informace má v rámci pevné místo

- zajištění transparentnosti: vkládání bitů – po 5 jedničkách vložíme vždy nulu

Znakově – řídicí informace i data jsou disjunktní množiny znaků (na začátku a konci rámce)

- zajištění transparentnosti: vkládáním znakových prefixů – začátek STX, BOX, konec ETX, EOF

1. Co je to protokol Stop & Wait, kde se používá, jaké má vlastnosti. Uveďte typy rámců a strukturu jimi přenášené informace.

Stop & Wait = protokol linkové úrovně

- zdrojová entita vyšle rámec, cílová přijme a odešle potvrzení (ACK), teprve pak zdrojová odesílá další rámec

* simplexní s kladným potvrzováním
* duplexní s kladným potvrzováním – přenos dat oběma směry, souběžný přenos, nesamostatné potvrzování "piggybacking"

- použití: tam, kde poměr T/τ je malý, T = celkový čas od odeslání rámce po přijetí ACK, τ = zpoždění mezi odesláním a přijetím rámce či ACK

- vlastnosti:

* rámce segmentovány do menších, protože je menší ppst chyby
* v čase se posílá pouze jeden paket
* omezená propustnost

- rámce: |číslo\_rámce|číslo\_očekávaného\_rámce|data|

- potvrzení: |číslo\_očekávaného\_rámce|ACK|

1. Navrhněte jednoduchý algoritmus pro vysílač a přijímač simplexního protokolu Stop & Wait.

Algorithm at node B (receiver) to receive from node A:

1.NFE ← 0, repeat steps 2 and 3 forever

2.If error-free frame received and SeqNum=NFE, then pass packet to higher level and NFE ← NFE + 1 (modulo 2)

3.At some bounded time after receiving error-free frame send request for NFE to A

http://www.cs.iastate.edu/~cs586/notes/ch2-2slides.pdf

1. Jak se liší protokol Stop & Wait od protokolů s klouzajícím okénkem?

Stop & Wait posílá rámce po jednom

Klouzající okénko může odesílat více rámců po sobě – max. počet nepotvrzených rámců je velikost okénka

1. Zakreslete průběh přenosu dat protokolem s klouzajícím okénkem a se sekvenčním příjmem. Jaký musí

platit vztah mezi velikostí vysílacího a přijímacího okénka a proč.

Sekvenční přenos – okénko vysílá N a přijímá 1

* + vysílač pošle 6 rámců, přijímač přijme 1. a ztratil se 2., 4 rámce zahodí a přijímat začne, až přijme opět 2.
	+ velikost okénka W < N rozsah číslování
1. Zakreslete průběh přenosu dat protokolem s klouzajícím okénkem a s nesekvenčním příjmem. Jaký

musí platit vztah mezi velikostí vysílacího a přijímacího okénka a proč.

Nesekvenční přenos – odesílá N a přijímá N

* odesílá jen rámec, který nedorazil
* potvrzuje se celé okénko
	+ data nemusí být ve stejném pořadí
	+ velikost okénka W < N/2 rozsah číslování pro případ, že by se ztratilo potvrzení
1. Co je to Petriho síť. Zakreslete Petriho síť pro simplexní protokol Stop a Wait s kladným potvrzováním.

Petriho síť =  reprezentace [distribuovaných systémů](http://cs.wikipedia.org/wiki/Distribuovan%C3%BD_syst%C3%A9m)

-  reprezentuje strukturu distribuovaného systému jako orientovaný [bipartitní graf](http://cs.wikipedia.org/wiki/Bipartitn%C3%AD_graf) s ohodnocením

- prostředek k popisu činnosti komunikačních protokolů

- uzly: místa (O), přechody (|) a orientované hrany spojující pouze místa a přechody

1. Co je to Petriho síť. Zakreslete Petriho síť pro simplexní protokol Stop a Wait se záporným potvrzováním.
2. Zakreslete formát rámce protokolu HDLC, vysvětlete význam jednotlivých polí a uveďte popis struktury řídicího pole.

Protokol linkové úrovně, bitově orinetovaný

|poč\_značka|adresa|řízení|data|FCS|konečná\_značka|

 01111110 8 b 8/16 b 8 b 16 b 01111110

Značka = start/konec přenosu

Řídící pole = rozlišuje typ rámce

* informační (k přenosu dat)
* řídící (k potvrzování přenosu)
	+ RR... Receive Ready (ACK)
	+ RNR... Receive not ready (ACK)
	+ REJ... Reject (NAK)
	+ SREJ... Selection Reject
* nečíslované (k navázání spojení, hlášení chyb a ukončení spojení)

FCS = Frame Check Sequence – kontrola rámce

1. Jaké znáte decentralizované metody přístupu ke komunikačnímu médiu a čím se kvalitativně liší.
2. S náhodným přístupem – řešení konfliktů pomocí náhody

Aloha (rádiové kanály), Synchronní aloha, CSMA, CSMA/CD

1. S rovnoměrným přístupem – předem dohodnuté pořadí vysílání, vychází z předávání pověření

Token ring, Token Bus

1. S prioritním přístupem – nejprve se vyšle priorita, pak data; soutěž, kdo vyhraje, vysílá

Priorita daná časem, Priorita daná kódem

1. 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 – sdílení přímého kanálu může vést ke kolizi (=souběžně vysílá více než 1 stanice)

Projev (Deketce kolize) – odpověď nedošla do doby ~ 2 τ

- opakování po náhodné době = snížení ppsti, že nastane další kolize

**Řešení** – Hromadná obsluha M/D/1 (M – náhodný příchod požadavků, D – zpracování požadavků trvá pevnou dobu, 1 – 1 prvek obsluhy), max. počet vstupních požadavků je 18% kapacity kanálu (aby nedošlo k zahlcení)

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

S náhodným přístupem – řešení konfliktů pomocí náhody, není garantováno, že uzel přenese určité množství dat za určitou dobu

Aloha – sdílení přenosového média mnoha účastníkům

- pokud některá ze stanic chce něco vysílat, tak prostě pošle zprávu

- pokud do určité doby (~ 2 τ) nedostane potvrzení, pošle zprávu znovu (po náhodné době)

**CSMA** – sdílený (vícenásobný) přístup s detekcí nosné vlny

- komunikační médium není rádio, ale vodič (sběrnicová síť)

- detekce nosné vlny (naslouchání) – pokud nikdo nevysílá, pak vysílám

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

**CSMA** – sdílený (vícenásobný) přístup s detekcí nosné vlny

- komunikační médium není rádio, ale vodič (sběrnicová síť)

- detekce nosné vlny (naslouchání) – pokud nikdo nevysílá, pak vysílám

* naléhající – pokud někdo vysílá, pak čekám na uvolnění kanálu a začnu vysílat, až přestane

 – ke kolizi dojde, pokud ve stejnou chvíli začne vysílat více účastníků

* nenaléhající – pokud někdo vysílá, pak přeplánuji vysílání za náhodně dlouhou dobu
* p-naléhající – s ppstí p naléhající, s ppstí (1-p) nenaléhající
1. Co je to CSMA/CD? Uveďte příklad lokální počítačové sítě, která tuto metodu používá.

**CSMA** – naslouchání nosné vlny, **CD** – detekce kolize

- při svém vysílání současně kontroluje přenosové médium, zda nezachytí jiné vysílání, které koliduje s jejím (oproti CSMA)

- pokud stanice zjistí kolizi, zastaví vysílání, počká náhodnou dobu a opakuje svůj pokus znovu

- Ethernet (LAN) !!!

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

S rovnoměrným přístupem – stanice mají předem dohodnuté pořadí vysílání (bezkolizní metoda)

- vychází z předávání pověření (= malý paket s nezaměnitelným obsahem, jedinečný v síti):

* ve fyzickém okruhu = Token Ring
* v logickém okruhu = Token Bus
1. Vysvětlete princip protokolu s bitovou mapou.

Bitová mapa – používá se ke komprimaci signálu, v němž je ve velkém množství zastoupen jeden znak

- máme-li takový soubor, metoda potlačení nul není příliš efektivní, protože 0 jsou ve skupinách po 2 nebo 3

- v tomto případě protokol s bitovou mapou má lepší kompresní poměr

- potlačovaný znak se v bitové mapě nahradí za 0 – adg\*\*a => adga + 111001

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

Předávání pověření ve fyzickém kruhu

- stanice tvoří kruh a předávají si pověření (= malý paket s nezaměnitelným obsahem, jedinečný v síti, kdo ho má, vysílá)

- jedna stanice je monitorovací a stará se o to, aby se neztratilo pověření

Rekonstrukce kruhu – ztratí-li se pověření

- ten, kdo ji ztratil, pošle do kruhu svou prioritu, kdo má vyšší, tak jí zvýší

- pokud ten, kdo má nejvyšší prioritu, objel celý kruh, je nastaven jako monitorovací stanice

1. 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?

Předávání pověření v logickém kruhu 

- stanice tvoří sběrnici a předávají si pověření (= malý paket s nezaměnitelným obsahem, jedinečný v síti, kdo ho má, vysílá)

Rekonstrukce kruhu – ztratí-li se pověření

- vysláno pověření tomu, kdo nejdéle detekuje nečinnost samotné sítě

Postup – kolize – algoritmus binárního vyhledávání adres vzestupně

- vytvoří se nová síť

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

S rovnoměrným přístupem – předem dohodnuté pořadí vysílání, vychází z předávání pověření

S prioritním přístupem – nejprve se vyšle priorita, pak data; soutěž, kdo vyhraje, vysílá

Priorita daná kódem – je vyslána priorita, soutěž – binární kód se porovnává od nejvyšší váhy bit po bitu od začátku, nejvyšší je vítěz A | 101 | 1 | 0 | konec vysílá 1 – neudělá nic

 B | 110 | 1 | 1 | 0 | vítěz vysílá 0 – slyší 0 pokračuje; slyší 1 končí

- problém monopolizace

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

Problém monopolizace – pokud uzel s vysokou prioritou stále žádá o povolení vysílat, pak vždy vyhrává

Řešení:

* dynamická priorita
	+ na počátku priorita 0, každou prohru si každý zvýší dynamickou prioritu ++1, po vysílání zpět na pův. prioritu
	+ zaručí, že se na všechny dostane v konečné době
	+ |A 4| 04 | 14 | 24 | 04 | 14 |...
	+ |B 5| 05 | 15 | 05 | 15 | 25 |...
	+ |C 6| 06 | 06 | 16 | 26 | 06 |...
* dynamická jednobitová priorita
	+ na počátku priorita 0, každou prohru si každý zvýší dynamickou prioritu ++1, ale maximálně 1x za dobu než odvysílají všichni
	+ |A 4| 04 | 14 | 14 | 04 | 14 |...
	+ |B 5| 05 | 15 | 05 | 05 | 15 |...
	+ |C 6| 06 | 06 | 06 | 06 | 06 |...
1. 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?

Ethernet (IEEE 802.3) – fyzická a linková vrstva

Protokoly: IPv4, IPv6 (služby sítě internet), AppleTalk, IPX/SPX

Přenosové rychlosti:

* 10 Mbps – 2,5 km – klasický ethernet – CSMA/CD – dvojlinka, optické vlákno, koaxiální kabel
* 100 Mbps – 250 m – fast ethernet – CSMA/CD – dvojlinka (twist) nebo optické vlákno
* 1 Gbps – 25 m – gigabitový ethernet – CSMA/CD – dvojlinka (twist) nebo optické vlákno
* 10 Gbps – nemá cenu – pracuje duplexně – dvojlinka (twist) nebo optické vlákno

Rozlehlost: LAN

Topologie: sběrnice nebo hvězdice (dvojlinka)

Ethernet II – rozdíl jen ve formátu rámce, který je řešitelný softwarově

| preambule | DA | SA | typ/délka | data | CRC | Ethernet II pole určující typ vyššího protokolu (typ obsahu)

 64 b 48 b 48 b 16 b 46 – 1500 b 32 b IEEE 802.3 udává celkovou délku pole dat

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

- stanice před zahájením vysílání kontroluje, zda je médium volné

- může ke kolizi dojít, pokud dvě či více stanic zahájí vysílání téměř současně

1. Které protokoly popisují standardy IEEE 802.11, IEEE 802.15 a IEEE 802.16?

IEEE 802.11 – Wifi

IEEE 802.15 – Bluetooth

IEEE 802.16 – WiMAX – bezdrátová distribuce dat zaměřená na venkovní sítě, tedy jako doplněk k [Wi-Fi](http://cs.wikipedia.org/wiki/Wi-Fi) chápanému jako standard pro vnitřní sítě

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

VLAN – logicky nezávislá [síť](http://cs.wikipedia.org/wiki/Po%C4%8D%C3%ADta%C4%8Dov%C3%A1_s%C3%AD%C5%A5) v rámci jednoho nebo několika zařízení

- domény všesměrového vysílání (stejně jako LAN) s cílem učinit logickou organizaci sítě nezávislou na fyzické vrstvě

- na switchi (přepínačích)

- k běžným [paketům](http://cs.wikipedia.org/wiki/Paket) je připojena informace o čísle virtuální sítě, kterou zařízení využije k rozpoznání příslušnosti k síti

- rozpoznání dle MAC, portu switche, autentizace

+ usnadňují správu sítě, zvyšuje její výkon a podporuje bezpečnost

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

**Most (bridge)** = [síťové zařízení](http://cs.wikipedia.org/wiki/S%C3%AD%C5%A5ov%C3%A9_za%C5%99%C3%ADzen%C3%AD), které spojuje dvě části sítě na linkové vrstvě

Funkce: směruje rámce podle jejich hardwarové [MAC adresy](http://cs.wikipedia.org/wiki/MAC_adresa) (router se rozhoduje podle IP adresy uvnitř přenášeného datagramu)

**Opakovač** =  [aktivní síťový prvek](http://cs.wikipedia.org/wiki/S%C3%AD%C5%A5ov%C3%A9_za%C5%99%C3%ADzen%C3%AD) na fyzické vrstvě, který přijímá zkreslený, zašuměný nebo jinak poškozený signál a opravený, zesílený a správně časovaný ho vysílá dále

1. Vysvětlete, jak funguje Spanning Tree algoritmus a kdy se používá.

STP = Spanning Tree – síťový protokol

- jeden most je v roli kořenového mostu (root bridge) a všechny ostatní mosty vybírají ze všech svých směrů právě ten, který vede ke kořenovému

- vzniká přísně stromovitá struktura, v jejímž kořeni je kořenový most

Použití – přepínání na linkové úrovni, pokud máme redundantní spojení a je třeba rozhodnout, kterou cestu vybrat

- obr.: dva paralelní transparentní mosty

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

Source Routing – směrování zdroje odesílateli umožňuje zadat cestu paketu sítí

- způsob průchodu datových rámců skrz jednotlivé mosty se určí předem a pokyny k průchodu se vloží do rámce

- pokyny mají formu lineárního seznamu mostů, přes které má datový rámec postupně projít

Použití – zabraňuje přetížení, umožňuje řídit výkon sítě, umožňuje nalezení všech možných cest k hostiteli

1. Jaké problémy řeší síťová úroveň?

- přenos dat mezi koncovými uzly, které spolu přímo nesousedí

- směrování, adresování (IP), řízení toku dat

- obsahuje funkce, které umožňují překlenutí rozdílných vlastností technologií v přenosných sítích

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

- každý směrovač pošle paket do všech rozhraní kromě toho, z nějž dorazil, používá ho OSFP

+ zkouší všechny cesty, takže najde i tu nejlepší (nejkratší); nejrychlejší rozšíření informace po síti; vyrovná se s jakýmkoliv výpadkem

– nehospodárný (duplicitní pakety, vysoká zátěž cest),

– problémem roztékání jsou cykly v síti, které způsobí, že paket se po čase vrátí znovu a znovu (nutno omezit životnost)

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

např. RIP, směrování nejkratší cestou v počtu přeskoků k cíli (hopů)

- maximální délka 15, 16 bráno jako nekonečná vzdálenost

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

LSA, používá se v OSFP

- vytvoří graf sítě a lokálně to Dijskrtem spočítá nejkratší trasu

- oproti DVA nezatěžuje, ale vyžaduje větší výpočetní výkon

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

- přeposílání IP datagramů z jednoho zdroje skupině více koncových stanic

- jeden datagram přijde každému v cíli (všem)

1. Co je to Dijkstrův algoritmus a jak funguje?

- slouží k nalezení nejkratší cesty v [grafu](http://cs.wikipedia.org/wiki/Graf_%28teorie_graf%C5%AF%29)

- vyžaduje nezáporně označené hrany (oproti Bellman-Fordvě alg.)

- při každém průchodu cyklu se do množiny navštívených uzlů přidá právě 1 uzel

- průchodů cyklem je nejvýše tolik, kolik má graf vrcholů (uzel po průchodu uzavře)

**Algoritmus**: Zjišťujeme 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, pak tuto hodnotu změníme (snížíme) → Uzel uzavřeme

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

- počítá nejkratší cestu v ohodnoceném [grafu](http://cs.wikipedia.org/wiki/Graf_%28teorie_graf%C5%AF%29) z jednoho uzlu do dalšího, kde mohou být některé hrany ohodnoceny i záporně

**Algoritmus**: Zjišťujeme 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, pak tuto hodnotu změníme (snížíme) → Uzly neuzavíráme ihned, ale procházíme několikrát všechny uzly a upravuje postupně hodnoty vzdáleností nejkratších cest

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

RIP = Routing Information Protocol

- [směrovací protokol](http://cs.wikipedia.org/w/index.php?title=Směrovací_protokol&action=edit&redlink=1) umožňující [směrovačům](http://cs.wikipedia.org/wiki/Router) (routerům) komunikovat mezi sebou a reagovat na změny [topologie](http://cs.wikipedia.org/wiki/Topologie_s%C3%ADt%C3%AD) [poč. sítě](http://cs.wikipedia.org/wiki/Po%C4%8D%C3%ADta%C4%8Dov%C3%A1_s%C3%AD%C5%A5)

- protokol podle vektoru vzdálenosti využívající Bellman-Fordům algoritmus pro určení nejkratší cesty v síti

+ jednoduchost, ale pouze pro malé sítě, snadno konfigurovatelný

– dnes nedostačující pro velikost sítí = zahlcení, není rychlý; omezený počet přeskoků

- další algoritmy: OSPF, IGRP, IS-IS

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

OSPF = Open Shortest Path First

- [routovací](http://cs.wikipedia.org/wiki/Router) [protokol](http://cs.wikipedia.org/wiki/Protokol), provádějící změny v routovacích tabulkách na základě změny stavu v [síti](http://cs.wikipedia.org/wiki/Po%C4%8D%C3%ADta%C4%8Dov%C3%A1_s%C3%AD%C5%A5)

- výpočet nejkratších cest se provádí [Dijkstrovým algoritmem](http://cs.wikipedia.org/wiki/Dijkstr%C5%AFv_algoritmus)

- v pravidelných krátkých intervalech zvláštními zprávami (Hello) kontrolují spojení se svými sousedními routery

- při zjištění jakékoliv změny zasílá oznámení všem routerům v síti, ty si pak podle nové informace přepočítají nové cesty v síti a podle toho upraví routovací tabulky

+ rychlost získání informací o topologii, odeslání routerům a obdržení informací o jejich síti

+ možnost členit velké oblasti na menší zóny

– paměťová a výpočetní náročnost

1. Co jsou to protokoly externího směrování a kde se používají?
2. Co je to zahlcení v sítích, čím vzniká a jak se mu bráníme.

**Zahlcení** – dojde k zaplnění přenosové kapacity, začnou se plnit [vyrovnávací paměti](http://cs.wikipedia.org/wiki/Vyrovn%C3%A1vac%C3%AD_pam%C4%9B%C5%A5) (buffery)

**Důsledek**: zvětšování [latence](http://cs.wikipedia.org/wiki/Latence) (zpoždění), ztrátám [datagramů](http://cs.wikipedia.org/wiki/Datagram) nebo nemožnosti navazovat další spojení

**Obrana**: priority, plánovač sítě, upozornění na hrozící nebezpečí

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

Tunelování = technika používající pro přenos jednoho nebo více [síťových spojení](http://cs.wikipedia.org/w/index.php?title=Síťové_spojení&action=edit&redlink=1) jiné síťové spojení

Využívá – VPN (Virtuální privátní síť), HTTP, SSH

1. Co je to mobilní IP a jak funguje.

Mobile IP – komunikační protokol umožňující uživatelům mobilních zařízení přesouvat se mezi sítěmi a zachovat při tom IP

- IP zařízení komunikuje svou adresou, i když je odlišná od adresy sítě

- určuje způsob, jak mobilní uzel naváže spojení s "domácím" agentem a jak ten bude směrovat datagramy do mobilního zařízení

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

- datově orientovaný protokol, který je používán v sítích s [přepojováním paketů](http://cs.wikipedia.org/wiki/P%C5%99epojov%C3%A1n%C3%AD_paket%C5%AF) (např. [Ethernet](http://cs.wikipedia.org/wiki/Ethernet))

- 32 b dlouhá

- nezaručuje doručení a integritu, nevylučuje duplicity (to dělá TCP o vrstvu výše)

Třídy

* A – lokální (neopustí počítač) 0.0.0.0 – 127.255.255 (8 b síť, 24 b host)
* B – veřejné 128.0.0. – 191.255.255.255 (16 b síť, 16 b host)
* C – privátní (neopustí síť za router) 192.0.0.0 – 223.255.255 (24 b síť, 8 b host)
* D – multicast (skupinové směrování) 224.0.0.0 – 255.255.255.255 (32 b síť)

- nejvyšší adresa v síti = Broadcast – všesměr (... .255)

- nejnižší adresa v síti = označení celé sítě (... .0)

- 127.0.0.1 = loopback – posílání sám sobě

**Podsítě** – podmnožina sítě, menší rozsahy realizované díky masce

**Proč se zavádí** – rozdělení síťového provozu nebo členění na více nezávislých celků

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

- 3 L – síťová (linková úroveň)

Maska

- popisuje rozdělení [počítačové sítě](http://cs.wikipedia.org/wiki/Po%C4%8D%C3%ADta%C4%8Dov%C3%A1_s%C3%AD%C5%A5) do [podsítí](http://cs.wikipedia.org/w/index.php?title=Podsíť&action=edit&redlink=1)

- pomocí masky sítě [router](http://cs.wikipedia.org/wiki/Router) rozhoduje o [směrování](http://cs.wikipedia.org/wiki/Sm%C4%9Brov%C3%A1n%C3%AD) ([anglicky](http://cs.wikipedia.org/wiki/Angli%C4%8Dtina) *routing*) [IP datagramů](http://cs.wikipedia.org/wiki/IP_datagram)

- v [binárním tvaru](http://cs.wikipedia.org/wiki/Dvojkov%C3%A1_soustava) má zleva samé jedničky až do místa, kde končí číslo sítě (/8 = 1111 1111.0000 0000.0000 0000.0000 0000)

- na místě části pro číslo síťového rozhraní jsou samé nuly

Router – aktivní [síťové zařízení](http://cs.wikipedia.org/wiki/S%C3%AD%C5%A5ov%C3%A9_za%C5%99%C3%ADzen%C3%AD), které procesem zvaným [routování](http://cs.wikipedia.org/wiki/Routov%C3%A1n%C3%AD) přeposílá [datagramy](http://cs.wikipedia.org/wiki/IP_datagram) směrem k jejich cíli

Implicitní adresa směrovače – slouží ke směrování všech datagramů, pro které ve směrovací tabulce není uveden záznam, a proto je označen jako síť 0.0.0.0 s maskou 0.0.0.0, takže pro jakoukoliv cílovou IP adresu

- adresa odděluje počítač od zbytku Internetu

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

IP **→ MAC**: ARP protokol

- v situaci, kdy je třeba odeslat [IP datagram](http://cs.wikipedia.org/wiki/IP_datagram) na adresu ležící ve stejné podsíti jako odesilatel (odesílatel nezná IP)

- vyslání ARP dotazu broadcastem, identifikují se všichni účastníci lokální sítě, hledaná IP odešle ARP odpověď

- informace o MAC se ukládají do ARP cache do vypršení platnosti (ne požadavek pro každý datagram)

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

ICMP – [operační systémy](http://cs.wikipedia.org/wiki/Opera%C4%8Dn%C3%AD_syst%C3%A9m) počítačů v síti pro odesílání chybových zpráv

- programy: traceroute, ping

- princip – ICMP zpráva je zapouzdřena v IP hlavičce, datagram je odeslán, každý stroj, který přeposílá datagram hlavičku sníží o 1 (TTL), pokud klesne na 0, stroj (route) datagram zahodí a pošle chybovou zprávu

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

NAT = adresy z lokální sítě přeloží na jedinečnou adresu, která slouží pro vstup do jiné sítě

+ umožňuje připojit více počítačů na jednu veřejnou [IP adresu](http://cs.wikipedia.org/wiki/IP_adresa) – řeší se tak nedostatek přidělených veřejných IP adres

+ zvyšuje bezpečnost počítačů připojených za NATem (potenciální útočník nezná opravdovou IP adresu)

– neexistuje skutečné připojení k Internetu a tak budou fungovat jen ty aplikace, kterým to nevadí

1. Kde se používá a jak funguje protokol ARP?

**ARP protokol** – k získání [ethernetové](http://cs.wikipedia.org/wiki/Ethernet) [MAC adresy](http://cs.wikipedia.org/wiki/MAC_adresa) sousedního stroje z jeho [IP adresy](http://cs.wikipedia.org/wiki/IP_adresa)

- v situaci, kdy je třeba odeslat [IP datagram](http://cs.wikipedia.org/wiki/IP_datagram) na adresu ležící ve stejné podsíti jako odesilatel (odesílatel nezná IP)

- vyslání ARP dotazu broadcastem, identifikují se všichni účastníci lokální sítě, hledaná IP odešle ARP odpověď

- informace o MAC se ukládají do ARP cache do vypršení platnosti (ne požadavek pro každý datagram)

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

Paket odeslán na server poskytovatele připojení, server určí ideální trasu – každý paket může putovat jinou trasou, a proto je jeho součástí informace o adrese odesílatele a příjemce, dále údaje o bezchybnosti dat a pořadové číslo paketu, díky němuž se dá původní soubor poskládat do výchozí podoby, protože jednotlivé pakety jsou doručovány v různém pořadí. Cíl odpoví a celý proces běží od cíle ke mně.

1. K čemu slouží protokol BOOTP? Jak funguje?

BOOTP – aplikační služba TCP/IP, systémová pro konfiguraci systému

- statické přidělování parametrů sítě stanicím (IP, maska, brána) – tyto informace jsou na BOOTP serveru

- používal se k získání parametrů IP protokolu PC (pro nastavení parametrů pro stanice používající [TCP/IP](http://cs.wikipedia.org/wiki/TCP/IP))

- pro připojení v síti potřebujeme IP adresu, masku, adresu směrovače, adresu DNS serverů

- startující stanice (klient) vyšle dotaz "kdo jsem?" broadcastem, BOOTP server najde v tabulce podle MAC adresy příslušné údaje a odpoví

- staticky = máme jí opravdu zaregistrovanou

1. K čemu slouží protokol DHCP? Jak funguje?

DHCP – dynamicky automaticky [konfiguruje](http://cs.wikipedia.org/w/index.php?title=Konfigurace_(software)&action=edit&redlink=1) počítače připojené do [počítačové sítě](http://cs.wikipedia.org/wiki/Po%C4%8D%C3%ADta%C4%8Dov%C3%A1_s%C3%AD%C5%A5)

- DHCP server přiděluje počítačům pomocí zejména [IP adresu](http://cs.wikipedia.org/wiki/IP_adresa), [masku sítě](http://cs.wikipedia.org/wiki/Maska_s%C3%ADt%C4%9B), [implicitní bránu](http://cs.wikipedia.org/wiki/Gateway) a adresu [DNS serveru](http://cs.wikipedia.org/wiki/Domain_Name_System)

- klient zažádá o IP adresu server, který eviduje půjčenou IP a čas, do kdy ji smí klient používat, poté může být přidělena jinému klientovi

- dynamicky = platnost omezena, prodlužuje se

- nástupce BOOTP, není zpětně kompatibilní

- relay agent – v situaci, kdy existují dvě nebo více sítí oddělené směrovačem a jen jedna síť obsahuje DHCP server. V takovém případě správce na směrovači zapne relay agenta a nastaví jej tak, aby všesměrové (*broadcast*) DHCP dotazy ze sítí bez DHCP serveru přeposílal DHCP serveru. Agent k přeposílanému dotazu přidá číslo sítě a masku sítě, na které klienta zaslechl, aby DHCP server poznal, ze kterého adresního rozsahu má klientovi adresu přiřadit.

1. Co je to protokol IPv6, jaké má základní vlastnosti, kde se používá? Jak se liší od IPv4?

**IPv6** nahrazuje dosluhující protokol [IPv4](http://cs.wikipedia.org/wiki/IPv4)

- délka 128 b

- masivní rozšíření [adresního prostoru](http://cs.wikipedia.org/wiki/Adresn%C3%AD_prostor) (cca o 296)

- reakce na současný nárůst přenosových rychlostí

- náhrada pouze sítové vrstvy

- nezná broadcast a ARP protokol

**Adresy IPv6 se dělí do tří kategorií:**

* unicast adresy – individuální
* multicast adresy – skupinové
* anycast adresy – výběrové

 |globální prefix|...|rozšířená fyzická adresa|

 16 b 48 b 64 b

1. Vysvětlete princip DVA, jakým způsobem se konstruují směrovací tabulky, co je to čítání do nekonečna a jaké algoritmy se používají pro urychlení konvergence.

DVA = Distance Vector Algorithms – implementace pomocí RIP (mezi všechny uzly posílá informaci o topologii sítě, kam vedou cesty a jak jsou dlouhé

- vektor {kam, delka\_cesty, smer}

Směrovací tabulky – datová struktura uložená v [operační paměti](http://cs.wikipedia.org/wiki/Opera%C4%8Dn%C3%AD_pam%C4%9B%C5%A5) [počítače](http://cs.wikipedia.org/wiki/Po%C4%8D%C3%ADta%C4%8D) nebo [routeru](http://cs.wikipedia.org/wiki/Router) sloužící pro [směrování](http://cs.wikipedia.org/wiki/Sm%C4%9Brov%C3%A1n%C3%AD) dat procházejících [počítačovou sítí](http://cs.wikipedia.org/wiki/Po%C4%8D%C3%ADta%C4%8Dov%C3%A1_s%C3%AD%C5%A5)

- konfigurace obvykle při startu PC

Čítání do nekonečna – čítání se zacyklí a pak tabulka nekonverguje

Urychlení konvergence – split horizon, split horizon inverted

1. 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.

Servery DNS – realizují systém [doménových jmen](http://cs.wikipedia.org/wiki/Dom%C3%A9nov%C3%A9_jm%C3%A9no)

-  vzájemné převody doménových jmen a [IP adres](http://cs.wikipedia.org/wiki/IP_adresa) [uzlů sítě](http://cs.wikipedia.org/wiki/S%C3%AD%C5%A5ov%C3%BD_uzel)

- porty [TCP](http://cs.wikipedia.org/wiki/TCP)/53 i [UDP](http://cs.wikipedia.org/wiki/UDP)/53

- strom doménových jmen s jedním kořenem (kořenová doména - .), pod ním domény nejvyšší úrovně (com, edu, cz) – spravuje autoritativní DNS server

- další patra domény

**Decentralizace** – nesmí se sejít stejné doménové adresy; v hierarchii smí být pepa.cz jen 1x, subdoména franta.pepa.cz také 1x

**Elektronická pošta** – významné pokud v mailové adrese používám sudboménu (@students.zcu.cz), DNS informuje o tom, že se má přijímat na zcu.cza při případné změně jména subdomény se nic neděje

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

**ARP protokol – IP na MAC**

- přenos datagramů IP na místní směrovače, odkud jsou předávány dále na cílové adresy mimo místní síť

- protokol ARP převádí IP adresu na adresu řízení přístupu k médiím rozhraní směrovače v místní síti

- informace o MAC se ukládají do ARP cache do vypršení platnosti (ne požadavek pro každý datagram)

- postup: určení IP adresy pro předání podle směrovací tabulky, ARP zkontroluje cache a když nic nenajde, pošle ARP dotaz broadcastem a není zjištěna shoda, ale zjistí, že adresa je adresa routeru, který vysílá dotaz, tak odešle svojí MAC hostiteli; směrovač pak předá data vzdálenému počítači opět dotazem ARP, ...

1. Co víte o náhodných metodách sdílení komunikačního kanálu?

S náhodným přístupem – řešení konfliktů pomocí náhody, není garantováno, že uzel přenese určité množství dat za urč. dobu

Aloha – sdílení přenosového média mnoha účastníkům

- pokud některá ze stanic chce něco vysílat, tak prostě pošle zprávu

- pokud do určité doby (~ 2 τ) nedostane potvrzení, pošle zprávu znovu (po náhodné době)

**CSMA** – sdílený (vícenásobný) přístup s detekcí nosné vlny

- komunikační médium není rádio, ale vodič (sběrnicová síť)

- detekce nosné vlny (naslouchání) – pokud nikdo nevysílá, pak vysílám

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

Obojí – standard pro bezdrátovou komunikaci

- používají 2,4 GHz pásmo (hrozí interference s mikrovlnnými troubami, bezdrát. telefony, Bluetooth a je ohrožena bezpečnost)

- technologie využívá bezlicenčního frekvenčního pásma, proto je ideální pro budování levné, ale výkonné sítě bez nutnosti pokládky kabelů

- malý dosah, energeticky nenáročné

Wifi – LAN, zajišťuje komunikaci na spojové vrstvě

- protokol [CSMA/CA](http://cs.wikipedia.org/wiki/CSMA/CA)

- standard s dalšími doplňky pro [lokální](http://cs.wikipedia.org/wiki/Lok%C3%A1ln%C3%AD_s%C3%AD%C5%A5) [bezdrátové](http://cs.wikipedia.org/wiki/Bezdr%C3%A1tov%C3%A1_komunikace) [sítě](http://cs.wikipedia.org/wiki/Po%C4%8D%C3%ADta%C4%8Dov%C3%A1_s%C3%AD%C5%A5) (Wireless LAN, WLAN)

-  zahrnuje několik druhů modulací pro posílání radiového signálu, přičemž všechny používají stejný protokol

- dosah řádově v desítkách m, rychlejší než BT

Bluetooth – PAN, komunikace na vyšších vrstvách (až na aplikační vrstvě) – spec. protokol pro každý typ připojitelného zařízení

- protokoly LMP, L2CAP a SDP

- dosah řádově v m, pomalejší než BT

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

TCP/IP: Klient Server

 socket (typ) socket (typ)

 bind (ip, port)

 listen

 connect (ip, port) accept (socket)

 send receive

 close close

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

BOOTP – aplikační služba TCP/IP, systémová pro konfiguraci systému

- statické přidělování parametrů sítě

- používal se k získání parametrů IP protokolu PC (pro nastavení parametrů pro stanice používající [TCP/IP](http://cs.wikipedia.org/wiki/TCP/IP))

- pro připojení v síti potřebujeme IP adresu, masku, adresu směrovače, adresu DNS serverů

DHCP – dynamické přidělování parametrů sítě, nástupce BOOTP

1. Jakou funkci má relační úroveň.

Řídí výměnu dat mezi relačními vrstvami obou systémů. Řeší problémy a chyby nad přenosovými protokoly (výpadek transportního spojení, ztráta paketů). Umožňuje vytvoření a ukončení relačního spojení, synchronizaci (tvorba synchronizačních značek paketům), obnovu spojení, oznamování výjimečných stavů.

- protokoly: SSL, RPC, AppleTalk,...

+ nenáročnost na CPU, – velké režie

1. Protokol OSPF,uspořádání sítě, typy směrovačů, použitý algoritmus pro výpočet směrování, způsoby stanovení váhy spoje, princip vytváření směrovací tabulky.

OSPF = Open Shortest Path First

- [routovací](http://cs.wikipedia.org/wiki/Router) [protokol](http://cs.wikipedia.org/wiki/Protokol), provádějící změny v routovacích tabulkách na základě změny stavu v [síti](http://cs.wikipedia.org/wiki/Po%C4%8D%C3%ADta%C4%8Dov%C3%A1_s%C3%AD%C5%A5)

- váha spoje – výpočet nejkratších cest se provádí [Dijkstrovým algoritmem](http://cs.wikipedia.org/wiki/Dijkstr%C5%AFv_algoritmus)

- v pravidelných krátkých intervalech zvláštními zprávami (Hello) kontrolují spojení se svými sousedními routery

- při zjištění jakékoliv změny zasílá oznámení všem routerům v síti, ty si pak podle nové informace přepočítají nové cesty v síti a podle toho upraví routovací tabulky

+ rychlost získání informací o topologii, odeslání routerům a obdržení informací o jejich síti

+ možnost členit velké oblasti na menší zóny

– paměťová a výpočetní náročnost

Směrovací tabulky – datová struktura uložená v [operační paměti](http://cs.wikipedia.org/wiki/Opera%C4%8Dn%C3%AD_pam%C4%9B%C5%A5) [počítače](http://cs.wikipedia.org/wiki/Po%C4%8D%C3%ADta%C4%8D) nebo [routeru](http://cs.wikipedia.org/wiki/Router) sloužící pro [směrování](http://cs.wikipedia.org/wiki/Sm%C4%9Brov%C3%A1n%C3%AD) dat procházejících [počítačovou sítí](http://cs.wikipedia.org/wiki/Po%C4%8D%C3%ADta%C4%8Dov%C3%A1_s%C3%AD%C5%A5)

- konfigurace obvykle při startu PC

1. Co je to symetrické šifrování, co je to asymetrické šifrování, uveďte používané algoritmy, uveďte používané délky klíčů, oba typy algoritmů porovnejte. Co je to kryptografický kontrolní součet (hashovaní funkce), jaké má vlastnosti, kde se používá a proč, jak je dlouhý.

Symetrické šifrování = k šifrování a dešifrování jediný klíč, který je potřeba distribuovat bezpečným kanálem

* DES – klíč K 56 b, každá iterace jiný klíč Ki
* Triple DES – klíč K 112 b, E: šifrování K1, dešifrování K2, šifrování K1; D: dešifrování K1, šifrování K2, dešifrování K1
* AES – klíč 128, 196, nebo 256 b
* IDEA

Asymetrické šifrování = pro šifrování a dešifrování používají odlišné [klíče](http://cs.wikipedia.org/wiki/%C5%A0ifrovac%C3%AD_kl%C3%AD%C4%8D), neřeší problém distribuce

- šifrování veřejným klíčem, dešifrování tajným klíčem

* RSA – klíč K 1024 nebo 2048 b
	+ E: C = MP(mod N), kde N = pq (prvočísla),
	+ D: M = CS (mod N)
* DSA

Hashovací funkce – jednosměrné šifrování, není možno zpětně vytvořit původní text, výpočetně složité

- použití:

* otisk prstu dat (fingerprint)
* bezpečné ukládání hesel (linux - MD5)
* el. podpis
* kontrola integrity dat
* porovnání shodnosti obsahu kopií dat
* generování pseudonáhodných posloupností
* k rychlejšímu prohledávání tabulky

- MD5 – 16 B

- SHA – 20 B