**Vypracované otázky PB156 (Počítačové sítě) ze zdejšího serveru (částečně rozšířené) a opravene**

**Doporuceni: nejdriv projit vsechny prezentace az pote tento dokument.**

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

**Propustnost:** Udává kapacitu přenosového kanálu (vyjadřuje maximální množství informace přenesené za jednotku času)

**Zpoždění:** Čas, který uplyne od odeslání zprávy zdrojovým uzlem po její přijetí na uzlu cílovém. Zahrnuje zpoždění v přenosové trase a na zařízeních, které jsou její součástí. (Někdy se také uvádí RTT delay = Round-Trip-Time delay, čas který uplyne od odeslání zprávy zdrojovým uzlem, jejím přijetím na uzlu cílovém, zpětným odesláním na zdrojový uzel až po její přijetí na zdrojovém uzlu.)

**Rozptyl = Kolísání zpoždění = Jitter:** Představuje variabilitu v doručování paketů cílovému uzlu

**Ztrátovost paketu viz 2)**

U internetu lze v dnešní době nejsnáze dosáhnout velké propustnosti (u nespojované sítě jdou pakety každý jinými cestami, takže každý můžeme jiné zpoždění, a to zvýší rozptyl).

1. **Které parametry sítě jsou nejdůležitější? Které z nich byste požadovali?**

Viz 1)

**Ztrátovost paketů:** průměrný počet ztracených paketů za určité období vyjádřený v % vzhledem k celkovému počtu přenesených paketů

Parametry záleží na typu sítě:

Aplikace pro lidské uživatele (př. internetové stránky) – může být větší ztrátovost paketů, může mít větší rozptyl, je dobrá větší propustnost

Real-time přenosy – co nejmenší zpoždění (a tedy i rozpyl), pro video a audio nevadí určitá ztrátovost (ale př. pro haptické přenosy už může být problém)

1. **Základní parametry počítačových sítí + rozsahy hodnot v dnešním Internetu?**

**Viz 1) 2)**

**Rozsahy:**

Propustnost: bezdrátové – 54Mbps, drátové 100 Mbps-několik Gbps u optiky

Rychlost: 100Mb/s – 10 Gb/s

Zpoždění: 100ms

Ztrátovost: 10^-6 <— nejak tak proste malo

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

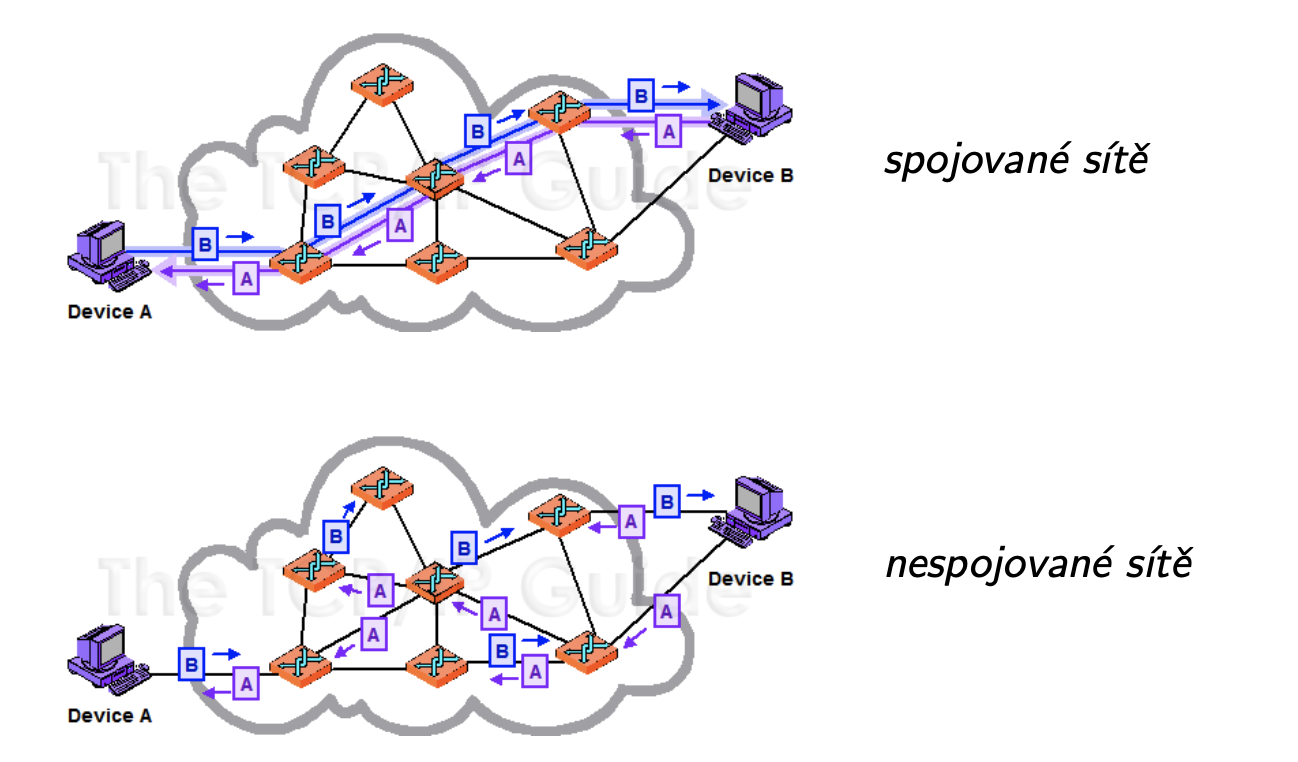
Protokol vrstvy datového spoje neřízeného přístupu k médiu. Stanice vysílá, jenom když zjistí klid v médiu, kterému naslouchá (tedy lze použít pouze ve voděném médiu). Nasloucháním na médiu také detekuje případné kolize (odtud CD = collision detection) a po její detekci vyčká náhodnou dobu a zkusí vysílat znovu. Oprotoi Aloha má jinou detekci kolizí. Aloha detekuje kolize pokud se ji nedostavi rámec, CSMA/CD naslouchá celou dobu.

1. **Kvalita služby při spojovaných/nespojovaných sítích. V kterém typu je lehčí zabezpečit kvalitu služby. Jakou kvalitu služeb očekáváte v dnešním internetu?**

**Spojované (= přepínání okruhů):** Kvalita služby je známájiž při uzavření spojení a může být předem definováno, jaká má být. Je tedy velmi jednoduché zajistit požadovanou kvalitu služby.

- Mezi komunikujícími uzly je před začátkem přenosu ustanoveno spojení, které je po dobu komunikace udržováno

* info o spojeni udržovány v síti
* okruh muze byt bud pevn´y (predvytvoreny) nebo vytvaren na zadost jednoducha (vıcemene automaticka) implementace kvality sluzby napr. analogove telefonnı sıte

**Nespojované (=přepínání paketů):**  Jelikož pakety mohou putovat každý jinou sítí, mohou se ztrácet, nemusí dorazit v pořadí v jakém byly odeslány, atd., má přenos každého paketu jiné parametry a implementace kvality služeb je velmi problematická, používá se proto tzv. best-effort služba, která nabídne takový servis, jaký zrovna může. Toto je případ dnešního internetu.

1. **Jakou funkci má portmapper?**

Kontroluje všechny porty na zařízení. Pokud přijde na některý port požadavek, zkontroluje, jestli má pro daný port přiřazenu aplikaci, pokud ano, tak ji "probudí" a předá jí ovládání tohoto portu, pokud ne, tak spojení odmítne.

1. **TTL-vlastnost v IP protokolu a k čemu se používá? Jakou maximální hodnotu může mít?**

TTL = Time-To-Live: Součást hlavičky IPv4 datagram.   
Maximální počet skoků (=směrovačů) navšívených datagramem. Odesílací uzel zde vloží číslo (cca 2 \* největší počet skoků mezi libovolnými dvěma uzly). Při každém průchodu směrovačem je tato hodnota o 1 snížena. Pokud po nějakém tomto odečtení dosáhne hodnota 0, je datagram zahozen.  
Velikost pole pro TTL v hlavičce je 8 bitů, tedy může mít maximální hodnotu 255.

Využívá se pro zamezení nekonečného putování datagramů sítí, pokud není možné datagram správně doručit – př. nevalidní adresa příjemce, zacyklení cesty, atd.

1. **Využití TTL v souvislosti s multicastem?**

Při vysílání typu multicast je nastavením různých hodnot TTL možné omezit rozsah šíření paketů, nebo zamezit nekonečnému přeposílání vadných paketů.

1. **Popište principy autokonfigurace adres v IPv6?**  
   **stavova**   
   základem server sparvující konfigurační parametry, které pak na požádání sděluje klientům. Mechanismus ala RARP -> BOOTP -> DHCP

**bezstavova**

V IPv6 se používá tzv. bezestavová konfugurace. Předpokládá se, že v síti jsou směrovače, které vědí vše potřebné. Čas od času sdělují, jaká je situace v síti tzv. ohlášením směrovače (= router advertisements), tím informují o všem potřebném (prefix sítě, implicitní směrovač, atd…). Nově příchozí klient buď čeká na ohlášení, nebo si informace aktivně vyžádá a na základě poskytnutých informací si vypočte vlastní IPv6 adresu (prefix + L2 adresa). Tuto metodu je nezbytné doplnit mechanismy pro oznamy lokálních DNS serverů.

1. **Co je kódování 4B/5B a jaký má účel + další kódování?**

**4B/5B:** Uměle zavedená redundance pro zabezpečení synchronizace včetně možnosti detekce chyb. Originální 4-bitové bloky jsou nahrazeny speciálními 5-bitovými vzorky (překlad realizován pomocí slovníku), které jsou zvoleny tak, aby ve zprávě nebyly více než tři 0 po sobě. Výsledný přenos je realizován s využitím NRZ-I. Nadbytečné bity mohou být využity pro detekci chyb (protože ne všechna slova délky 5 jsou validní kódová slova).

**Manchester:** Každý bit je kódován 2 prvky signálu, což zaručuje plnou samosynchornizovatelnost, ale za cenu snížení efektivní přenosové kapacity.

**NRZ-L:** 1 je kódována zápornou a 0 kladnou amplitudou. Žádná samosynchronizovatelnost.

**NRZ-I:** 1 je kódována změnou polarizace amplitudy, 0 žádnou změnou. Posloupnosti jedniček jsou synchonizovatelné, posloupnosti nul ne.

1. **Co je a kde byste užili Forward error detection? Proč?**

Forward Error Detection (FEC) se využívá na vrstvě datového spoje pro detekci chyb a snahu o jejich korekci (s využitím redundance dat). Je vhodné pro často chybující přenosová média nebo ty s velkou latencí (u obou není vhodné použití opakovaného přenosu), což jsou například bezdrátové sítě (kvůli chybovosti) nebo u přenosů na velké vzdálenosti (kvůli latenci). Mezi používané samoopravné kódy patří např. Hammingův kód, pro detekci chyb lze využít kontrolu parity (slabý nástroj, detekuje pouze jednobitové změny bez možnosti opravy) nebo Cyclic Redundancy Check – viz 12).

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

Cyclic Redundancy Check – slouží k možnosti detekce všech jedno- a dvoubitových a většiny dávkových chyb. Kóduje se pomocí (n, k)-kódu, kde k je blok informačních dat a n délka výsledného kódového slova (a tedy obsahuje n-k redundantních bitů). Klíčem pro kódování je polynom stupně (n-k), ten jednoznačně určuje generující matici kódu (určovaná pomocí zbytků po dělení polynomiálního vyjádření zprávy polynomem kódu). Po vynásobení matice zprávou dostaneme platné kódové slovo. Kontrola se provádí pomocí matice kontroly parity (určena jednoznačně generujícím polynomem), jejím součinem s přijatou zprávou se získá tzv. syndrom slova. Pokud je nulový, bylo přijato validní kódové slovo. Jinak lze pomocí syndromu opravit přijaté slovo na validní kódové slovo.

Je to zbytek po deleni dvou vhodne zvolených polynomů. Používá se na L2.dirs

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

**Přepínání (switching):** Používá se v linkové vrstvě. V síti (spojené linkou) je aktivní prvek (switch, bridge), který přepíná provoz mezi více připojenými segmenty součastně. Umožňuje transparentní propojení sítí, všechen provoz přes něj prochází. Odděluje sdílená média a tak zabraňuje přenášení kolizí. Adresování je založeno na MAC adresách identifikující jednotlivé stanice (resp. síťové karty) v síti. Bridge (popř. switch jakožto víceportový bridge) posílá rámce pouze do cílové adresy.

**Backward Learning Algorithm –** algoritmus, kterým se přepínací prvek učí umístění stanic nasloucháním na médiu (sleduje zdrojové adresy rámců, které jím procházejí), při průchodu rámce s cílovou adresou, kterou již viděl jako zdrojovou pošle rámec tam, odkud přišel rámec se zdrojovou adresou tohoto zařízení.

**Směrování (routing):** Proces nalezení cesty mezi dvěma komunikujícími uzly v rámci síťové vrstvy. Bere v úvahu ceny linek (př. dle kapacity, zpoždění, využití, reálné ceny, atd…). Úkolem je vyhledávání optimální směrovací trasy dle dané metriky. Zpravidla směrovač řeší úkol přístupem hop-by-hop, tedy pouze komu předat paket jako dalšímu. Aktivními prvky jsou zde směrovače (=routery), které pracují podle IP adres.

**Směrovací protokol RIP:** Představitel Distance Vector přístupu ke směrování. Sousední směrovače si v pravidelných intervalech (používá se 30 sekund) či při topologické změně vyměňují kompletní kopie svých směrovacích tabulek a na základě obsahu přijatých updatů si doplňují nové informace (a vypočítávají si cesty pomocí př. Bellman-Fordova algoritmu). Sítě jsou identifikovány s využitím mechanismu CIDR, jako metrika se používá počet hopů (kde maximum je 15, 16 odpovídá nekonečnu). Je vhodný pro použití na malých a stabilních linkách.

**Směrovací protokol OSPF:** Představitel Link State přístupu ke směrování. Jednotlivé směrovače si zasílají pouze informace o stavu linek, na něž jsou bezprostředně připojeny a tak si udržují kompletní informace o topologii dané sítě (tedy jsou si vědoma všech ostatních zařízení na síti) a poté se počítá nejkratší cesta (př. pomocí Dijkstrova algoritmu). Metrikou je cena (rozsah 1 – 65 535, menší cena, lepší metrika)

1. **Uveďte základní vlastnosti protokolu IPv6. Které vlastnosti oproti protokolu IPv4 považujete za nejdůležitější?**

Rozšířený adresní prostor: 128-bitová IPv6 má 2^128 jedinečných adres oproti 2^32 v IPv4. Pouze classless adresace, n bitů – globální směrovací prefix, 64-n bitů – adresa podsítě, 64 bitů adresa rozhraní (úvodní nuly lze z adresy vynechat).

Jednodušší formát hlavičky: Základní hlavička o pevné velikosti 40B obsahující pouze základní informace.

Možnost dalšího rozšíření: Skrze tzv. rozšiřující hlavičky.

Podpora přenosů reálného času: Skrze značkování toků a prioritizaci provozu.

Podpora zabezpečení přenosu: Podpora autentizace, šifrování a verifikace integrity přenášených dat.

Podpora mobility: Skrze tzv. domácí agenty.

Podpora autokonfigurace zařízení: stavová a bezestavová konfigurace. Viz 9).

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

Způsob síťové komunikace, kde jsou data přenášena od zdroje ke skupině příjemců (vícebodová komunikace). Je nutné zajistit replikaci (ale ne nadbytečnou) dat a jejich doručení. Každým spojem má jít nejvýše jedna kopie dat. Síť funguje jako hop-by-hop služba. Doručení je nezaručené (používá se UDP protokol jako best-effort služba se skupinovou adresou). Rozsah šíření paketů je omezen jejich TTL.

Identifikace skupinu se děje skrze multicastovou IP adresu (v IPv4 třída D, v IPv6 prefix ff00::/8).

Ke směrování multicastu existují dva základní přístupy:

**Source Based Tree:** Aktivita vychází od zakládajícího uzlu, který periodicky vysílá a ořezává větve bez členů (bez odezvy), šířka je omezena TTL, vhodné pro úzce lokalizované skupiny, kvůli záplavě broadcasty.

**Core Based Tree**: Je ustanoveno jádro s body setkání, které zájemce o skupinu kontaktuje, takže lépe škáluje ale je závislý na dostupnosti jádra.

Využívá se př. při vysílání streamovaného videa ve smyčce, při posílání velkých objemů dat produkovaných přístrojem, pro videokonference, atd…

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

Porty jsou rozdělené organizací IANA(=Internet Assigned Number Authority, dnes řízené neziskovou organizací ICANN) do 3 tříd:

Well-known (dobře známé) porty: rozsah 0-1023, identifikují konkrétní známou služby, jsou přidělovány organizací IANA.

Dále jsou to registrované porty a dynamické porty.

Př.: 20-FTP-data, 21-FTP-Control, 23-TELNET, 25-SMTP, 53-DNS, 80-HTTP

1. **Co je to End-to-End přístup? 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 (E2E):** Aplikací požadovanou funkcionalitu lze zajistit pouze se znalostí a prostřednictvím samotné aplikace (tedy na koncích přenosu). Pokud je to možné, měly by být operace komunikačního protokolu (používán př. TCP/IP) definovány tak, aby byly prováděny buď v koncových bodech komunikačního systému, nebo co nejblíže k nim. Je vhodný pro aplikace, které vyžadují vysoký stupeň věrnosti přenesených dat a součastně tolerují zpoždění.  
Vhodné pro zajištění př. služby transportní vrstvy (zajištění spolehlivosti přenosu,…), pro komunikaci aplikací (webserver - prohlížeč), ….

1. **Hop-by-hop, také komplementární pojem, uvést pro každý typ vhodnou vlastnost sítě?**

**Hop-by-Hop (HbH):** Určitá funkcionalita je opakována na každém dvoubodovém přenosu (což vyžaduje uchovávání stavových informací na vnitřních prvcích sítě a limituje škálovatelnost). Je vhodné pro aplikace, kde je minimalizace zpoždění je důležitější než věrnost přenesených dat.   
Přístup je použitý př. pro směrování paketů v rámci síťové vrstvy, pro komunikaci real-time aplikací (př. videokonference),…

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

Je zaveden na 4, tedy transportní, úrovní ISO/OSI. Používá se k adresaci služeb na této úrovni, identifikuje odesílající aplikaci na zdrojovém uzlu a aplikaci přijímající na uzlu cílovém. Pro číslování portů se používá 16bitové číslo (rozsah 0 – 65 535). Organizací IANA (viz 16).) jsou rozděleny do 3 tříd:

Well-known (= dobře známé) porty: čísla 0 – 1023, identifikují vždy konkrétní známou službu a jsou přidělovány organizací IANA.

Registrované porty: čísla 1024 – 49 151, jsou volně využitelné, ale lze je u organizace IANA zaregistrovat.

Dynamické porty: čísla 49 152 – 65 535, dynamicky přidělované porty.

Mechanismus adresace na transportní vrstvě je formou de/multiplexingu. Na odesílací straně je mnoho aplikací ale jeden transportní protokol, který odesílá data všech aplikací, proto je aplikace identifikována svým číslem zdrojového portu. Na přijímající straně je jeden transportní protokol, přijímající data všech aplikací, proto je aplikace pro doručení dat vybrána dle cílového portu.

1. **Jaké protokoly se starají o překlad IP adres do MAC adres a proč? Kde se překlad používá?**

Překlad je nutný pro zajištění hop-by-hop mechanismu doručení dat v IP síti. Vlastní dodání zprávy je na základě fyzické (MAC adresy), ale pokud je příjemce na jiné LAN než odesílatel, směrovač po přijetí datagramu jej vloží do nového rámce s MAC adresou dalšího směrovače, který jej má přiblížit cíli. Pokud je odesílatel na stejné LAN jako příjemce, je v IP datagramu IP adresa příjemce. Je tedy nutné zajistit mapování IP adres na MAC adresy. Je možné použít buď statické (s tabulkou párů adres, obtížně spravovatelné) nebo dynamické (skrze ARP protokol) mapování.

**Address Resolution Protocol (ARP):** Směrovač zašle všem uzlům na dané LAN síti ARP request paket, ten obsahuje IP a MAC adresu odesílatele a IP adresu hledaného uzlu. na paket odpoví pouze ten uzel, jehož IP adresa se shoduje s hledanou, ostatní paket zahodí, odpověď je formou ARP reply paketu. ARP pakety jsou baleny do rámců vrstvy L2 (vrstvy datového spoje), do položky pro data. Původně vysílající směrovač si zapamatuje co mu bylo odpovězeno a příště už ví, jak přeložit tuto IP adresu.

1. **Token bucket - popis a kde se používá?**

Metoda pro řízení množství a rychlosti odesílaných paketů a předcházení zahlcení sítě. Token bucket umožňuje shromažďování tokenů v okamžitu nečinnosti uzlu. Za každou přenesenou datovou buňku je z bucketu odebrát token. Dle jeho velikosti je ovlivňována velikost krátkodobých špičet. Pokud v bucketu není žádný token, je paket zahozen.

1. **Vlastnosti algoritmu Leaky bucket, využití algoritmu?**

Metoda pro řízení množství a rychlosti odesílaných paketů a předcházení zahlcení sítě, slouží k vyhlazování přenosu. Příchozí pakety jsou shromažďovány v bucketu (pokud je plný, jsou pakety zahozeny) a konstantní rychlostí jsou vypouštěny dále do sítě.

1. **Co je a čím se liší PVC (Permanent Virtual Circuit) a SVC (Switched Virtual Circuit) v protokolu ATM?**

**Asynchronous Transfer Mode (ATM):** Spojově orientovaný protokol, umožňuje jednosměrné spojení. Řeší konflikt mezi typy sítí s přepojováním okruhů a přepojováním paketů, jak bitový tak paketový tok transformuje do „buněk“ stanovené velikosti označených identifikátory virtuálního okruhu. Používá se zejména pro sdílení multimediálních informací (kvůli zajištění kvality služby).

**PVC:** Permanentní virtuální okruh – Jsou pevně zadané správcem sítě na každém ATM přepínači a existují stále, i když jimi nejsou přenášená žádná data. Umí zajistit stálou kvalitu služby, nepotřebuje adresaci, ale kvůli pevnému zadání okruhů je zde špatná škálovatelnost a udržovatelnost.

**SVC:** Přepínaný virtuální okruh – Jsou vytvářeny dynamicky na základě okamžitých potřeb (k tomu se používají signalizační protokoly). Po skončení přenosu okruh automaticky zaniká.

1. **Co je SONET, SDH**

**SONET (=Synchronous optical network):** Standard pro digitální komunikaci pomocí optických vláken. Synchronizace je pevná přes celou síť, řešené pomocí atomových hodin. Dovoluje mezistátním sítím pracovně synchronně a redukuje množství vyrovnávacích pamětí mezi jednotlivými prvky sítě.

**SDH (= Synchronious digital hierarchy):** Modernější standard vycházející ze SONETu. Oba standardy jsou dnes široce používány (SONET př. v USA a Kanadě, SHD jinde).

1. **Měl by protokol TCP opodstatnění na Internetu, v případě, že by všechny dvojbodové přenosy byly bezeztrátové. Zdůvodněte?**

TCP je protokol, jehož hlavní úkol je zajišťovat spojovanou a plně spolehlivou službu. Data budou doručena kompletní a ve správném pořadí. V hypotetické bezeztrátové síti není nutné zajišťovat kontrolu chybovosti a posílání potvrzování přijatých segmentů by přineslo množství nepotřebné redundantní informace. Použití protokolu UDP by přenosy zrychlilo.

Na druhou stranu TCP umí zajistit i kontrolu řízení toku a zahlcení sítě, které by mohly v této bezeztrátové síti stále užitečné. Také by bylo potřeba zajistit poskládání přijatých paketů do správného pořadí (což TCP umí).

1. **Co je fragmentace paketu? Proč k ní dochází? Jaký vliv má na kvalitu přenosu dat? V jakém protokolu se s ní setkáváme? Jak řeší tento problém protokol, který fragmentaci nepovoluje?**

Pakety na cestě prochází sítěmi s různými vlastnostmi, což může znamenat i rozdílné maximální velikosti dat, které lze přenést (MTU = Maximum transfer unit: maximální velikost přenositelného IP datagramu). Tento problém řeší protokol IPv4 fragmentací, kdy je původní datagram rozdělen na několik menších datagramů (tzv. fragmenty), každý z nich získá vlastní IP hlavičku a na cílovém uzlu jsou složeny do původního datagramu (k tomu se využívají pole v hlavičce: identification, flags, offset). Fragmentace se provádí na zdrojovém uzlu a na směrovačích. Skládají se pouze na cílovém uzlu. Pokud se ztratí nějaký fragment, je ztracen celý datagram (což negativně ovlivňuje kvalitu přenosu dat). Je možné provádět i fragmentaci fragmentů.

Protokol IPv6 umožňuje fragmentaci pouze na zdrojovém uzlu, nikoliv na směrovačích (což má za cíl snížit zátěž vnitřních uzlů). Zdrojový uzel potřebuje znát maximální velikost paketů platnou pro celou cestu k síti. Používá se mechanismus Path MTU Discovery, který je proveden před vlastní komunikací a využívá Packet too big chybové zprávy protokolu ICMPv6 (nastává problém s dynamickými cestami, kde je nutné při dlouhotrvajících přenosech pravidelně opakovat Path MTU Discovery)

1. **DNS, jmenný prostor?**

**Jmenný prostor:** Způsob pojmenování předmětných entit pro lepší využití uživateli. Existuje buď jako plochý jmenný prostor (jména bez vnitřní struktury, nelze použít ve větších systémech) nebo jako hierarchický jmenný prostor, kde jména sestávají s částí s definovanými významy, což umožňuje decentralizaci správy jmen.

**Jmenný prostor internetu = doménový jmenný prostor (=Domain Name Space) (DNS):** je variantou hierarchického uspořádání, který má strukturu uspořádaného stromu s maximálním počtem úrovní 128. každému uzlu je přidělena jmenovka (=label, max. 63 znaků, jmenovka kořenového je prázdný řetězec) a doménové jméno (=domain name, sekvence jmenovek od daného uzlu ke kořenovému oddělených tečkou).

**Služba DNS:** Slouží pro překlad doménových jmen na IP adresy a zpět. Dříve bylo řešeno pomocí tzv. host souborů (obsahovaly dvojice doménové jméno, adresa), což bylo neškálovatelné řešení. Nyní díky decentralizaci správy jsou jednotlivá centra zodpovědná za určité podčásti doménového jména.

**Vyhledání (př. bear.cup.ca.us.):**

Počítač se dotazuje lokálního DNS serveru na IP pro nějakou slovní adresu. Lokální sever se zeptá jednoho ze 13 kořenových (**.**). Ten mu pošle adresy o úroveň nižších serverů v adrese (**us**), lokální server se opět jednoho z nich zeptá a dostane adresy nižších serverů (**ca**), takto se postupuje dokud nedostane finální adresu cílového stroje (**bear**).

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

viz 29).

1. **ISO/OSI model: 1. až 7. vrstva: funkce, příklady protokolů?**

**ISO/OSI:** 7vrstvý model navržený organizací OSI organizací za účelem zajištění kompatibility a interoperability komunikačních systémů různých výrobců. Každá z vrstev je zodpovědná za určitou funkcionalitu a komunikuje pouze se svými přímo sousedícími vrstvami. 7 vrstev nebylo komunitou široce akceptováno a je v praxi používán TCP/IP model.

7. **Aplikační vrstva (**HTTP**,** Telnet, FTP, SMTP, SSH,...) – Účelem vrstvy je poskytnout aplikacím přístup ke komunikačnímu systému a umožnit tak jejich spolupráci.

**6. Prezentační** (SMB) – Funkcí vrstvy je transformovat data do tvaru, který používají aplikace (šifrování, konvertování, komprimace)

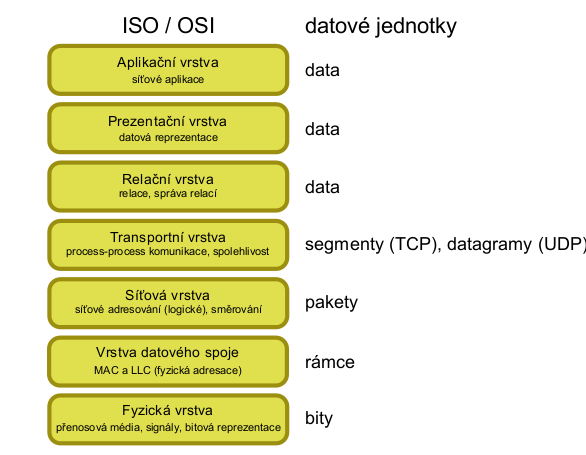
**5. Relační** vrstva – Smyslem vrstvy je organizovat a synchronizovat dialog mezi spolupracujícími relačními vrstvami obou systémů a řídit výměnu dat mezi nimi

**4. Transportní vrstva** (TCP, UDP) – Tato vrstva zajišťuje přenos dat mezi koncovými uzly. Jejím účelem je poskytnout takovou kvalitu přenosu, jakou požadují vyšší vrstvy.

**3. Síťová vrstva (**IP, ICMP) – Tato vrstva se stará o [směrování](https://cs.wikipedia.org/wiki/Sm%C4%9Brov%C3%A1n%C3%AD) v síti a síťové adresování. Poskytuje spojení mezi systémy, které spolu přímo nesousedí. **Služby:** tvorba paketů, adresace IP, směrování,...

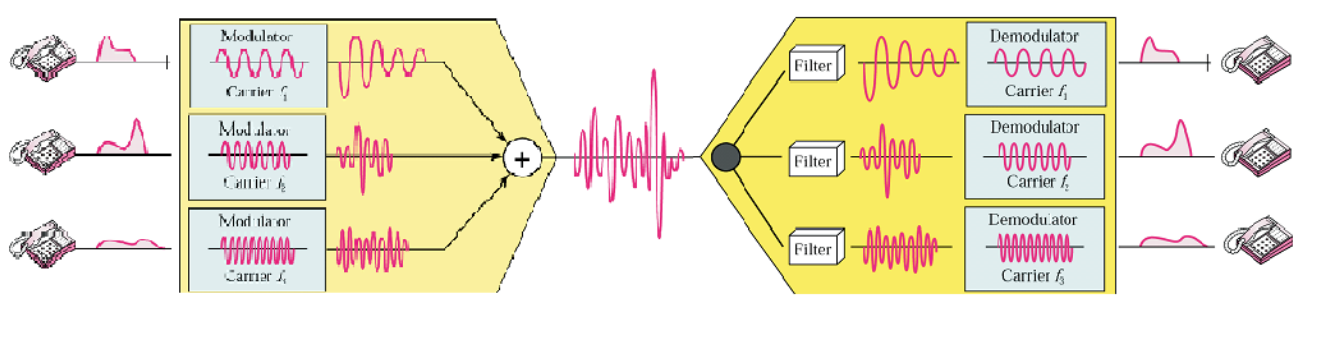
**2. Linkova vrstva** (Kontrola přístupu k médiu) – přenos dat mezi dvěma uzly a řízení přístupu. MAC adresy.

**1. Fyzická vrstva** (kabely,..) - řídí děje v médiu, kódování, nemá adresování. **Služby:** multiplexing. Bit-rate control, transformace na signál.



1. **Co je signál? Co je multiplexing, jaké existují typy?**

**Kódování**: viz. 10).

**Multiplexing**: Technika sdílení dostupné přenosové kapacity s cílem efektivnějšího využití média, uplatnitelné zejména u optických vláken a bezdrátů. 

**Časový** – Celé frekvenční pásmo se přiděluje na časový díl. Celková dosažitelná rychlost v médiu musí být větší než požadovaná rychlost pro jeden signál. Lze použít i pro přenos digitálních dat. Vyžaduje přesnou synchronizaci vysílače a přijímače. O časové díly se může soupeřit (statistický model) nebo jsou časové díly kanálům pevně přiděleny (synchronní model).

**Frekvenční** – Používaný pro analogové signály. Celé frekvenční pásmo se dělí na podpásma pro každý kanál trvale jedno. Celá šířka pásma je větší, než šířka pásma nutná pro jeden signál. Je nutné použít modulační zařízení na překlad vysílaného signálu do přiděleného podpásma, multiplexující zařízení na poskládání modulovaných signálů a opačné zařízení na straně příjmu. Musí mít ochranné odstupy mezi pásmy, plýtvá pásmem, pokud se nevysílá.

**Ortogonální frekvenční multiplex:** Signály se nejdřív rozdělí na subsignály, například na symboly a ty se přenášejí paralelně. Rychlejší než normální frekvenční multiplex.

**Wave Division** – Varianta pro optické signály. Různé frekvence světelných paprsků, kde každá barva (vlnová délka, frekvence,…) reprezentuje 1 kanál.

**Časově-frekvenční multiplexing** – Komunikující kanál dostane frekvenční podpásmo na jistý časový díl (SGM s FHSS). Lepší ochrana proti odposlechu, interferenci, vyšší rychlost přenosu než při kódovém multiplexu. Nutná přesná synchronizace.

**Kódový multiplexing** (CDMA) – Každý signál se kóduje unikátním kódem. Všechny signály používají stejné pásmo najednou. Unikátní kódování dokáže rozlišit jednotlivé kódy a ostatní chápat jako šum. Efektivně využívá šířku pásma. Není potřeba synchronizace. Nižší rychlost, horší regenerace signálu.

1. **Analogový vs. Digitální signál, defekty signálu a co je způsobuje?**

**Analogový signál** je spojitý v čase. Lze jej šířit kabelem i bezdrátem.

**Digitální signál** je diskrétní v čase. Mění se skokově 10101... Lze ho šířit pouze kabelem.

**Defekty** mohou být způsobeny slábnutím a zkreslením. Signál v médiu slábne vlivem odporu média se vzdáleností. Delší kabel – větší odpor, u bezdrátových sítí – větší vzdálenost – více slábnutí. Amplitudy signálu nejsou tak patrné, jako v původním signálu, signál může být špatně rozpoznán. Tento problém se řeší zesilovači a opakovači, které signálu vrací původní podobu.

Zkreslení je způsobeno ztrátou tvaru, to je způsobeno rozdílnou rychlostí šíření signálu o různých frekvencích, ze kterých je celkový signál složený. Signál může být zkreslen i šumem, který pochází z okolních vysílačů s podobnou frekvencí.

Vliv ostatnich signalu v okoli —> proto je kroucena dvojlinka kroucena —> eliminace sumu.

1. **Algoritmy přístupu k sdílenému médiu (MAC), tři typy a uvést i příklady?**

MAC (medium access control) odpovídá za řízení přístupu k médiu pro více stanic. Cíl je eliminovat kolize během komunikace. Protokoly mohou být, řízené, neřízené, multiplexově orientované.

**Neřízený přístup:**

**Aloha** – Stanice vysílá kdykoli má rámec k odeslání. Kolize se detekuje nepřijetím potvrzení v definovaném čase. Po kolizi se čeká náhodnou dobu a posílá se znovu. Málo efektivní, 18% využití.

**CSMA/CD** – Upravená Aloha, stanice vysílá jen, když je v médiu klid a současně naslouchá pro detekci kolize, po čemž vyčká náhodnou dobu a opakuje vysílání. Nelze použít u bezdrátu. Viz 4).

**CSMA/CA** = Collision avoidance - Obcházení kolizí. Lze použít v bezdrátu. Stanice testuje volnost média a následně vyčká ještě chvíli, než data odešle. Vyžaduje potvrzování.

**Řízený přístup (Pr. Token ring):** Stanice smí vysílat jen tehdy, když k tomu mají právo, od řídící (nebo jiné stanice). Získání práva prostřednictvím rezervace (kdy stanice vysílá v předem domluvených vyhrazených intervalech), vyzývání (centrální stanice vybírá a vyzývá stanici, která bude vysílat), předávání příznaku (stanice si předávají instanci tokenu indikujícího právo k vysílání).

**Multiplexové** viz. 30).

1. **Popiš spanning tree algoritmus?**

[LAN](https://cs.wikipedia.org/wiki/Local_Area_Network) sítích **odstraňuje smyčky**. [Switch](https://cs.wikipedia.org/wiki/S%C3%AD%C5%A5ov%C3%BD_p%C5%99ep%C3%ADna%C4%8D) s managmentem zjistí pomocí protokolu [topologii sítě](https://cs.wikipedia.org/wiki/Topologie_s%C3%ADt%C3%AD) a odpojí [redundantní](https://cs.wikipedia.org/wiki/Redundantn%C3%AD) spoje, které v síti způsobují množení [broadcastů](https://cs.wikipedia.org/wiki/Broadcast). Protokol také umožňuje automaticky aktivovat odpojené spoje v případě, kdy dojde k přerušení aktivní cesty.

Cílem algoritmu je nepoužívat některé porty můstku a zabránit cyklům v topologii sítě a množení broadcastů, funguje na vrstvě datového spoje.

Můstek (bridge, switch = víceportový můstek): Transparentní propojení sítí. Založeno na MAC adresách.

Každý můstek posílá periodické zprávy. Když dostane zprávu od souseda, upraví definici nejlepší cesty. Preferuje kořen s menší adresou, menší vzdálenost, při stejné vzdáleností menší adresu.

Nejnižší adresa se stane kořenem. Strom postupně roste, nalezené nejlepší cesty definují aktivní porty můstku. Všechny ostatní porty se vypnou.

Na začátku se všechny můstky prohlásí za kořen a rozešlou to sousedům. Kořenem se stane nejnižší adresa. Ostatní si za svůj kořen zvolí ten port s nejnižší cenou ke kořenovému můstku. Aktivní porty se postupně nastavují na ty můstky, kde je nižší adresa.

1. **Adresy v IPv4:**

Typy adres:

**Adresa site -** prvni adresa v siti

**Individuální (unicast) – identifikace jednoho síťového rozhraní.**

**Broadcast** – zaslání dat všem možným příjemcům. Posledni adresa v siti

**Multicast** – slouží pro adresaci skupiny.

Nejrozšířenější protokol síťové vrstvy. Dopravuje data přes směrovače na místo určení. Využívá IP adresování. Posílají se pakety – nespojovaná komunikace – každý může jít jinudy. Poskytuje best effort službu, nespolehlivou. Doplněn o další podpůrné protokoly: ARP, ICMP, IGMP, RARP. Problémem IPv4 bylo rychlé vyčerpávání adresního prostoru, absence zabezpečovacích mechanismů,… Vedlo ke snaze o přejítí na IPv6 (dnes se používají oba protokoly součastně).

1. **Hlavička paketu v IPv4 a IPv6?**

**IPv4:** Obsahuje verzi (4 bity), délku hlavičky (4 bity), rozlišení důležitosti (8 bitů), celkova delka (16 bitů), identifikace (16 bitů), flags (3 bity), offset fragmentace (13 bitů), ttl (8 bitů), identifikaci protokolu vyšší vrstvy (8 bitů), kontrolní součet hlavičky (16 bitů), adresu odesilatele a příjemce, volitelné pole. Po této hlavičce následují samotná data.

**IPv6: jednodušší -** Obsahuje verzi, prioritu, flow label podpora přenosu v reálném čase, payload length– délka datagramu, next header – rozšířená hlavička nebo hlavička transportního protokolu, hop limit – ttl, zdrojová adresa, cílová adresa. Celková délka základní hlavičky je 40B.

1. **Adresování v external sítích (Classless a Classful) + protokoly které využívá?**

**Classful:** historicky první metoda přidělování adres. Adresy byly rozděleny do tříd A, B, C, D, E (A: 2^7 sítí, každá 2^24 uzlů, B: 2^14 sítí, každá 2^16 uzlů, C: 2^21 sítí, každá 2^8 uzlů, D jsou multicastové adresy, E rezervovaný prostor). Adresa IP má 4 bloky s 255 možnostmi (8 bitů), celkem tedy 32 bitů. Poměr mezi 1. a 2. částí určuje kolik adres je pro adresaci sítě a kolik pro adresaci zařízení. Velmi plýtvá adresovým prostorem. Nejmenší třída musela mít 256 adres počítačů, i když jich třeba tolik nebylo připojených. Byla snaha dělit adresy jemněji, ale to vede k velkému nárůstu směrovacích tabulek.

**Používal se subnetting:** Zavádí možnost tříúrovňové hierarchie, místo dvouúrovňové. Část adresy určovala síť, další podsíť a teprve poslední část počítač. Zvenčí se jeví jako jedna síť = 1 záznam v tabulce. Podsítě rozlišuje až hraniční směrovač.

**Používal se supernetting:** Opak subnettingu. Spojuje několik samostatných IP adres v jednu. Musí ale jít o sousední adresy a musí mít obsazeny všechny bitové kombinace v síťové části.

**Pro určení která část adresy určuje co** se používá maska sítě. Obsahuje 1 v bitech, kde je adresa sítě a 0 v bitech, kde je adresa uzlu (počítače). Adresa sítě se získá jako IP adresa uzlu AND maska sítě.

**Classless (a CIDR popisující konvence použití):** Zobecnění sub/supernettingu. Zavádí zcela variabilní nastavení délky bloků v adrese (adresa sítě + maska sítě). Adresy se přiřazují hierarchicky – umožňuje agregaci směrování.

Nahrazuje přidělování adres po třídách a zavádí CIDR blok daný maskou, velikost bloku je dána příslušnou maskou (a tedy je možné velmi pružně přizpůsobovat). V důsledku jsou adresy závislé na poskytovateli, který získá CIDR blok a ten rozděluje jak chce.

1. **CIDR, NAT?**

**CIDR:** viz 36).

**NAT:**  Mechanismus pro snížení tempa vyčerpávání adresového prostoru. Určeno pro domácí použití (počítalo se s připojením přes modemy s dynamickým přidělováním adres). Současné připojení k internetu často vyžaduje trvalou alokaci adresy pro ADSL nebo kabelové připojení.

Kdyby každý počítač měl mít po zapnutí přidělenou adresu od poskytovatele, vedlo by to k častým požadavkům na přidělení adresy. NAT skrývá celou vnitřní síť za routerem pod jednu společnou IP. Vnitřní počítače rozlišuje podle portu, u příchozích paketů je vyžadována dodatečná informace kterému stroji z vnitřní sítě mají být data poslána, k tomu se využívají překladové tabulky. Zároveň představuje ochranu vnitřní sítě jako vedlejší efekt.

Muze byt i nekolik NATu za sebou.

1. **Co jsou to protokoly ARP a RARP a kde se používají?**

**ARP** je protokol síťové vrstvy pro zjištění fyzické (MAC) adresy uzlu na základě IP adresy. viz 20).

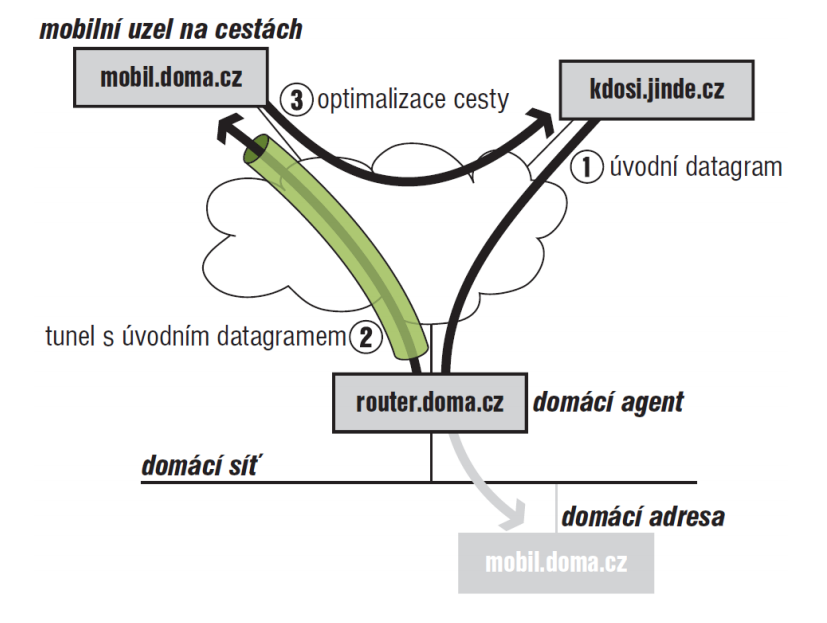
**RARP** Protokol sloužící opačně k ARP, slouží k získání IP adresy na základě znalosti MAC adresy, dnes se nepoužívá.

1. **ICMP (=Internet Control Message Protocol)?**

Jelikož IP protokol poskytuje nespolehlivou (best-effort) službu bez mechanismu pro informování odesílatele o vzniklých chybách a bez mechanismů pro zjišťování stavu sítě.

Proto byl vytvořen ICMP, který doprovází IP protokol a poskytuje informace o chybách a stavu sítě. Zprávy jsou baleny do IP protokolu (protože ICMP je protokol síťové vrstvy), v hlavičce IP je pole Protocol nastaveno na 1. ICMP se používá například na ping a traceroute (aplikace), destination unreachable, time exceeded (oznamy o chybách), etc…. ICMP používá ochranu proti rekurzivnímu generování dalších ICMP paketů. V IPv6 navíc obsahuje i funkce ARP a IGMP.

1. **Vysvětlete, co znamená mobilita v IPv6. Nakreslete i komunikační schéma. Je něco podobné u IPv4?**

Základní myšlenka: pohyblivé zařízení má nějakou domovskou síť. Zařízení má svou neměnnou domovskou adresu, pod kterou je stále dostupné, a dočasnou adresu závislou na síti, kde zrovna zařízení je. Zařízení má domácího agenta (jeden směrovač), ten na sebe stahuje data pro mobilní zařízení a předává mu je tunelem. Cesta k zařízení se může optimalizovat, aby nemusela pořád probíhat přes domácího agenta.

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

Správnost, jednoduchost, robustnost, stabilita, spravedlnost, efektivnost, optimálnost. Vybere cestu s nejlepším ohodnocením (na základě předem stanovené metriky a ohodnocení cest v síti) a s co nejmenším zpožděním. Protože žádný jednotlivý prvek internetu nezná celou strukturu sítě, a navíc se samotná struktura sama trvale mění (výpadky proudu, poškozený HW,...)., nemůžou být směrovací tabulky zadávané ručně pro každou změnu, ale počítají si je směrovače samy na základě dohodnutého směrovacího protokolu.

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

Viz 13). a 4. prezentace cele doporucuji projit znovu cca 25. slide

DV (bellman-ford) - RIP

LS (Dijkstra)- OSPF

1. **Co je směrovač, na které vrstvě pracuje, jaké má funkce, kde v Internetu se s ním setkáme?**

Směrování se odehrává na 3. (síťové) vrstvě. Spočívá v nalezení nejvýhodnější cesty mezi 2 komunikujícími uzly a dopravení paketů adresátovi. Zohledňuje se topologie sítě a zátěž. Faktory určující cenu hrany (spojení mezi směrovači) mohou být: celkový počet skoků, kapacita, zpoždění, vytíženost, reálná cena linky,...

Skrze směrovací protokoly si směrovače vytváří tabulky adres se sousedícími směrovači a podle nich se vybírá cesta, která pokud možno optimálně posune příchozí pakety k jejich cíly.

V internetu se řeší metodou hop-by-hop, kdy každý směrovač rozhoduje pouze o jednom dalším kroku v cestě paketu.

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

Viz 13.) a 43).

RIP - funguje na principu Distance vector. tj komunikuji pouze sousede a ty si vymenuji nazajem smerovaci tabulky a podle toho si je dane routery aktualizuji.

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

**Statické:** Ručně zadané záznamy do tabulky. Jednodušší, ale málo flexibilní. Vhodné pro malé sítě se statickou topologií.

**Dynamické:** Používá se na internetu. Využívá složité algoritmy, je tedy náročnější na výpočetní zdroje uzlů, přes které pakety prochází. Pravidelně aktualizuje směrovací tabulky pro případ změn v trasách. Nezaručuje pořadí doručení (pakety mohou jít různými cestami, pokud se používá přepínání paketů).

1. **Centralizované vs. distribuované směrování, které z nich se používá v Internetu jeho výhody, a kde bychom použili to druhé?**

**Centralizované:** Obsahuje centrum (routing kontrol center), které řídí směrování. Každý směrovač mu posílá zprávy o své situaci. Centrum vypočítá optimální cesty a rozešle je zpět směrovačům. Ulehčuje práci směrovačům, neobsahuje redundanci informací, ale špatně škáluje, je pomalé a náchylné na výpadek centra.

**Izolované směrování:** Neposílají se žádné informace. Každý směrovač se rozhoduje sám za sebe. Např: náhodná procházka – cesty se vybírají náhodně, záplava – paket se pošle do všech linek – enormní zátěž sítě, cesta se najde vždy, pokud existuje, mimořádně robustní.

**Distribuované:** Směrovací informace si periodicky vyměňují sousedé či malé skupiny směrovačů. Na jejich základě si budují (dle určitých algoritmů, o nichž musí být mezi směrovači dohoda) mapu sítě. Pružné a robustní – **používá se v Internetu**.

1. **K čemu jsou autonomní systémy, jak je zabezpečené směrování?**

Vzájemně propojené sítě, které spadají pod společnou správu, tvoří autonomní systém, za který odpovídá jeho provozovatel. Zvenku musí všechny systémy mít jednotné rozhraní, zevnitř nemusí. Cílem autonomních systémů je snížit směrovací režii a zjednodušit správu celé sítě.

Každému autonomnímu systému (= doméně) je přiřazen 16bitový identifikátor ASN (=Autonomous Syste, Number) (přiděluje organizace ICANN).

Autonomní systém, který je připojen pouze k jednomu dalšímu AS je nazýván stub AS.

AS který je připojen k nejméně dvěma dalším AS a neumožňuje mezi nimi přenášení provozu se nazývá multihomed AS.

AS který je připojen k nejméně dvěma dalším AS a umožňuje mezi nimi přenášení provozu se nazývá transit AS.

Směrování se dělí na vnitřní (intradoménové )a venkovní (mezidoménové). Vnitřní je plně pod správou administrátora systému, interní směrovače znají cesty do všech podsítí uvnitř AS. Venkovní používá jiné protokoly. U vnitřního jde o výkon, u venkovního o škálovatelnost a hrají zde roli politiky (a cena).

1. **Popište základní principy směrování multicastu protokolem Source Based Tree?**

Viz 15). Funguje tak, ze server odesle vsem data a odzeze ty od kterych nedostnane odpoved ze chteji dal posilat. (asi)

Aktivita shora od zakadajiciho

- Periodicky broadcast

orezavani vetvi bez clenu

omezeni sirky - ttl

pro uzce lokalizovane skupiny

nevyhoda: rezije, zaplava broadcasty

1. **Popište základní principy směrování multicastu pomocí protokolu Core based tree?**

Viz 15). Fuguje tak ze pocitace se prihlasi serveru ze chteji posilat na multicast neco. (asi)

ustanoveno jadro - body setkani (MP)

zajemce o skupinu kontaktuje MP

redukce broadcastu —> lepe se skaluje

nevyhoda: zavislot na dostupnusti jadra

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

Viz 8).

TTL

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

Viz 15).

Způsob síťové komunikace, kde jsou data přenášena od zdroje ke skupině příjemců (vícebodová komunikace). Je nutné zajistit replikaci (ale ne nadbytečnou) dat a jejich doručení. Každým spojem má jít nejvýše jedna kopie dat. Síť funguje jako hop-by-hop služba. Doručení je nezaručené (používá se UDP protokol jako best-effort služba se skupinovou adresou). Rozsah šíření paketů je omezen jejich TTL.

Identifikace skupinu se děje skrze multicastovou IP adresu (v IPv4 třída D, v IPv6 prefix ff00::/8).

1. **Jak byste zabránili přetížení sítě při multicastu v IPv4?**

Viz 15). a 8).

1. **Detailní popis služby 3. vrstvy se zaměřením na adresaci a směrování?**

Směrování viz 13). a 43)

Adresace viz 34).

Síťová vrstva obecně viz 29).

1. **Go-back-n ARQ vs. Selective Repeat, které z nich se používá a na co?**

**Stop-and-wait ARQ**: Nejjednodušší mechanismus řízení toku a chyb. Odesílající strana po odeslání paketu čeká jistou dobu na potvrzení, aniž by posílala další rámec. Po uplynutí doby (= timeout) se paket odesílá znovu. Pakety jsou číslovány střídavě 0 a 1 a potvrzení paketu (ACK) se odesílá spolu s číslem následujícího očekávaného paketu. Negativní potvrzení se nezasílá, příjemce vadné pakety zahazuje a vyčká na jejich znovu odeslání. Při obousměrné komunikaci se může potvrzení přibalit do odeslaného paketu (Piggybacking).

**Go-back-n ARQ (v protokolu TCP):** Zasílá se více paketů (řeší problém neefektivity Stop-And-Wait ARQ kde lze do sítě v 1 chvíli zaslat pouze 1 paket) bez čekání na potvrzení. Pakety se číslují sekvenčně v určitém rozmezí. Potvrzování obsahuje číslo dalšího očekávaného paketu a znamená kumulativní potvrzení všech paketů s nižším pořadovým číslem. Informace o odeslaných paketech se uchovává pomocí sliding Windows odesílatele, které má maximální velikost (2^m)-1 kde jsou pakety číslovány 0 – (2^m-1). Pakety mimo pořadí se zahazují. Není příliš efektivní, obzvlášť pro vysoce ztrátové linky.

**Selective-repeat ARQ:** Podobný jako Go-back-n ARQ, ale sliding window je i na straně příjemce, pro uchovávání paketů doručených mimo pořadí, které se ukládají a skládají později. Opět fungují kumulativní potvrzení a piggybacking. Používá i negativní potvrzování při ztrátě nějakého paketu.

1. **Porovnejte protokoly TCP a UDP. Který z nich použijete na přenos hlasu, a proč?**

**UDP:** Nejjednodušší transportní protokol poskytující nespojovanou a nespolehlivou službu, přidává pouze process-to-process komunikaci a jednoduchou kotrolu chyb. Výhodou je jednoduchost a minimální režie.

Využití: Procesy vyžadující jednoduchou komunikaci stylu dotaz – odpověď (př. DNS služba), real-time přenosy (multimediální přenosy – tedy př. hlasu), multicastové přenosy, atd…

**TCP:** Transportní protokol poskytující spojovanou a plně spolehlivou službu. Data budou doručena kompletní a ve správném pořadí. Před začátkem přenosu je nutné ustanovit spojení skrze tzv. handshake. Zajišťuje end-to-end službu pro dvoubodové plně duplexní spojení.

Využití: Procesy vyžadující spolehlivé doručování dat.

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

Služba, která vyrovnává rozdílné rychlosti komunikujících stran a mohou být využity pro řízení toku a chyb. Viz 21) a 22).

1. **Uveďte základní vlastnosti protokolu TCP. Uveďte, zda se jedná o spojovaný či nespojovaný, spolehlivý či nespolehlivý, ... protokol. Do které vrstvy ISO OSI modelu patří?**

Viz. 55).

1. **Popište základní vlastnosti algoritmu potvrzování zprav v TCP?**

TCP potřebuje detekovat poškozené a ztracené pakety. K tomu slouží kontrolní součty a potvrzování přijetí. Může se využít kumulativní potvrzování – více potvrzení naráz.

Používá Go-back-n ARQ doplněný o buffer pro out-of-order pakety.

1. **Máme 2 procesy, které spolu komunikuji pomoci TCP. Je nutné dodržet nějaké pořadí, když spolu chtějí komunikovat?**

Zahájení komunikace je definováno dle použitého protokolu. Protokol definuje formát, časování a pořadí zpráv, vyměňovaných mezi komunikujícími stranami. Před začátkem komunikace se udělá handshake, který ustanoví spojení a zahrnuje výměnu všech potřebných parametrů. U TCP se používá tzv. třícestný handshake (jedna strana pošle svůj inicializační segment, druhá ten svůj ke kterému připojí potvrzení přijetí předchozího segmentu, první strana pošle potvrzení).

Používá se potvrzování zpráv. Při obousměrné komunikaci se využívá přibalení potvrzení do odeslaného paketu s daty (piggybacking).

Ukončení je iniciováno jednou z komunikujících stran, ale musí být uzavřeno oběma (jedna strana pošle ukončovací segment, druhá potvrzení a svůj ukončovací segment, první pošle potvrzení).

1. **Reakce TCP na ztrátu paketu - co se stane?**

Po vypršení času určeného pro přijmutí zprávy potvrzující doručení dat (paketu) se data odešlou znovu. Tento čas (timeout) je založen na Round-trip-time (RTT) \* 2. RTT je čas potřebný pro cestu segmentuj odesílatele k příjemci a zpět.

1. **Co to je Flow Control? Co je Congestion Control? Popište principy obou. Jak se realizují?**

**Flow control (= řízení toku):** Řízení množství zasílaných dat tak, aby se zabránilo zahlcení příjemce. Vyžaduje zpětnou vazbu příjemce, který informuje o stavu jeho bufferu. Informace se posílá v rámci potvrzování. Pokud se buffer plní a neubývá, je nutné zpomalit přenos dalších dat.

**Congestion control (=řízení zahlcení):** Řízení množství zasílaných dat tak, aby se zabránilo zahlcení sítě. Snaha posílat tolik paketů, aby to vyhovovalo dostupné kapacitě sítě. Kapacita se musí odhadovat.

Zahlcení je stav, kdy se vstupní a výstupní fronty paketů směrovačů naplní. Další není možné přijímat. Mechanismus je závislý na dostupnosti informací ze sítě (př. ATM sítě poskytují explicitní zpětnou vazbu p blížícím se zahlcení, IP sítě potřebují umět odhadnout stav).

**Proaktivní přístup k řízení zahlcení:** Snaží se zahlcení předcházet. Kupříkladu v TCP Vegas. Tam založeno na myšlence, že se začínající zahlcování sítě projeví prodlužováním RTT a ten je v průběhu spojení monitorován a v případě jeho navyšování je navyšováno cwnd (určuje množství dat možných zaslat do sítě aniž by došlo k zahlcení).

**Reaktivní přístup k řízení zahlcení:** Detekuje zahlcení a řeší ho, a to nastavováním cwnd (různé varianty mají různé metody výpočtu).

1. **Proaktivní varianta TCP?**

Viz 61).

1. **Kde se využívá plánování (scheduling), popište fungování Priority Queuing?**

**Scheduling:** Používá se při zajišťování kvality služby. Souvisí s obsluhou vstupních a výstupních front paketů směrovačů a příjemci a odesílateli. Umožňuje garantovat zpoždění. Nutné kombinovat s dalšími technologiemi.Základní přístupy jsou FIFO, Priority Queuing, Weighted Fair Queuing,..

**FIFO:** Nejjednodušší přístup využívající pouze jednu frontu, pracuje přístupem, kdo dřív přijde, je dříve obsloužen. Nemá podporu priority a zvýhodňuje agresivní proudy.

**Priority Queuing:** Příchozí pakety jsou řazeny do prioritních tříd a pro každou třídu je vlastní fronta. Pakety vyšších tříd mají přednost. Garantuje přednostní obsluhu pro toky s vyšší prioritou, ale existuje zde možnost vyhladovění front s nižší prioritou, pokud existují kontinuální toky s vyšší prioritou.

**Weighted Fair Queuing:** Funguje podobnějako Priority Queuing, ale frontám jsou přiřazeny váhy (vyšší váha = vyšší priorita) a jsou obsluhovány mechanismem Round Robin (fronty jsou obsluhovány střídavě a čím je vyšší váha fronty, tím více paketů je z fronty odebráno).

1. **Relační vrstva, funkce, příklady protokolů?**

Smyslem relační vrstvy je organizovat a synchronizovat dialog mezi spolupracujícími systémy a řídit výměnu dat mezi nimi. Připravuje data pro vrstvy pod ní. Jedno transportní spojení může a nemusí zajišťovat více relací. Případně jedna relace může mít více transportních spojení. Není uplatněno v TCP/IP modelu.

**Řídí dialog** mezi stanicemi, určuje, která stanice může vysílat. Dialog může být plně duplexní, poloduplexní nebo simplexní. Poloduplexní režim se realizuje předáváním tokenu opravňujícího k vysílání.

**Synchronizace:** Umožňuje znovu poslat data, která sice byla v pořádku doručena, ale ztracena například výpadkem napájení. Řeší se kontrolními body, příjemce si může vyžádat na vysílacím návrat k zadanému kontrolnímu bodu.

**Protokoly:** SSL, NetBIOS, RPC, ASP

1. **Prezentační vrstva, funkce, příklady protokolů?**

Zajišťuje konverzi dat to stejného jednotného formátu. (kódování znaků, little/big Endian,...)

Prezentační vrstva může data přeložit do mezitvaru, který bude srozumitelný na druhé straně spojení. Data se popisují speciálním jazykem ASN.1. je zde nutnost domluvy na společném kontextu (definuje, jaké struktury budou přenášeny a jaká bude jejich přenosová syntaxe). Dále může zajišťovat př. šifrování a kompresi dat. Není uplatněno v TCP/IP modelu.

**Protokoly:** ASCII, EBCDIC, NDR,...

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

Stav zahlcení sítě je přesycení sítě daty, které nejsou přijímací zařízení schopné zpracovat. Předcházení zahlcení sítě se dá např pomocí tzv. Flow control (omezení velikosti posílaných dat, koordinace mezi vysílacím a přijímacím uzlem). Stanice při vysílání detekují (nebo odhadují) stav předpokládané trasy dat a následně přizpůsobuje rychlost vysílaní naměřené propustnosti.

Viz 56).

Viz 61).

1. **Klient-server vs. P2P + příklady multimediálních aplikací?**

**Client-server:** Komunikace je iniciována klientem, který ovládá uživatel. Po ustanovení komunikačního kanálu klient zasílá požadavky na server a ten mu odpovídá. Po ukončení komunikace je kanál uzavřen. Používá ho většina aplikací na internetu: WWW, FTP, DNS, SSH,...

**Existují dva typy klienta:**

**Tenký:** Aplikace na straně klienta vykonává minimum činností, většina výpočtů se chce po serveru. Velké nároky na komunikaci a výkon serveru.

**Tlustý:** Většina výpočtů na straně klienta. Menší nároky na server a komunikaci, nižší objem přenesených dat.

**Peer-to-peer:** Jednotliví klienti komunikují přímo, uzly jsou rovnocenné, každý je klient i server. Každý uzel poskytuje své zdroje (výpočetní síla, úložná kapacita, atd…) ostatním uzlům a využívá jejich zdroje

Aplikace: VoIP, Skype, sdílení souborů – př. Gnutella,...

1. **P2P sítě vs. client-server, které jsou na co vhodné?**

Viz 67).

1. **Posílání emailů, protokoly POP3, SMTP, MIME?**

**SMTP – simple mail transfer protocol**: Je internetový protokol aplikační vrstvy určený pro přenos zpráv elektronické pošty (e-mailů). Zpráva je odeslána na mail transfer agent, odkud je odeslána na mail exchange server, který ji doručí do schránky adresáta. Protokol zajišťuje doručení pošty pomocí přímého spojení mezi odesílatelem a adresátem; zpráva je doručena do tzv. poštovní schránky adresáta, ke které potom může uživatel kdykoli (off-line) přistupovat (vybírat zprávy) pomocí protokolů POP3 nebo IMAP.

Zpráva obsahuje obálku (adresa odesílatele, adresa příjemce, případné další informace) a vlastní zprávu (hlavička – definuje odesílatele, příjemce, předmět zprávy a tělo zprávy – vlatsní přenášená zpráva).

**POP3** je internetový protokol, který se používá pro stahování emailových zpráv ze vzdáleného serveru na klienta. Jedná se o aplikační protokol pracující přes TCP/IP připojení. Ze vzdáleného serveru se stáhnou všechny zprávy. Většina POP3 serverů umožňuje stáhnout i pouze hlavičky zpráv a následně vybrat zprávy, které se stáhnou celé. Tuto nevýhodu může odstranit protokol **IMAP**, který pracuje se zprávami přímo na serveru.   
**MIME** je internetový standard, který umožňuje pomocí elektronické pošty zasílat zprávy obsahující text s diakritikou, lze k ní přiložit přílohu v nejrůznějších formátech, umožňuje funkci digitálního podpisu apod. Specifikuje MIME type.  
**Popis emailové adresy: složka@server**

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

Přenos multimédií vyžaduje poměrně velké objemy přenesených dat. Klade nároky na zpoždění, chybovost, propustnost,... Jde například o streamování videa, zvuku, videokonference,...

**Nepoužívá se TCP** – vysoké zpoždění, nedovoluje dostatečnou šířku pásma. Potvrzuje pakety – zbytečnost při přenosu real-time.

**Používá se UDP** – má minimální režii, neověřuje doručení.

Přenos videa je náročnější na zpoždění, protože je potřeba zachovat minimálních 25FPS, jinak člověk pozná, že se obraz seká. Objemy dat jsou větší, lze používat komprese, ale ta může způsobovat zvyšování latence. Přenos zvuku má menší objemy dat, chybovost může být nepatrně větší. Zpoždění je opět problém obzvlášť při komunikaci (skákání si do řeči).

1. **Co znamená "AAA", popište každé A?**

Zkratka se vztahuje k bezpečnosti v počítačových sítích. Aby byla komunikace bezpečná, měla by nabízet následující služby:

**Autentizace** – ověření identity odesílatele zprávy (PIN, heslo, biometrika, token, odpověď).

**Autorizace** – udělení oprávnění nějakou službu použít na základě vyhodnocení autentizace a řízení přístupu.

**Accounting** – Účtování – sledování využívání služeb (kdo, co, kdy) za účelem správy, plánování, účtování, atd….

A **důvěrnost** – ochrana před přečtením 3. stranou (šifrování),

**integritu** – ochrana před neoprávněnou modifikací (podepisování). a **nepopíratelnost** – nepopíratelnost odeslání a přijetí pro případ potřeby důkazu..

1. **Podepisování digitálním podpisem?**

Zajišťuj integritu, nepopíratelnost a autentizaci komunikujících stran. Používá asymetrickou kryptografii. Zpráva se podepisuje soukromým klíčem a ověřuje veřejným klíčem. Podepisuje se hash dokumentu. Hash je malý konstantně dlouhý řetězec, podepisování netrvá dlouho, původní dokument se k němu přidává v nezašifrované podobě. V případě dalšího šifrování se zpráva podepisuje před zašifrováním.

1. **Asymetrická kryptografie**.

Využitím veřejného a soukromého klíče se eliminuje existence sdíleného tajemství. Používá se RSA algoritmus pro de/šifrování a algoritmus Diffie-Hellmana pro výměnu klíčů. Asymetrická kryptografie je založena na vlastnostech při počítání kongruencí modulo prvočíslo. Bezpečnost je založena na problému řešení diskrétního logaritmu, který při součastných výpočetních kapacitách nelze pro dostatečně velká prvočísla efektivně řešit. Problémem je napsání algoritmu, který by neobsahoval vedlejší cesty možného úniku informací.

1. **Rozdíly mezi CBR (Constant Bit Rate), VBR (Variable Bit Rate) a ABR (Available Bit Rate) v síti ATM.**

Rozdíl je v rychlosti přenosu dat. CBR - pevná šířka pásma, které je vyžadováno po celou dobu spojeni. V podstatě emulace pevné linky (Video, Audio,..). VBR - šířka pásma taková, jakou zrovna aplikace požaduje (komprimované video, vzdálená správa,...). ABR - šířka pásma dle aktuálních možností sítě (nevhodné pro realtime aplikace, či video streaming). UBR - nic negarantuje.

1. **Jaky je rozdíl mezi Expedited Forwarding (EF PHB) a Assured Forwarding (AF PHB)?**

EF zajišťuje nízké zpoždění, jitter a ztrátovost paketu > prioritní zpracování paketu na směrovačích. Pakety nad dohodnuty limit striktně zahazovány. Emulace virtuálního okruhu. AF zajišťuje propustnost za cenu většího jitter a zpoždění. Obsahuje 4 třídy se specifikovaným objemem prostředků, 3 důležitosti paketu v rámci každé třídy. Pozvolna indikace zahlceni.

1. **Základy protokolu, jímž v bezdrátových sítích klient vybírá přístupový bod (Access Point, AP).**

Rádiové vlny kolem 2,4 GHz. 1,2,5.5 a 11 Mb/s. Klient posle tzv Probe, všechny AP v "doslechu" pošlou Probe Response, Uzel si jeden vybere a posle Association Request, příslušný AP odpoví Association Response.

1. **Mezi doménové směrování, kde se používá. Používají se i různé nebo jen stejné protokoly směrování uvnitř domény a mezi nimi?**

Používá se na hraničních směrovačích (tj. těch, které spojují dvě různé sítě). V mezi doménovém směrování se používají protokoly EGP a BGP. Protokol EGP, cílem byla dosažitelnost, nikoli efektivita. BGP pracuje nad TCP, umožňuje definici pravidel, path vector směrování -> podobné jako distance vektor, posila vsak cele cesty a ne koncové uzly. Umožňuje definici pravidel, hledá se nejkratší cesta, nepoužívá metriku, pouze dostupnost.

1. **Vlastnosti ATM.**

Snaha vybrat nejlepší vlastnosti telefonních a datových sítí. Rozděluje data na buňky (ATM cells) 48B data, 53B celkem. Nemožný multicast. V současnosti zastaralé.

1. **Telepresence - aplikace + požadavky na síť.**
2. **Uveďte příklady telepresenčních aplikaci. Odhadnete požadavky na sít jmenovaných aplikací.**

Telekonference, televideokonference, teleimerse. Mnohonásobné různorodé proudy dat. Jde to přes UDP. Nesmí přes TCP, je nežádoucí potvrzování. Video musí být v reálném čase, aby byla možná hádka (skákání si do řeči). Velké nároky na síť - velká propustnost řádově v MB/s. Peer-to-peer, symetričnost přenosu, spojitá granularita přenosu, koncová synchronizace - reálný čas.

1. **Rozdíl mezi "dense" a "sparse" modem při šíření multicastu.**

V Dense modu router posílá data dál na všechny porty (tj. na začátku všem, postupně se počet odběratelů snižuje), v Sparse modu posila data jen tomu, kdo se přihlásí (tj. na začátku nikomu, postupně se počet odběratelů zvyšuje).

1. **Srovnejte princip přenosu paketu v IP sítích s přenosem buněk v ATM sítích.**

Pakety jdou nejlepší cestou maximální rychlosti. V ATM je stanovena max rychlost PCR (peak cell rate), střední rychlost SCR (sustained cell rate) a min rychlost MCR (minimal cell rate) a MSB (maximum burst size) což je maximální počet buněk poslaných PCR tedy nejvyšší rychlosti.