**PB156 – Počítačové siete: súhrn otázok**

**1. Definujte propustnost, zpoždění, rozptyl a řekněte, kterého z těchto parametrů dosáhnete u Internetu nejsnáze.**

* Propustnost (bandwith) – vyjadruje max. množstvo prenesenej informácie za jednotku času (b/s a násobky) nejhlehčí ji dosáhnout na internetu
* Zpoždení (latency,delay) – čas, ktorý uplynie od odoslanie správy po jeho prijatie (typicky v ms, niekedy sa udáva RTT delay- zpoždení obojsmerného prenosu)
* Rozptyl (jitter)- kolísaní zpoždení

**2. Co je to End-to-End argument? A jaký je komplementární pojem? Uveďte jednu síťovou vlastnost, kterou je třeba zajišťovat end-to-end a jednu, kterou je potřeba zajistit oním komplementárním algoritmem.**

* End-To-End prístup (E2E)  
  Požadovanú funkcionalitu je možné zaistiť iba pomocou znalostí a prostřednictvím samotnej  
  aplikácie  
  Pokud je to možné, operace komunikačního protokolu provádět v koncových bodech  
  systému, nebo co nejblíže k nim  
  vysoká vernosť dát; data musí být stejná a nevadí zpoždění
* Hop-By-Hop prístup (HbH)  
  Opakovaním funkcionality na úrovni každého dvoubodového přenosu je možné výrazně zvýšiť  
  výkon  
  Vyžaduje uchovávanie stavovaých informácií na vnitřních prvcích sítě → limitovaná  
  škálovatelnost  
  Vhodný pre real-time aplikácie: minimalizace zpoždění, menší věrnost dat

**3. Co je signal? Co je multiplexing, ake pozname typy?**

* Signál- elektromagnetické vlnenie, ktoré sa šíri médiom
* Multiplexing- rozdelenie spoja na logické kanály kvôli lepšej efektivite, uplatnenie zejména u optických vláken a bezdrátú
  + pre analógové
    - frequency-division multiplexing (každý přenášený signál je modulován samostatným nosným signálem s unikátní nosnou frekvencí,modulované nosné signály sa poskladajú a spoločne prenesú médiom)
    - wave-division multiplexing (varianta fdm pre svetlo, rôzne farby)
  + pre digitálne
    - Time-division multiplexing (v libovolném okamžiku kanál využíva výhradně jeden vysílající (po jistou dobu), nutnosť precíznej synchronizácie)

**4. Algoritmy pristupu ku zdielanemu mediu (MAC), tri typy a uviest i priklady.**

* Funkcionalita zodpovedná za koordináciu prístupu viacerých staníc k zdieľanému prenosovému médiu (eliminácia kolízií pri vysielaní)
  + neřízený přístup
    - Aloha- stanica vysiela kedykoľvek má pripravený rámec (neefektívne)
    - CSMA/CD- stanica vysiela, keď zistí pokoj v médiu, zároveň detekuje kolízie (CD), nepoužiteľná v nevodenom médiu
    - CSMA/CA- obchádzanie kolízií (hl. v nevodenom médiu)
  + řízený přístup (stanica môže vysielať, keď k tomu získa právo, napr. Rezervace, vyzívaní, předávání příznaku)
  + multiplexově orientován přístup (sprístupnenie mplx vrstvy L1 vrstve L2, napr. TDMA,FDMA)

**5. Zakladni parametry pocitacovych siti + rozsahy hodnot v dnesnim Internetu.**

* Propoustnost (bandwidth)- vyjadruje max. množstvo prenesenej informácie za jednotku času (b/s a násobky)
* Ztrátovost (packet loss) – priemerný počet stratených paketou v určitom období v porovnaní so vš. odoslanými paketmi
* Zpoždení (delay, latency) - čas, ktorý uplynie od odoslanie správy po jeho prijatie (typicky v ms, niekedy sa udáva RTT delay- zpoždení obojsmerného prenosu)
* Rozptyl (jitter) - kolísání zpoždení

**6. ISO/OSI model: 1. az 7. vrstva: funkcie, priklady protokolov**

* Fyzická – zabezpečuje prenos bitov (transformovaných na signál (analógový/digitálny)) fyzickým médiom (vodeným/nevodeným), (Frame, Relay, PPP, FDDI,)
* Linková –zaisťuje prenos rámcov medzi dvoma komunikujúcimi uzlami (zaisťuje spoľahlivosť prenosu, ochranu pred zahlcením, riadenie prístupu k médiu), LAN-s topologie (zbernicová, kruhová, hvězdicová), Backward Learning Algorithm, Spanning Tree Algorithm, (Frame, Relay, PPP)
* Sieťová –logicky spojuje heterogénne LAN-siete, zaisťuje smerovanie paketov, fragmentuje ich, zabezpečuje adresáciu uzlov, mapuje IP adresy na fyzické, stará sa o základný monitoring siete(IPv4, ARP, ICMP, IPv6, ICMPv6)
* Transportná –zaisťuje tvorbu paketov, riadené spojenie (spojované/nespojované), adresaci portú, Reliability, a Quality of Service, zaisťuje komunikáciu konkrétnych aplikácií s voliteľou spoľahhlivosťou prenosu (na úkor rýchlosti),(UDP- rýchly, TCP-spoľahlivý)
* Relačná –v TCP IP nie je, spavuje relace (tzv. dialógy), (SSL, SDP, RPC)
* Prezenčná –konvertuje prenášané dáta do jednotného formátu(komunikace „každý s každým“/ “medzitvar“), (AFP, ASCII, NDR, LPR, XDR)
* Aplikačná –poskytuje sieťové aplikácie- rozhranie medzi užívateľom a sieťou (client-server vs. peer-to-peer/ push vs. pull/ vysoké vs. nízké nároky), (DNS, HTTP, SMTP, FTP, RTP/RTCP)

**7. Co je kódování 4B/5B a jaký má účel?**

* Uměle zavedená redundace pro zabezpečení synchronizace (a možnosti detekce chyb), kódovanie 4-bitových blokov 5-bitovými vzorkami (po sebe môžu nasledovať najviac 3 nuly)

**8. Co je a kde byste užili Forward error correction? Proč?**

* detekce chyb a snaha o jejich korekci (s využití redundance dat) vhodné pre často chybujúce médiá či médiá s veľkou latenciou (napr. Hemmingov kód)

**9. Algoritmus CRC - co to je a k čemu se využívá?**

* Cyclic Redundancy Check- garantuje silnú kontrolu (korekce 1,2-bitových aj väčšiny dávkových chýb), k postupnosti bitov sa pridá vygenerovaná postupnosť bitov (zbytok po delení M(x)/C(x)), C(x) je vhodne zvolený polynóm menšieho stupňa, M(x) je prenášaná správa

**10. Co je CSMA/CD?**

* MAC protokol neriadeného prístupu k médiu, upravená Aloha, stanica vysiela keď zistí kľud v médiu a súčasne na médiu naslúcha prípadnej kolízii (CD- collision detection), využiteľné v LAN Ethernetu, nepoužiteľné v nevodenom médiu

**11. Popíš spanning tree algoritmus.**

* Používa sa na výpočet kostry grafu: každý uzol (bridge) posiela periodicky správu (vlastná adresa, adresa koreňového mústku, vzdálenost od koreňa)
  + výber koreňového mústku-
    - po zapnutí všetky mústky prehlásia že sú koreň
    - zašlú konfiguračnú správu a na základe nej je zvolený koreňový mústek s najnižším ID
  + výber koreňových portú-
    - Každý mústek si za svoj koreňový port zvolý ten s najnižšou cenou cesty k Root Bridge
    - Ak majú 2 porty rovnakú cenu je zvolený ten s nižším ID (druhý sa vypne)
  + výber aktívnych/neaktívnych portov
    - Root Bridge nastaví všetky svoje porty ako aktívne
    - Na všetkých spojoch na ktorých nie sú root porty si sa zisťuje kto má vyššie bridge ID a ten sa vypne

**12. Uveďte základné vlastnosti protokolu IPv6. Ktoré vlastnosti oproti protokolu IPv4 považujete za najdôležitejšie?**

* Motivácia: rýchle vyčerpávanie adresného priestoru, nedostatky IPv4 (real-time aplikácie, zabezpečenie, autokonfigurácia, bez podpory mobility) –mnohé boli doimplementované
* IPv6
  + má 128 bitov (16 bajtov)
  + hexadecimálny zápis (miesto dekadického)
  + dvojice bajtov oddelené „:“
  + iba classless
  + sieťe popvisované pomocou notácie CIDR
  + nemajú broadcasty (nahradené špeciálnymi multicastmi)
  + majú anycasty- skupina príjemcov, dáta sa však doručia len jednému
  + jednoduchší fromát hlavičky- základná má pevných 40B (možnosť rozšírenia)
  + Hop Limit v IPv6 je TTL (Time To Live) v IPv4

**13. Vysvetlite, čo znamená mobilita v IPv6. Znázornite aj komunikačnú schému. Je niečo podobné u IPv4?**

* IPv6 na rozdiel od IPv4 podporuje mobilitu, a to pomocou tzv. Domácich agentov
* „každé zariadenie je niekde doma“- tam má nemennú domácu adresu, podľa toho, kde sa zariadenie v skutočnosti nachádza má dočasnú Care-of Adress
* Domáci agent je smerovač v domácej sieti, ktorý má tvralé spojenie s mobilným zariadením, sťahuje na seba datagramy smerujúce k m. zariadeniu a predáva mu ich
* Kvôli optimalizácii je možné (nie však nutné) oboznámiť tretiu stranu s aktuálnou dočasnou adresou mobilného uzlu (vyššia efektivita)

**14. Popište principy autokofigurace adres v IPv6.**

* Delí sa na:
  + Stavová- základom je server spravujúci konfiguračné parametre, ktoré na požiadanie poskytuje klientom (mechanizmus ala RARP🡪BOOTP🡪DHCP, navrhnuté v DHCPv6)
  + Bezstavová – smerovače z času na čas posielajú vš. potrebné informácie (ohlášení směrovače), nový klient počká na ohlásenie alebo si ho vyžiada a na základe ohlásenia si vypočíta vlastnú IPv6 adresu

**15. Adresovani v external sitich (Classless a Classful) + protokoly ktere vyuziva**

* V IPv6 je len Classless adresovanie, takže popisujem IPv4
* Classfull: adresný priestot má 5 tried
  + A,B,C,D,E
  + A,B,C majú 4 bajyt pevne „rozdelené“ na bajty siete (NetID (S)) a uzlov (HostID (U)) postupne S:U:U:U, S:S:U:U, S:S:S:U
  + D je vyhradené na multicast a E pre budúcu spotrebu
  + nevýhodou je plytvanie priestorom resp. nárast smerovacích tabuliek
* Classless:
  + Supernetting:
    - trojúrovňová hierarchia (sieť, podsieť, uzol)
    - napr. Rozdelenie zložiek v rámci jednej organizácie
    - zvonka sa javí ako jedna sieť (podsiete rozlíšené až na hraničnom smerovači)
  + Subnetting :
    - Spojuje niekoľko samostatných IP adries v jednu väčšiu
    - Adresy však musia susediť (musia sa zhodovať v určitom počte vyšších bajtov)
  + obe spôsoby potrebujú identifikovať počet bitov identifikujúcich sieť- požíva sa maska siete (32-bitový reťazec obsahuje 1 v bitoch odpovedajúcich sieťovej časti, píše sa dekadicky za lomítkom za IP adresou)

**16. Co je fragmentace paketu? Proc k ni dochazi? Jaky vliv ma na kvalitu prenosu dat? V jakem protokolu se s ni setkavame? Jak resi tento problem protokol, ktery fragmentaci nepovoluje?**

* Rozdeľovanie paketov na menšie celky obstarané novou hlavičkou s dĺžkou závislou na vlastnosiach a schopnostiach siete
* Dôvodom fragmentácie je, že prechádza rôznymi sieťami, ktoré majú rôzne MTU (maximum transfer Unit), čo vyjdadruje maximálnu veľkosť dát ktorá môže prejsť danou sieťou
* Stretávame sa s ňou v protokole ICMP (doprovodný k IPv4) a jeho 6-tková verzia
* IPv6 na rozdiel od IPv4 nepovoľuje fragmentáciu na vnútorných uzloch (zníženie záťaže) takže je nutné zistiť maximálnu možnú veľkosť paketov. Fragmentovať môže zdrojový uzol a defragmentovať len cieľový

**17. Jake protokoly se staraji o preklad IP adres do MAC adres a proc? Kde se preklad pouziva?**

* Aby bola možná spolupráca L3 a L2 vrstvy je potrebné mapovať IP adresy na MAC adresy, pričom mapovanie môže byť statické (tabuľka, ťažko spravovateľné) a dynamické (pomocou Adress Resolution Protocol)
* Existuje aj RARP (Reversed ARP), t.j. preklad MAC adries spätne na IP adresy, ale už sa nevyužíva

**18. Jaký problém mají řešit směrovací protokoly? Které vrstvě ISO OSI toto náleží? Popište stručně princip jednoho Vámi zvoleného směrovacího protokolu.**

* Smerovanie je proces nájdenia cesty medzi dvoma komunikujúcimi uzlami
* Protokoly definujú presné pravidlá komunikácie, formátu zpráv nesúcich smerovacie informácie pre určitý algoritmus
* Náležia k sieťovej vrstve ISO/OSI modelu (3-tia)
* Protokol RIPv1 (RIPv2-pridáva autentizáciu smerovacích informácií)
  + je hlavný predstaviteľ Distance Vektor smerovania ktoré využíva Bellman-Fordov algoritmus
  + susedné smerovače si pravidelne alebo pri topologickej zmene vymieňajú svoje kompletné smerovacie tabuľky a na základe updatov si upravuju vlastné smerovacie tabuľky (všetky informácie len svojim susedom)
  + siete sú identifikované prostredníctvom CIDR
  + metrikou je počet hopov (prenos paketov medzi dvoma susednými smerovačmi má dĺžku 1, nekonečno=16)
  + smerovače zasielajú informáciu každých 30s (alebo triggered update pri zmene stavu hrany, časový limit je 180s-potom sa detekuje chyba spojenia)
  + vhodné pre malé siete a stabilné linky, nevhodné pre redundatné siete

**19. Jaké funkce očekáváte od směrovacího algoritmu? Jakou roli ve směrovacích algoritmech mají směrovací tabulky a jak se vytvářejí?**

* Sprostredkúvajú funkcionalitu smerovania
* Proces vytvorenia a údržby smerovacích tabuliek (zahrňuje výber komunikačnej cesty)
* vlastné doručenie dát
* delenie:
  + podľa okamihu rozhodovania
    - Pri uzatváraní spojenia (vytváranie okruhu)= spojované služby, virtuálne kanály
    - Pri príchode paketu = nespojované služby, datagramy
  + poľa miesta rozhodovania
    - Jediný uzol= centralizované algoritmy
    - Všetky uzly= distribuované algoritmy
* Vlastnosti: správnosť, jednoduchosť, efektivita a škálovateľnosť (minimalizácia množstva riadiacich informácií a smerovacích tabuliek), robustnosť a stabilita (distribuovaný algoritmus), spravodlivosť, optimálnosť (podľa zvoleného kritéria)
* Smerovacia tabuľka
  + základná dátová štruktúra
  + sada ukazateľov podľa ktorých sa rozhoduje, čo urobiť s ktorým paketom
  + obdahujú cesty k prefixom (počiatočná IP adresa a blok)
  + agregácia záznamov- hľadá sa najdlhší prefix, ktorý vyhovuje požiadavkam (tzv. Longest-Prefix Match Algorithm)

**20. Centralizovane vs. distribuovane smerovani, ktere znich se pouziva v Internetu jeho vyhody, a kde by sme pouzili to druhe.**

* Centralizované
  + v sieti je RCC (Routing Control Center) ktoré zhromažďuje správy smerovačov o ich stave, informácie zanalyzuje a smerovačom pošle tabuľky
  + výhody: globálna informácia, uľahčenie práce smerovačov
  + nevýhody: zlá škálovateľnosť (vhodné len pre malé siete), pomalé, pri výpadku centra prestane aktualizoať
* Distribuované
  + smerovacie informácie si vymieňajú susedia, či malé skupiny smerovačov
  + na základe periodicity infrormácií sa vypočítavajú mapy siete (smerovačie sa musie dohodnúť na smerovacom algoritme)
  + dostatočne pružné a robustné, vhodné pre veľké siete, vaužívané v Internete

**21. Popište základní vlastnosti a princip směrovacího algoritmu Distance Vector vs. Link State**

* Distance Vector (RIPv1, RIPv2)
  + Bellman-Fordov algoritmus
  + Susedné smerovače si v pravidelných intervaloch či pri topologickej zmene vymieňajú kompletné kópie svojich smerovacích tabuliek
  + na základe obsahu prijatých update-ov si potom dopĺňajú nové informácie a inkrementujú svoje distance vector číslo (metrika udávajúca počet hopov k danej sieti)
  + t.j. *všetky informácie len svojim susedom*
  + problém: pomalá konvergencia vedie k vzniku nesprávnych udájov v smerovacích tabuľkách (vznik smerovacej slučky), riešením je delenie horizontu (smerovač neposkytuje cestu späť uzlu od ktorého sa o nej dozvedel)- problémostáva v zložitejších topológiách
  + vhodné pre malé siete a stabilné linky, nie príliš vhodné pre redundantné siete
* Link State (OSPF)
  + jednotlivé smerovače si zasielajú informácie iba o stave liniek, na ktoré sú bezprostredne pripojené
  + udržujú si tak kompletné informácie o topológii danej siete – zariadenia sú si vedomé všetkých ostatných zariadení na sieti
  + potom sa počíta najkratšia cesta
  + t.j. *informácie o svojich susedoch všetkým*
  + výhoda: zaručená rýchlosť a konvergencia, vhodné aj pre väčšie siete
  + nevýhoda: zložitejší algoritmus, väčšie nároky na CPU a pamäť smerovača

**22. Směrování a přepínání - rozdíl, na jaké vrstvě se používá, co je vhodnější kde + popis jednoho směrovacího protokolu**

* Prepínanie
  + zaisťuje switch (prepínač)
  + prebieha na druhej vrstve OSI modelu
  + využívame napr. pri práci s ATM (Asynchornious Transfer Mode) (v Lokálnej sieti)
* Smerovanie
  + zaisťuje router (smerovač)
  + Prebieha na tretej vrstve ISO modelu
  + využívame napr. pri komunikácii medzi ISP (Interner Service Provider) a firmou (v Internete)
  + Protokol RIPv1 (RIPv2-pridáva autentizáciu smerovacích informácií)
    - je hlavný predstaviteľ Distance Vektor smerovania ktoré využíva Bellman-Fordov algoritmus
    - Nepodporuje Variable Length Subnet Masking
    - susedné smerovače si pravidelne alebo pri topologickej zmene vymieňajú svoje kompletné smerovacie tabuľky a na základe updatov si upravuju vlastné smerovacie tabuľky (všetky informácie len svojim susedom)
    - siete sú identifikované prostredníctvom CIDR
    - metrikou je počet hopov (prenos paketov medzi dvoma susednými smerovačmi má dĺžku 1, nekonečno=16)
    - smerovače zasielajú informáciu každých 30s (alebo triggered update pri zmene stavu hrany, časový limit je 180s-potomsa detekuje chyb spojenia)
    - vhodné pre malé siete a stabilné linky, nevhodné pre redundatné siete

**23. Statické vs. dynamické směrování - jaký je rozdíl a co používá v Internetu. Proč?**

* Členenie podľa vytvorenia/udržovania smerovacej tabuľky
* Statické
  + administrátorom ručne editované záznamy
  + smerovač nemôže vytvárať alternatívne cesty pokiaľ sa nastavená cesta preruší
  + jednoduchší, málo flexibilný
  + vhodné pre statickú topológiu
* Dynamické
  + reaguje na zmeny v sieti
  + zložité algoritmy
  + nutnosť pravidelnej aktualizácie smerovacích tabuliek (potreba protokolu, možnosť dočasnej nekonzistencie)
  + nezaručuje poradie doručenia
  + napr. centralizované, izolované, distribuované
* V internete sa využíva dynamické distribuované smerovanie, je dostatočne pružné a robustné. Nebolo by reálne možné spravovať „manuálne“ smerovacie tabuľky takej obrovskej siete.

**24. Popíšte základné princípy smerovania multicastu protokolom Core Based Tree.**

* Source-based Tree
  + aktivita zhora, od zakladajúceho
  + periodický broadcast
  + orezávanie vetiev bez členov
  + obmedzenie šírky- TTL
  + nevýhody: réžia, záplava
  + protokoly: DVRMP (RIP), MOSPF (OSPF), PIM-DM
* Core-based Tree
  + Ustanovené jadro- body stretnutia (MP)
  + záujemca o skupinu kontaktuje MP
  + aktivita zdola od príjemcu
  + redukcia broadcastu – lepšie škáluje
  + nevýhoda: závislosť na dostupnosti jadra
  + protokoly: CBS, PIM-SM
  + CBS (Core-based Tree)
    - zdroj ako koreň budovaného stromu
    - AS (adresový priestor) rozdelený na regióny, pre každý región zvolený bod stretnutia (tzv. Rendezvous Router)
    - Uzly v prípade záujmu kontaktujú body stretnutia (budovanie stromu od listov)

**25. Čím byste hlídali rozsah šíření multicastu po síti v protokolu IPv4? Svou volbu zdůvodněte.**

* TTL
* Time To Live v souvislosti s Multicastem totiž skutečně omezuje rozsah šíření zpráv, jinými slovy, multicastové Time To Live řeší to, kam až multicast dosáhne, jestli do stejné podsítě, sítě, regionu... Podle logiky: 0 - omezeno na hostitele. 1 - omezeno na konkrétní podsíť. 32 - omezeno na konkrétní síť 64 - omezeno na konkrétní oblast. 128 - omezeno na kontinent 255 - neomezeno

**26. Je multicast v běžných IP sítích zaručená nebo nezaručená služba? Svou odpověď zdůvodněte.**

* Multicast je v bežných IP sieťach zaručená služba nakoľko multicastové adresy sú v protokole IPv4 (D) aj IPv6 (prefix ff00::/8)

**27. Jak byste zabranili pretezeni site pri multicastu v IPv4?**

* Požijem Core Based Tree, ktorý má na rozdiel od source-based tree nižšiu réžiu a nerobí záplavy

**28. Naco su autonomne systemy, ako je zabezpecene smerovanie**

* Cieľom rozdelenia Internetu na autonómne systémy je zníženie smerovacej réžie (jednoduchšie smerovacie tabuľky, zníženie množstva vymmieňaných smerovacích informácií atď.)
* Zjednodušenie správy celej siete
* Autonómne systémy = domény
  + každej doméne priradený 16-bitový identifikátor (Autonomous System Number)- priraďuje ho organizácia ICANN (Internet Corporation For Assigned Names and Numbers)
  + odpovedajú administratívnym doménam
    - Siete a smerovače uprostred jedného AS spravované spravované jednou organizáciou(napr. CESNET, PASNET)
    - Delenie v závislosti na pripojení AS do siete
      * Stub AS- pripojený len k jednému ďalšiemu AS
      * Multihomed AS- je pripojený najmenej k dvom AS, ale neumožňuje medzi nimi prenos
      * Transit AS- je pripojený najmenej k dvom ďalším AS, medzi ktroými umožnoje prenos prostredníctvom svojich LANs
* Smerovanie je oddelené kvôli škálovateľnosti (nutná splupráca)
  + interior routing (intradoménové)
    - Smerovanie vnútri AS, úplne pod kontrolou správcu AS
    - Tzv. Interior Gateway Protocols (IGP), napr. RIP, OSPF
    - Interné smerovače (vnútri AS) poznajú cestu do všetkých podsietí vnútri AS (môžu použiť implicitné-default cesty)
    - Hraničné smerovače (Bourder Routers) sumarizujú a zverejňujú interní cesty a aplikujú smerovacie pravidlá (policy)
    - Jadro siete nepoužíva implicitné cesty- smerovače musia poznať cesty ku všetkým sieťam
    - Vnútri AS hraje hlavnú rolu výkon
  + exterior routing (interdoménové)
    - Smerovanie medzi AS
    - Tzv. Exterior Gateway Protocols (EGP), napr. EGP, BGP-4
    - Medzi AS hrajú hlavnú rolu politiky (peniaze) a škálovateľnosť (veľkosť tabuliek)

**29. Pojem port. Na jaké úrovni vrstvy ISO / OSI je zaveden?**

* Adresy entit transportnej vrstvy (L4)
* Pakety obsahujú zdrojový a cieľový port (identifikácia zdrojovej a cieľovej aplikácie)
* Spolu s IP adresou tvoria jedinečnú identifikáciu aplikácie v sieti
* Port je identifikovaný 16 bitovým číslom
* Porty sú delené do troch tried organizáciou IANA
  + Well-known 0-1023 –identifikujú známu konkrétnu službu
  + Registrované 1024-49151- nie sú prideľované v IANA ale dajú sa tam registrovť
  + dynamické 49152-65535- dynamicky prideľované, hlavne ako zdrojové porty odosielacích aplikácií

**30. TTL-vlastnost v IP protokolu a k čemu se užívá? Jako maximální hodnotu může mít?**

* Súčasť hlavičky datagramu v IPv4 protokole
* TTL=Time-To-Live
* Riadenie maximálneho počtu skokov (=smerovačov) navštívených datagramom
* Odosielajúci uzol vloží číslo (približne 2 krát najväčší počet skokov medzi dvoma ľubovoľnými uzlami)
* Po prichode smerovačom TTL dekrementované (znížené) o 1
* Ak po dekrementovaní platí TTL=0 datagram je zahodený

**31. Vyuziti TTL v souvislosti s multicastem.**

* Obmedzuje rozhas šírenia správ prostredníctvom multicastu (Source-Based tree)

**32. Co je to multicast? Kde se používá?**

* Spôsob zasielania rovnakých správ (zdrojom) skupine koncových staníc (príjemcov)
* Skupina sa líši počtom členov, dynamikou, aktivitou členov, vzdialenosťou...
* Potreba zaistenia replikácie dát a ich doručenia
* Každým spojom putuje najviac jedna kópia dát (Hop-by-Hop nie End-to-End)
* Doručenie nezaručené (best effort, UDP, skupinová adresa)
* Rozsah šírenia obmedzený TTL paktov
* Dva základné prístupy sú Source-Based Tree a Core-Based Tree
* Vysielajúci: každý môže vysielať (pokiaľ má multicastovú/skupinovú adresu), vysielajúcich je premenlivý počet, môže, ale nemusí byť členom skupiny
* Prijímajúci: žiadny/jeden/viac, ktokoľvek sa môže pridať či opustiť skupinu alebo patriť do viacerých skupín súčasne
* Pozitíva: Nekonečná škálovateľnosť, nezaťažuje sieť násobnými kópiami
* Negatíva: problematické účtovanie, problém so zaistením doručenia, ľahký terč útoku, absencia kontroly členstva
* Využitie:
  + streamové video vysielané v slučke- nedfinované množstvo príjemcov, šírka pásma: jednotky Kb/s až Mb/s, kvalita prenosu
  + Dáta produkované prístrojom (napr. LHC)- definované množstvo príjemcov, veľké objemy dát po dlhú dobu, spoľahlivé doručenie
  + videokonferencia (napr. nekomprimovaná HD konferencia)- obmedzený počet príjemcov, komunikácia každý s každým, šírka pásma: stovky Kb/s až Gb/s, nízka latencia (reálny čas)

**33. Co jsou to well-known porty, uveďte jeden příklad a kdo rozhoduje o jejich rozdělení**

* Dobre známeporty- Prvá trieda portov (0-1023)
* Identifikujú známou konkrétní službu
* Prideľované okrganizáciou IANA
* Napr.
  + 17-Quote-returns a quote of the day
  + 13-Daytime-returns the day and the time
  + 9-discard-discard any datagram that is recieved (\*lecture5, p.22/85)

**34. Popište základní principy směrování multicastu pomocí protokolu Source based tree.**

* Aktivita zhora od zakladajúceho
* Periodický bradcast
* Orezávanie vetiev bez členov
* Obmedzenie šírky- TTL
* Pre úzko lokalizované skupiny
* Nevýhoda: réžia, záplava broadcastmi
* Protokoly:
  + DVMRP (Distance Vector Multicast Routing Protocol)
    - Rozšírenie unicastového DV smerovania
    - 3 prístupy budovania stromu
      * Reverse Path Forwarding (RPF)
      * Revrese Path Broadcasting (RPB)
      * Reverse Path Multicasting (RPM)
  + MOSPF (Multicast Open Shortest Path First)
    - Rozšírenie unicastového OSPF protokolu
    - Využíva znalosť topológie vytvorenú OSPF protokolom (všetky uzly počítajú strom ciest z koreňa, ktorým je zdroj multicastového vysielania)
  + PIM-DM (Protocol Independent Multicast- Dense Mode)
    - Využitie v prostredí kde je pravdepodobné, že väčšina smerovačov bude bude participovať na multicastovaní
    - Podobný DVMRP protokolu (využíva RPF prístup ale k svojej činnosti nepotrebuje unicastový protokol (t.j. RIP))

**35. Reakce TCP na ztrátu paketu - co se stane**

* TCP disponuje kontrolou toku dát
* Dáta sa nemôžu zasielať ďalej pokiaľ nebude stratený paket nájdený, znovu poslaný a prijatý
* Preto sa TCP nepoužíva pri real time prenosoch (je relatívne jedno, či sa na chvíľu sekne obraz, ale je potrebu neustále prijímať dáta)

**36. Porovnajte protokoly TCP a UDP. Ktorý z nich použijete na prenos hlasu, a prečo?**

* TCP
  + zaistennie bezchybnosti prenosu je na úkor zvýšenia end-to-end latencie
  + zaistenie férovosti nedovoľuje dostatočnú šíku pásma na vyťažených linkách
* UDP
  + najjednoduchší transportný protokol poskytujúci nepojovanú a nespoľahlivú (best effort) službu
  + nemá réžiu spojenú s overovaním (a zaisťovaním) bezchybnosti prenosu
  + minimalistický, efektívny, rychlejší, malá hlavička
  + minimálne navyšuje latenciu prenosu
  + vhodný pre prenos multimediálnych dát (prenos hlasu)
  + výhodný obzvlášť pre interaktívne prenosy
  + využívaný v drvivej väčšine prípadov (až na špeciálne výnimky)

**37. Mal by protokol TCP opodstatnenie na Internete, v prípade, že by všetky dvojbodové prenosy boli bezstratové? Zdôvodnite.**

* Áno, kvôli správnemu zoradeniu paketov a ako kontrola pred zahltením príjemcu

**38. Čo to je Flow Control? Čo je Congestion Control? Popíšte princípy obidvoch. Ako sa realizujú?**

* Flow control- mechanizmus na zábranu zahltenia prijímacej strany
  + je potrebná explicitná spätná väzba od príjemcu ktorý informuje o stave svojhu prijímacieho buffer-u (reciever window, rwnd, infomácia zasielaná v rámci ACK alebo piggibackingu). Znižujúci sa rwnd znamená zahlcovanie, rwnd=0 znamená že je treba pozastaviť vysielanie
* Congestion control- snaha o prispôsobenie rýchlosti vysielania dostupnej kapacite siete (resp. najmenšej voľnej kapacite na trase)
  + mechanizmus je závislý na dostupnosti informácií zo siete
    - Sieť dokáže informovať o blížiacom sa zahltení (napr. ATM siete)
    - Bez spätnej väzby- nutnosť odhadovať dostupnú kapacitu
  + Prístup
    - Proaktívny- predchádzanie zahlteniu
    - Reaktívny – detekcia a riešenie vzniknutého zahltenia (znížením rýchlosti vysielania)

**39. Kvalita služby pri spojovaných/nespojovaných sieťach. V ktorom type je ľahšie zabezpečiť kvalitu služby. Akú kvalitu služieb očakávate v dnešnom internete?**

* Spojované siete (= prepínanie okruhhov)
  + medzi komunikujúcimi uzlami je vopred ustanovené spojenie (nazývané tiež okruh), ktoré je udržované behom celej komunikácie
  + informácie o spojení sú udržovaná sieťou
  + sieť musí uchovávať stav okruhu (môže byť buď pevný (predvytvorený) alebo vytvorený na žiadost)
  + jednoduchá (viacemenej automatická) implementácia kvality služby
  + napr. analógové telefónne siete
* Nespojované siete (= prepínanie paketov)
  + pre prenos dát nie je využitá definovaná cesta
  + dáta sú rozdelené do malých častí (nazývaných pakety), ktoré sú odoslané do siete
  + pakety môžu byť v sieti smerované ľubovoľnými/rôznymi cestami, zlučované či fragmentované
  + na prijímajúcej strane sú z paketov extrahované príslušné časti dát, ktoré sú následne znovuzložené do pôvodnej podoby
  + nie je potreba uchovávat stav v sieti
  + veľmi problematická implementácia QoS (tzv. best-effort služba)
  + napr. Internet

**40. Popište funkci vyrovnávacích pamětí (buffer) na síti. Jaký vliv na parametry má použití vyrovnávacích pamětí?**

* Používajú sa v rámci prenosu dát pomocou TCP
* Aplikáciou predané dáta sa uchovávajú v bufferoch, kde „čakajú“ na odoslanie a taktiež sa do bufferov ukladajú prijaté dáta, ktoré čakajú na spracovanie

**41. Uveďte rozdíly mezi přenosem zvuku a videa v požadavcích na parametry přenosové sítě.**

* Zvuk – objem audio dát je relatívne malý preto nie je kompresia nie je nevyhnutná
* Video –kompresia je nevyhnutná aj keď existujú výnimky (pre účely minimalizácie end-to-end talencie je občas lepšie použiť nekomprimovaný formát napr. uncompressed HD
* Čo sa týka priepustnosti siete na audio stačí 1 Kbps-1Mbs zatiaľ čo na video treba 10´s Kbps-5Mbps
* Ani jedno nie je príliš ctilivé na stratu dát , ale za to citlivé na čas. Pre real-time audio/video je to 100´s ms zatiaľčo pre store audio/video je to pár sekúnd

**42. Popište základní vlastnosti algoritmu potvrzování zprav v TCP.**

* Acknowledgements
* Detekce ztratených (na strane príjemcu), duplikovaných a out-of-order segmentov
* Pakety sú číslované tzv. Sekvenčnými číslami (SEQ)
* pozitívne potvrdzovanie- potvrdenie úspešného prijatia paketu
* negatívne potvrdzvovanie- informácia o neúspešnom prijatí/strate paketu
* V prípade výskytu chyby sú dáta opätovne preposielané (využívané ARQ mechanizmy, musia sa vysporiadať s duplicitami)

**43. P2P siete vs. client-server, ktore je na co vhodne**

* Client-server
  + komunikácia iniciovaná klientom (klient= aplikačný program ovládaný užívateľom)
  + po ustanovení komunikačného kanálu klient zasiela požiadavky na server a ten mu odpovedá (request-response mechanzmus)
  + po ukončení komunikácie je komunikačný kanál uzavrený
  + centrlizácia zdrojov
  + valná väčšina aplikácii na Internete
  + rozlišujeme:
    - Fat user (väčšinu práce vykonáva klient)
    - Thin user (väčšinu práce vykonáva server)
  + napr. webové prehliadače, stremovanie médií
* Peer-to-Peer
  + jednotliví klienti spolu komunikujú priamo (uzly sú si rovnocenné)
  + každý uzol poskytuje svoje zdroje ostatným uzlom (decentralizácia zdrojov)
  + napr. zdieľanie súborov (Gnutella), Skype, videokonferencia, VoIP, torrenty atď.

**44. Kde sa vyuziva planovanie (scheduling), opiste fungovanie Priority Queuing**

* Všetky sieťové toky sú v TCP/IP obhospodarované ekvivalentne
* Sú prípady kedy je nevyhnutné niektoré toky uprednostniť, resp, poskytnúť im definovanú kvalitu služby (QoS) (obmedziť maximálnu možnú stratovosť, latenciu, garantovať požadovanú prenosovú rýchlosť, atp.)
* Nevyhnutné pre prenosy reálneho času (multimediálne prenosy, kritické riadiace dáta atp.)
* Plánovanie súvisú s obsluhou vstupných/výstupných front u odosielateľa, príjemcu a vnútroných sieťových prvkoch
* Štruktúra front, a manipulácia s nimi výrazne ovplyvňuje možnosti garancie oneskorenia prenosu (je nevyhnutné kombinovať aj s ďal ími prístupmi- congestion aviodance, traffic shaping)
* Prístupy k obdluhe front
  + FIFO- first-in-first-out
  + weighted fair queuing
  + Priority queuing
    - Prichádzajúce pakety sú zaradené do prioritných tried
    - Každá prioritná trieda má vlastnú frontu
    - Pakety v triede s vyššou prioritou sú obsluhované skôr
    - Výhoda: pakety s vyššou prioritou majú garantovanä prednostnú obsluhu
    - Nevýhoda: pokiaľ existuje kontinuálny tok paketov s vyššou priotitou, pakety s nižšou prioritou nebudú nikdy obslúžené (starvation)

**45. Mame 2 procesy, ktere spolu komunikuji pomoci TCP. Je nutne dodrzet nejake poradi, kdyz spolu chcou komunikovat?**

* Áno, pred začiatkom prenosu je nutnosť ustanovenia spojenia- tzv. Handshake pri ktorom si komunikujúce strany vymieňajú potrebné parametre
* Prípadne obe strany musia iniciovať spojenie- tzv. Three-way handshake (full-duplexní prenos)
* Spojenie musí byť uzavreté oboma komunikujúcimi stranami

**46. Uveďte příklady služeb a jejich přiřazení ISO-OSI modelů sítí.**

* Aplikačná- predstavuje rozhranie medzi užívateľom a sieťou
* Prezenčná- zaisťuje jednotnú prezentáciu dát u oboch komunikujúcich strán
* Relačná- spravuje ustanovené spojenia medzi komunikujúcimi aplikáciami
* Transportná- zaisťuje identifikáciu a doručenie dát medzi dvoma komunikujúcimi procesmi
* Sieťová- zaisťuje identifikáciu a doručenie dát medzi dvoma komunikujúcimi uzlami
* Linková- zaisťuje prenos dát medzi dvoma komunikujúcimi uzlami prepojenými zdieľaným médiom
* Fyzická- riadi deje v prenosovom médiu

**47. Co si představujete pod pojmem "zahlcení sítě"? Jakým způsobem byste se s tím vypořádali?**

* Keď je množstvo dát zaslaných do siete väčšie ako okno príjemncu alebo okno zahlcení (congestion window) alebo, keď rýchlosť príchodu paketov je väčšia než rýchlosť ich zpracovania resp. rýchlosť výstupu paketov je menšia než rýchlosť ich zpracovanie
* Preventívne riadením toku (proaktívny prístup) alebo keď k nemu dojde znížením rýchlosti vysielania (reaktívny prístup)

**48. Token bucket - popis a kde se používá**

* Mechanizmus na riadenie množstva a rýchlosti odosielaných paketov
* Umožňuje krátkodoé špičky (ovplyvňuje peak rate a burst size)
* Umožňuje zhromažďovanie tokenov v okamžiku nečinnosti uzlu
* Veľkos kýbličku ovplyvňuje veľkosť krátkodobých špičiek

**49. Vlastnosti algoritmu Leaky bucket, využití algoritmu**

* Mechanizmus na riadenie množstva a rýchlosti odosielaných paketov
* slúži na vyhladzovanie prenosu (ovplyvňuje average rate)
* obdoba deravého vedra, voda z neho vyteká konštantnou rýchlosťou bez ohľadu na to akou rýchlosťou priteká
* ak je kýbliček plný prichádzajúce pakety sú zahodené
* je veľmi reštriktívny (obmedzujúci)- penalizuje nečinné uzly (nedovoľuje uzlu nazhromaždiť tokeny a použiť ich pre budúci špičkový prenos)

**50. Posielanie emailov, protokoly POP3, SMTP, MIME**

* SMTP
  + štandardný mechanizmus pre posielanie elektronickej pošty
  + štruktúra
    - Envelope- adresa odosielateľa a príjemcu + ďalšie prípadné informácie
    - Message-
      * Hlavičky- definujú odosielateľa, príjemcu, predmet...
      * Telo správy- vlastná správa
* FTP (File Transfer Protocol)
  + Štandardný mechanizmsu internetu určený na prenos súborov medzi uzlami
  + oproti iným klint-server aplikáciám ustanovuje FTP-klient a FTP-server ustanovujú dve samostatné TCP spojenia
* MIME
  + je to ibe rozširujúci protokol, funguje iba so SMTP, obsahuje dodatočné hlavičky
  + povoľuje posielať správy a súbory s diakritikou

**51. Co znamena "AAA", popiste kazde A**

* Authentication (autentizace)- overenie identity užívateľa podľa toho čo pozná (meno+heslo), čo má (privátny kľúč), čím je (odltačok prsta, snímač zornice a pod.) čo vie (odpoveď na kontrolnú otázku)
* Autorization (autorizace)- oprávnenie (zamietnutie požiadavky) použiť určitú službu alebo zdroj (na základe zoznamu pre riadenie prístupu). Nasleduje po autenizácii
* Accounting (účtování)- sledovanie využívania sieťových služieb užívateľom (správa, plánovanie, účtovanie či iné účely)

**52. Proaktívna varianta TCP**

* ide o snahu predchádzať zahlteniu zatiaľ čo v reaktívnom prístupe sa zahltenie detekuje a následne rieši

**53. Ktoré parametre siete sú najdôležitejšie? Ktoré z nich by ste požadovali?**

* Najdôležitejšie vlastnoti
  + Delivery- doručenie dát správnemu príjemcovi
  + Accuracy- doručenie nepoškodených dát
  + Timeliness – doručenie dát včas
* Parametre
  + Propoustnost (bandwidth)- vyjadruje max. množstvo prenesenej informácie za jednotku času (b/s a násobky) nejhlehčí ji dosáhnout na internetu
  + Ztrátovost (packet loss) – priemerný počet stratených paketou v určitom období v porovnaní so vš. odoslanými paketmi
  + Zpoždení (delay, latency) - čas, ktorý uplynie od odoslanie správy po jeho prijatie (typicky v ms, niekedy sa udáva RTT delay- zpoždení obojsmerného prenosu)
  + Rozptyl (jitter) - kolísání zpoždení
* Požadovala by som všetky (minimalizovanie negatívnych maximalizovanie pozitívnych) plus zabezpečenie či už pomocou autentizácie, autorizácie, šifrovania pod.

**54. DNS, menný priestor**

* Služba na preklad doménových mien na IP adresy a naopak
* V počiatkoch internetu riešené pomocou host súborov (doménové meno-IPadresa) – neškálovateľné riešenie
* Menný priestor= spôsob pomenovania predmetných entít
  + Plochý
    - Mená bez akejkoľvek vnútornej štruktúry
    - Nemožnosť využiť vo veľkom systéme
  + hierarchický
    - Mená s hierarchickou vnútornou štruktúrou
    - Možnosť decentralizácie správy (prideľovania a kontroly) mien- zodpovednosť za určitú podčasť doménového mena
* Menný priestor inetnetu
  + Domain Name Space
  + varianta hierarchického usporiadania
  + štruktúra invertovaného stromu
  + maximálny počet úrovní=128
  + každeému uzlu je pridelená menovka (label=reťazec, max.63 znakov) a doménové meno (domain name= sekvencia menoviek oddelená „.“ Od daného uzlu ku koreňovému)
  + domény napr. com., edu., org., gov., (základné) cz., sk., fr., us., (národné)

**55. CIDR, NAT**

* CIDR (Classless Inter Domain Routing)
  + Konvencia popisujúca použtie IP adries, význam masiek, supernetting a subnetting
  + nahradzuje pôvodný classfull charakter IPv4 adries, adresy sa prideľujú po tzv. CIDR blokoch
  + veľkosť CIDR bloku je daná príslušnou maskou (možné veľmi dobre prispôsobovať)
  + zníženie tempa vyčerpávania adresného priestoru
  + adresy sú závislé na poskytovateľovi
    - Pôvodne boli IP adresy nezávislé na spôsobe ich pripojenia
    - Teraz poskytovateľ získava CIDR blok, ktorý rozdeľuje podľa svojho uváženia
    - Vonkajšie smerovače smerujú len na základe CIDR bloku
    - Pri zmene poskytovateľa je potrebné sieť preadresovať
* NAT (Network Adress Translation)
  + ďalší mechanizmus na zníženie tempa vyčerpávania adresného priestoru
  + Schováva vnútorné siete za jednu (niekoľko) externých adries
  + v rámci vnútornej siete možnosť využiť mnoho intených adries
  + rezervované privátne adresy, unikátne v rámci organizácie
  + vedľajší efekt: ochrana vnútornej siete
  + preklad adries prechádzajúcich sieťovým prvkom

**56. Go-back-n ARQ vs. Selective Repeat, ktoré z nich sa používa a na čo?**

* Go-back-n ARQ
  + rieši degradáciu výkonu pri Stop-and-Wait ARQ
  + vysiela viac paketov bez čakania na ich potvrdenie (vyššia efektivita)
  + pakety sú číslované zvyšujúcimi sa sekvenčnými číslami (ak sa dôjde na koniec, ide sa od znova)
  + potvrdenie paketu= ACK so sekvenčným číslom následujúceho (očakávaného) paketu (využitie tzv. Kumultívneho potvrdenia, v prípade obojstrannej komunikácie- piggybacking)
  + informácie o odoslaných/prijatých paketoch sa uchovávajú pomocou mechanizmu tzv. Sliding window (udržované na oboch stranách)
  + využité v TCP
* Selective repeat
  + rieši neefiktivitu Go-back-n ARQ pre vysoko stratové linky (kt. Zahadzuje pakety poslané mimo poradie)
  + pakety opäť číslované zvyšujúcimi sa číslami
  + rozšírenie okna príjemcu (namiesto jedného paketu ich môže pojať viac, out-of-order pakety sú bufferované)
  + potvrdenie paketu rovnako ako v predchádzajúcom
  + používa aj negative acknowledgements

**57. Detailne popis sluzby 3. vrstvy so zameranim na adresaciu a smerovanie**

**59. Analogovy vs. Digitalny signal, defekty signalu a co ich sposobuje**

* Analógový signál je spojitý v čase. Je možné ho šíriť vodičmi aj éterom (napr. Hlas, hudba)
* Digitálna signál je diskrétny v čase (mení sa skokovo). Je možné ho šíriť len vodičmi. Dáta v diskrétnych hodnotách (čísla, znaky...)
* Defekty:
  + slabnutie (útlm) –strata enrgie signálu spôspobená napr. odporom média
  + Skreslenie – strata tvaru spôsobená rozdielnou rýchlosťou šírenia signálov na rôznych frekvenciách
  + šum – vplyv cudzorodej energie (termálny šum, indukovaný šum, přeslech)

**60. Hlavicka paketu v IPv4 a IPv6**

* IPv4
  + VER- verzia IP protokolu
  + HLEN- dĺžka hlavičky IP datagramu vo 4B slovách (nevyhnutné kvoli poľu Option= premenlivádĺžka datagramu)
  + DS/TOS- (Differentiated Service/Type Of Service) triedy datagramu v rámci kvality služby, na rozlíšenie dôležitých (riadiacich, real-time) a menej dôležitých datagramov
  + Identification- pole identifikuje pôvodný datagram, ktorému fragmenty patria (t.j. fragmetny jendého datagramu majú rovnaké identifikačné číslo)
  + Flag- 3-bitová hodnota
    - 1 bit rezervovaný
    - Do-not-fragment bit- hodnota 1- datagram nesmie byť fragmentovaný
    - More-fragment bit- hodnota 1- fragment nie je posledným fragmentom (0 určuje poslený fragment daného datagramu)
  + Offset- relatívna pozícia fragmentu v pôvodnom datagrame, 13 bitov= offset max. 8191, nie je možné pokryť väčšie datagramy, jednotka offsetu stanovená na 8 B
  + \*3 predchádzajúce sa využívajú pri fragmentácii paketu
  + TTL- riadenie maximálneho počtu skokov (=smerovačov) navštívených datagramov (číslo, pri prechode smerovačom dekrementované o 1, ak sa rovná 0 datagram je zahodený )
  + Protocol- identifikácia protokolu vyššej vrstvy využívajúceho služieb IP vrstvy (nevyhnutné kvôli špecifikácii sieľového protokolu, ktorému má byť datagram doručený)
  + Header Checksum- kontrolný súčet hlavičky IP datagramu bez dát
  + Source IP Adress+Destination IP Adress- 32 bitová IPv4 adresa identifikujúca odosielajúci/prijímajúci uzol
  + Options- voliteľná súčasť IPv4 datagramu, určená hlavne pre budúce rozšírenie IPv4
  + +Data (nie súčasť hlavičky)
* IPv6- pevná veľkosť základnej hlavičky (40 B), Chcecksum je zaistený na L2 a L4, Options a fragmentačné informácie je možné zaistiť rozširujúcimi hlavičkami= t.j. nie sú súčasťou základnej hlavičky
  + VER- (Version) verzia protokolu
  + PRI- (Priority) tiež Traffic Class, priorita datagramu (zaradenie do určitej prepravnej triedy)
  + Flow Label- identifikácia prúdu datagramov od jedného odosielateľa k rovnakému cieľu s rovnakými vlastnosťami (pôvodne pre podporu aplikácií v reálnom čase, súčasne nevyužité)
  + Payload length- celková dĺžka IPv6 datagramu bez základnej hlavičky
  + Next Header- hlavička transportného protokolu alebo rozširujúca hlavička
  + Hop limit- =TTL v IPv4
  + Source/Destination Adress- IPv6 adresa zrojového/cieľového uzla
  + Payload extension headers- napr. Hop-by-hop Options (volby pro všechny), Routing (smerovanie), Fragment (fragmentácia), Encapsulating Security Payload (šifrovanie obsahu), Athentication Header (autentizácia) atď.

7)segmentace TCP  
9)protokoly na přístup k přenosovému médiu. Na které vrstvě pracují?  
10)popište 5.vrstvu  
11)ad-hoc síť  
13)plánování priority quer vs weighted fair quer