Co je to síťový protokol? Napište definici. Jak jsou protokoly standardizované? Pro jednotlivé vrstvy OSI modelu uveďte příklady protokolů.

Síťový protokol - Definuje kdo, kdy a jak komunikuje
(Definuje formát a pořadí zpráv k komunikaci a také akce které se provádí během přijímání či odesílání zpráv)

Jak jsou protokoly standardizované
De facto - někdo něco udělá a následně je to přijmuto komunitou
De juro - standardy jsou určeny vyšší autoritou (zákon, IT organizacemi - ISO, ANSI,...)

Uveďte příklady protokolů
Fyzická vrstva - IEEE 802
Vrstva datového spoje - Aloha
Transportní - IPv4, IPv6
Datová - TCP/UDP
Spojová - ASP
Prezenční - AFP
Aplikační - HTTP

Srovnejte TCP/IP a ISO/OSI model, popište funkce vrstev, protokoly a algoritmy, které se zde používají. Zdůvodněte existenci obou modelů.

TCP/IP a ISO/OSI

Podobné vlastnosti:

- Modely navržené za účelem dosažení kompatibility a intermobility komunikačních systémů vyvinutých různými výrobci
- Každá vrstva je zodpovědná za určitou funkcionality
- Vrstvy komunikují jen se sousedními vrstvami

Rozdíly:

- ISO/OSI má 7 vrstev
- TCP/IP má pouze 4 vrstvy - některé vrstvy z ISO jsou zahrnuty v jiné vrstvě

Existence ISO/OSI - konceptuální model, velmi dobře viditelné části => dobré na pochopení
Existence TCP/IP - prakticky používaný model

Funkce vrstev
Fyzická vrstva

- Ramce na frames
- End to end přenos bitů, Bit-rate control, Bit synchronization, Multiplexing

- IEEE 802
- Alg??

Vrstva datového spoje
- Pateky na rámce
- Funkce: Adresace za pomocí MAC adres, Error control, řízení toku dat, buduje lokální sítě
- Protokoly: MAC (aloha, CSMA/CD, CSMA/CA)
- Algoritmy: Spanning tree alg, Backward learning alg

Síťová vrsta:
- Segmenty na pateky
- Funkce: Routování, LAN na WAN
- Protokoly: IP, RIP, ICMP, ARP,..
- Algrotitmy: Bellman-Ford, Dijsktra

Transportní Vrstva:
- Data na segmenty
- Funkce: Zajišťuje doručení dat mezi komunikujícími entitami, QoS, flow a congestion control
- Protokoly: TCP, UDP,...
- Algoritmy: ??

Aplikační vrstva:
- Funkce: služba pro uživatele/konktrétní aplikace
- Protokoly: HTTP, FTP, SMTP
- Algoritmy: ??

Popište L2 vrstvu ISO/OSI modelu, adresaci na této vrstvě, funkci vrstvy, protokoly a případně algoritmy, které se zde používají.

Popis:
Je to vrstva datového spoje.
Převádí pateky na rámce.
Zajišťuje detekci a opravu chyb (*Request for Retransmision*, *Forward error correction*)
Zajišťuje řízení toku dat za účelem vyvarování se přetížení (Aloha, CSMA/CD, CSMA/CA)
Umožňuje budovat LAN se systematickou topologií

Adresace:
Adresuje se za pomocí MAC adres (přiřazené výrobcem), Rámce obsahují zdrojovou a cílovou adresu.

Protokoly:
Aloha, CSMA/CD, CSMA/CA

Algoritmy:
Backward learning alg, Distrubuted spanning tree alg

L3 vrstva, účel, funkce, způsob adresace, protokoly, algoritmy protokolů.

L3 vrstva - Síťová vrstva

Funkce:
- Převádí segmenty na packety
- Spojuje LAN na WAN
- Fragmentace paketů v případě malého MTU
- Jedinečná adresace v rámci celého internetu
- Routování paketů skrze síť

Adresace:
- Za pomocí unikátní IP adresy (IPv4, IPv6)
- Paket obsahuje zdrojovou a cílovou adresu
- Pakety se posílají internetem za pomocí protokolů jenž vybírají uzly pro přenos
- Protokoly jsou vybrány na základě vlastností sítě (dynamických a statických)

Protokoly:
- IPv4, IPv6 - adresovací protokoly
- ICMPv4, ICMPv6 - control protokoly
- RIPv1, RIPv2, OSPF - směrovací protokoly

Algoritmy:
- Distance vector (Bellman-Ford) pro RIP(v2)
- Link state (Dijksta) pro OSPF

Co je IP multicast, jaký L4 protokol využívá; vytváření multicastových skupin (+ protokoly).

IP multicast:
- Je to identifikace skupiny zařízení, která požadují data
- Přes každý síťový spoj putuje jenom jedna kopie dat
- Best effort
- Omezeno pomocí TTL
- v IPv6 má prefix ff00::/8

Protokol:
- UDP - best efford,

Vytváření skupin:
- Source based tree
    - Aktivita shora dolů
    - Periodický broadcast
    - Ořezávání větví bez členů
    - Protokoly: DVMRP, MOSPF
- Shared tree
    - Aktivita zdola nahoru

    - Je ustanoven bod setkání
    - Zájemce o data kontaktuje bod setkání
    - Redukce broadcastu - lepší škálovatelnost
    - Bod setkání je single point of failure
    - Protokoly: CBT

Bezpečnost v IPv6, způsob zabezpečení, schéma.

Authentization protokol
Encryption protokol
Key management

Authentizacion header:

- Autentizace paketu nebo její části
- Musí být ustanoveno Security Association (aby výpočet byl schopen provést pouze zdrojový a cílový uzel)
- Provede se výpočet (hash) nad tady v datagramu
- Výsledek se uloží do hlavičky paketu
- Cílový uzel provede stejný výpočet a porovná jej s výsledkem v hlavičce

Encryption Security payload:

- Zajišťuje důvěrnost dat
- Zašifruje data
- Do IP paketu vloží:
    - ESP header - obsahuje dvě pole
    - Zašifrované data
    - ESP Authentication data - Integrity check
    - ESP Trailer - určuje konec zašifrovaných dat

Hlavičky datagramu v IPv6; typy adres. Uveďte příklad IPv6 adresy a pravidla pro zkracování.

Hlavička obsahuje:

- Verze
- Traffic class - priorita paketu
- Flow label - na označení paketů se stejným flow (QoS)
- Délka dat - délka IP datagramu bez hlavičky
- Next header - definuje hlavičku následující po IP hlavičce
- Hop limit - TTL
- Zdrojová a cílová adresa - 128 bitů na každou adresu

Typy adres:

- Unicast - identifikace jednoho zařízeni
- Multicast - identifikace skupiny zařízení
- Anycast - identifikace skupiny zařízení kde data dostává pouze první

Příklad IPv adresy:

- 2001:f00a:0000:0000:0000:0000:0000:dbb4

Zkracování:

- V rámci čtveřice vynecháváme nuly z leva
    - :0042: -> :42:
- V rámci celé adresy vynecháváme maximálně jednu posobě jdoucí n-tici obsahující 0000
    - 2001:f00a:0000:0000:0000:00aa:0000:dbb4 -> 2001:f00a::00aa:0000:dbb4

Jaké jsou rozdíly mezi tvorbou hlavičiek v IPv4 a IPv6? Jak je v IPv6 řešená v hlavičce fragmentace datagramu?

Rozdíly hlaviček:

- IPv6 má pevně danou délku hlavičky (40B)
- IPv4 má navíc checksum, options, fragmentation info

Fragmentace:

- Fragmentace je možná za pomocí extension headers

Jak je řešena koexistence IPv4 a IPv6? Vypište tři základní způsoby řešení a podrobně je popište.

Koexistence je řešení třemi základními způsoby:

- Dual stack:
    - zařízení je schopno podporovat obě hlavičky zároveň
    - Výhody:
        - Jakmile bude IPv4 depricated, tak stačí jenom odebrat zpracovávání IPv4
        - Jednoduché a flexibilní
    - Nevýhody:
        - Musí zároveň běžet dva stacky protokolů - vyšší nároky na zdroje
        - Směrovací protokol se musí vypořádat s oběma protokoly
        - Všechny aplikace musí být schopny rozhodnout, zdali host komunikuje s IPv4 nebo IPv6
- Tunelování:
    - IPv6 datagramy jsou zapouzdřeny do IPv4
    - Výhody:
        - Je možné používat IPv4
        - Po deprikaci IPv4 pouze odebereme tunelování
    - Nevýhody:
        - Dodatečná zátěž na routery
        - Problémy s fragmentací
        - Tunelovací routery jsou možné single point of failure
        - Bezpečnostní riziko
- Translation:
    - Přeložení IPv6 hlaviček na IPv4 hlavičku
    - Výhody:

        - Jednoduché dočasně řešení
    - Nevýhody:
        - Nepodporuje pokročilou funkcionalitu IPv6
        - Překlady jsou ztrátové - hlavičky mají jiné vlastnosti
        - Omezuje architekturu tolopogie
        - Odpověď musí jít přes stejný NAT - zatížení + single point of failure

Jakým způsobem je v IPv6 řešená mobilita? Popište včetně schématu.

Mobilní prvek (MN) má svoji domácí adresu, která je dostupná přes domácího agenta (HA). Pokud je mobilní prvek připojen na cizí adrese (Care of adresa), tak se nahlásí HA, aby mu přeposílal segmenty na care of adresu a via versa.

Optimalizace (Return Routability Procedure):

- Je možné aby se correspondent note dorozumíval s MN přímo, je však nutné ověřit, že se nejedná o man-in-the-middle útok
- MN musí dokázat, že vlastní jak HA, tak i Care-of adresu
    - **Home Test Tnit** (HoTI) - MN posílá Home init Cookie CN přes HA
    - **Care-of Test Init** (CoTI) - MN posílá Care-of init Cookie CN přímo
    - **Home Test** (HoT) - CN posílá Home Nonce Index přes HA
    - **Care-of Test** (CoT) - CN posílá Care-of nonce Index přímo MN
    - MN a CN si vypočítají management key a dále komunikují přímo

Neighbour discovery v IPv6.

Je součástí ICMPv6

Využívá se 5 zpráv:

- Neighbour Solicitation (NS) - Získání L2 adresy, Duplicate address detection, NUD
- Neighbour Advertisement (NA) - Odpovídá na NS, informuje o změnách L2 adres
- Router Solicitation - host žádá o autokonfiguraci
- Router Advertisement - obsahuje informace o autokonfiguraci
- ICMP redirect

Co jsou to Distance Vector směrovací protokoly? Jak pracují? Jmenujte 3 zástupce, jednoho z nich popište detailně.

Distance vector:

- Způsob směrování na transportní vrstvě
- “Informace o celé síti pouze sousedům”
- Číslo vektoru vzdálenosti - metrika
- Každý směrovač si drží směrovací tabulku (Destination, Distance, Next hop)

- Směrovače si pravidelně (či při změně topologie) vyměňují a kopírují celou směrovací tabulku
- Belman-Ford algoritmus

Zástupci:
- RIPv1, RIPv2, RIPing
- IGRP (Interior Gateway protokol) - větší možnost hopů, 5 charakteristik
- EIGRP (Extend Interior Gateway protokol) - podpora masek sítě

Popis RIP:
- Metrikou je počet hopů
- Routery si posílají informace periodicky každých 30 sekund (pomocí UDP)
- Timeout je nastaven na 180 sekund
- Vhodný pro malé a stabilní sítě
- Nevhodné pro redundantní sítě
- Nedokáže se vypořádat s cykly a nejdelší vzdálenost je 15 (a pak nekonečno)
- Verze:
    - RIPv1 - dnes nepoužívané, broadcastové zprávy
    - RIPv2 - podpora masky sítě, multicast místo broadcastu
    - RIPing - podpora IPv6

Co jsou to Link State směrovací protokoly? Jak pracují? Jmenujte 2 zástupce, jednoho z nich popište detailně.

Link State:
- Způsob směrování na transportní vrstvě
- “Informace o sousedech celé síti”
- Routery si periodicky vyměňují informace o stavech svých přímých spojení
- Routery si udržují kompletní informace o topologii sítě - každý router ví o všech ostatních routerech v síti
- Dijkstra

2 zástupci:
- OSPF (Open shortest path first)
- IS-IS (Intermediate System to Intermediate System) - běží na L2 vrstvě

OSPF:
- Nejpoužívanější LS protokol
- Sbírá informace o stavu spojení z dostupných routerů a konstruuje topologickou mapu sítě
- Metrikou je cena (obvykle 1000000000/šířka pásma), lze nastavit manuálně
- Autentifikuje zprávy - od OSPFv2, v OSPFv3 se spoléhá na IPv6
- CIDR podpora
- Směrovací oblasti - Autonomní systémy mohou být rozděleny na subdomény pro optimalizaci
- Load balancing - OSPF může využít více odchozích spojení se stejnou nejnižší cenou
- OSFP zprávy jsou zapouzdřeny přímo do IP diagramů
- Využívá 5 zpráv:

    - Hello paket
    - Database description paket
    - Link state packet
    - Link update paket
    - Link state acknowledgement paket

Funkce směrovače, schéma, účel, vliv CIDR na směrování.

Účel:

- Najít cestu v okolí
- Posílat data správným směrem

Funkce směrovače:

- Příjem paketu
- Přečtení IP hlavičky
- Kontrola, zda není paket pro něj
- Pokud ne:
- Snížit TTL hlavičku a vyhodnotit
- Checksum rekalkulace
- Vyhodnocení MTU:
    - IPv4 fragmentace pokud je paket moc velký
    - IPv6 ICMP *packet too big* zpráva pokud je paket moc velký
- Nalézt cestu dle protokolu
- Odeslat

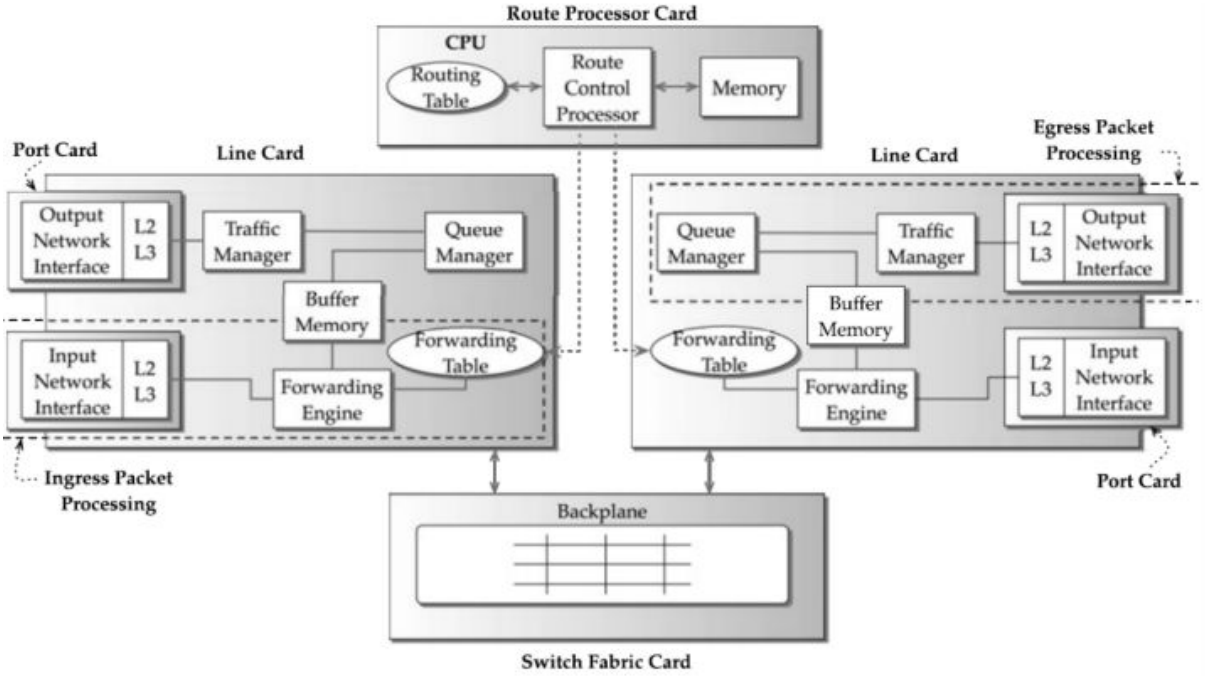
Schéma:

- Network interfaces
- Forwarding Engines
- Queue Manager
- Traffic Manager
- Backplane
- Route Control Processor

Vliv CIDR:

- Přináší komplikace jelikož IP adresa s sebou nenese masku
- Prefixy ve forwarding table, se kterými musí cílová adresa být shodná mohou být libovolné délky (Longest Prefix Matching)
- => pomalejší směrování

Popište fyzické komponenty směrovačů a zakreslete je do náčrtu.



RIP vs OSPF - shody, rozdíly.

Shody:

- Protokoly distribuovaného směrování
- Používají metriky
- Udržují směrovací tabulky které si vyměňují

Rozdíly:

- RIP:
  - Založen na Distance Vector
  - Nezvládá cykly
  - “Informace o celé síti sousedům”
  - Vhodný pro menší a stabilní sítě
  - metrikou je HOP
- OSPF:
  - Založen na Link state
  - Vhodný pro větší sítě
  - “Informace o mých sousedech všem”
  - jako metrika se používá cena

Uveďte, co je Traffic Engineering, jak a kdy sa používá. Jaké metody TE znáte?

Traffic Engineering:

- objevuje další možné cesty (kromě nejkratší) jsou v síti k dispozici
- Používá se proti přehlcení sítě

Jak a kdy:

- TE periodicky sleduje využití v síti (jednou za den/týden - dle administrátora)
- TE periodicky sleduje topologii sítě
- => vytvoření traffic matice
- Odhaduje tak stav zatížení
- Určuje nové váhy jednotlivým spojením dle pozorování
    - posílá se za pomocí OSPF, IS-IS

Metody TE:

- Sledování sítě:
    - NetFlow, sFlow
- Topologie sítě
    - IS-IS, IGP
- Určení váhy
    - Single-comodity
    - Multiple comodity

Protokoly IGRP a EIGRP

Interior Gateway routing protokol:

- Routing protokol založen na distance vector
- Běží přímo na IP protokolu
- Externí směry mohou být propagovány
- Umožňuje více cest pro rozložení zátěže
- Využívá pěti metrik pro každou cestu
    - banhwidth (B)
    - delay (D)
    - reliability
    - load
- Dále využívá pěti nezávislých koeficientů
- Metrika pro další hop se následně počítá z kombinace metrik cest a koeficientů
    - Výchozí hodnoty jsou nastaveny tak, že Cena = B + D
- Nepodporuje masku sítě
- “chatty protocol”

Enhanced Interion Gateway routing protokol:

- Rozšiřuje IGRP
- Přidává podporu pro maskování
- Poskytuje bezsmyčkové směrování

- Poskytuje spolehlivé doručování

Co znamená MPLS (Multiprotocol Label Switching) a jak pracuje; pro sítě jakého rozsahu je vhodný? Co je to GMPLS?

Multiprotocol label switching:

- Přeposílání za pomocí labelů
- Connection oriented
- Jednosměrné směrování
- Je možné přidat více štítků => vezme se s nejnižší cenou

Jak pracuje:

- Při příchodu paketu do MPLS sítě je tomuto paketu přidána nová hlavička s labelem
    - Nejčastěji za pomocí cílové IP, avšak není nutné (QoS)
- Každý router ví, jak se na základě štítku rozhodnout
    - Krátký pohled na štítek je rychlejsí než parsování IP adresy
    - Vyžaduje nové protokoly pro šíření labels
- Label paketu se může během průchodu měnit
- Pokud je paket pro router, je otevřen a zpracován
- Pokud je cílová destinace mimo MPLS tak jej koncový router rozbalí do původní podoby a odečte TTL

Do sítě jakého rozsahu:

- Pro velké sítě

GMPLS

- Generalized MPLS - rozšíření MLSP
- Schopnost přepínání paketů
- Schopnost time division multiplexing
- Schopnost Lambda switch - přepínání vlnové délky v optickém vláknu
- Schopnost Fiber switch - přepínání úrovní optických vláken

Co jsou to autonomní systémy a jakým způsobem se zde řeší směrování? Proč je výhodné AS zavádět?

AS:

- Rozdělení internetu na menší domény (odpovídá administrativním doménám)
- Pro zmírnění se tím přetížení routerů
- Kvůli různým politikám
- Každý AS má 16bitový identifikátor
- Typy:
    - Stub
    - Multihomed
    - Transit

Směrování:

- Interní:
    - V rámci AS
    - Důraz na efektivitu - RIP, IS-IS, OSPF

- Externí:
    - Mezi ASs
    - Důraz na politiky jednotlivých AS a škálovatelnost
    - BGP-4

Jaké jsou základní typy QoS based směrovacích algoritmů? Alespoň jeden popište podrobněji.

Základní typy:

- Source-based
- Hop-by-Hop
- Hierarchical

Source based:

- Každý router má globální statovou informaci o síti
- Na tomto základě je vybrána cesta
- Zdrojový router uvědomí ostatní routery jak přeposílat tok dat
- Výhody:
    - Jednoduchost
- Nevýhody:
    - Špatná škálovatelnost
    - Každý router potřebuje udržovat kompletní informace o stavu sítě

Klasifikace paketů a jejich filtrování.

- Poskytuje různé záruky služeb pro různé toky síťového provozu
- Flexibilní účtování dat (dle typu síťového provozu)
- Ochrana před útoky

- Existují pravidla:
    - Pravidlo obsahuje funkci říkající jestli má na paket být aplikována akce pravidla
    - Pravidlo obsahuje akci, která se má stát pokud paket vyhovuje podmínce pravidla
- Paket může odpovídat více jak jednomu pravidlu => vybíráme pravidlo s nejmenší cenou
- Algoritmy:
    - Naivní - pravidla jsou v listu a prochází se celý list pravdel
    - Dvourozměrné řešení - Hiearchické stromy
    - N rozměrné řešení

TCP, popište varianty TCP protokolu pracující na L2 vrstve.

Transmision Control Protokol:

- Protokol transportní vrstvy
- Connection-oriented

    - Vytváří spojení za pomocí třícestného handshaku (virtuální)
- Zajišťuje plně spolehlivou službu
- Pokud je to možné, data jsou posílána a přijímána ve správném pořadí
    - pomocí ACK
- Rozlišuje aplikace za pomocí protokolu
- Pouze point-to-point komunikace (pouze dva uzly)
- Kontroluje množství posílaných dat
    - Chrání příjemce před přetížením - Flow control
    - Chrání síť před přetížením - Congestion control
- Množství dat posíláno do sítě je menší z:
    - Velikostí okna příjemce - rwnd
    - Velikosti okna přetížení - cwnd
- Hlavička:
    - Zdrojový port
    - Cílový port
    - Číslo posloupnosti
    - Acknowledgement number
    - HLEN - celková délka hlavičky
    - Control - 6bitů, identifikují různé kontrolní informace
    - Velikost okna
    - Checksum
    - Urgent pointer

TCP spolupracující s L2 vrstvou

- QuickStart
    - Předpoklad: překonat fázi slowstartu nelze bez spolupráce s nižšími vrstvami
    - Vyžaduje změny v IP vrstvě
    - Přidání do hlavičky 2 čtyřbitové pole - Initial Rate a QS TTL
    - Příjemce nastaví ideální (pro něj) Initial Rate a QS TTL (dostatečně velké) - nejlépe TTL
    - Odešle paket
    - Každý router který podporuje Quickstart navíc sníží QS TTL a popřípadě sníží Initial rate
    - Jakmile se paket dostane k odesílateli, tak ví jestli síť podporuje Quickstart (dle porovnání QS TTL a TTL) a pokud ano, nastaví cwnd na Initial Rate
    - Dále klasické TCP
- E-TCP
    - Obsahuje Early Congestion Notification (1 bit)
    - ECN je nastaven routerem pokud se dostává do stavu zahlcení
    - Příjemce musí ECN zrcadlit (nejlépe jenom poprvé)
    - Odesílatel zmrazí cwnd jakmile dostane ACK s nastaveným ECN
- Fast
    - Podobné TCP Vegas
    - FAST dělá větší kroky když je system vyveden z rovnováhy a menší když se blíží rovnováze
    - Může využívat ECN pokud jej síť podporuje

Řízení toku a zahlcení v TCP. Jak se počítá velikost vysílacího okna v tradicnich TCP protokolech? Jak to ovlivňuje množství přenesených dat na vysokorychlostních linkách?

Řízení toku a zahlcení v TCP:

- Kontrola toku
  - explicitní feedback od příjemce za pomocí rwnd. Je deterministická.
  - Aby odesílatel nezahltil příjemce
- Kontrola zahlcení
  - Přibližný odesílatelův odhad
  - S využitím operace cwnd
  - okno ownd = min(cwnd, rwnd)

Počítání okna v tradičních TCP protokolech:

Založeno na AIMD (additive increase, Multiplikative decrease)

- TCP Tahoe
  - Pro RTT beze ztrát (vyšší než sstresh) cwnd++
  - Pro ztrátu - sstresh = 0,5, cwnd = 1, znovuodeslání ownd
- TCP Reno
  - Přidává rychlé znovuodeslání
    - po třech ACK bez odeslání paketů okamžitě odešle jeden segment
  - Přidává rychle zotavení
    - loss -> sstresh = cwnd = cwnd * 0,5
- TCP Vegas
  - Měří zahlcení sítě za pomoci RRT
  - Když je zaznamenáno zpoždění, tak lineárně zmenší okno pro zahlcení

Jak to ovlivňuje množství přenesených dat na vysokorychlostních linkách:

Pokud je paket ztracen chybou sítě (aniž by došlo k přehlcení), tak TCP začne se slow startem a než se začne velikost okna blížit k bandwidthu uplyne netriviální čas (až hodiny)

Funkce TCP, fáze přenosu, rozepsat Tahoe/Reno/Vegas.

viz. výše

Popište protokol RBUDP (Reliable Blast UDP). Do jaké skupiny protokolů patří? Kdy ho lze s výhodou použít?

Popište protokol:

- Používá kombinaci TCP a UDP
- Ustanoví spojení za pomocí TCP

- Přenese všechna data za pomocí UDP
- Odešle se TCP paket informující konec přenosu
- Pokud na konci příjemce nedostal všechny pakety, zažádá si o ně za pomoci TCP
- (odesílatel odešle za pomocí UDP, a znovu dokola)

Do jaké skupiny protokolů patří:

- Patří do skupiny transportních protokolů

Kdy jej lze s výhodou použít:

- disk to disk přenos

Porovnání P2P s Client-Server.

Client-server:

- dva moduly, klient a server
- Server:
    - Jedna centralizovaná instance (může být replikovaná)
    - Pasivně poslouchá
    - Dokáže zpracovávat více požadavků zároveň (za pomocí front/paralelizace)
    - Vyhrazený spolehlivý hardware
    - Single point of failure
- Klient:
    - Více heterogenních instancí
    - Aktivně inicializuje komunikaci
    - Klienti spolu přímo nekomunikují (pokud, tak přes server)
    - Výpadek klienta neohrozí systém

P2P:

- Mnoho identických SW modulů na různých HW
- Peery mezi sebou komunikují přímo
- Každý peer je zároveň server i klient
- Peery mají tendenci být nespolehlivé
- P2P je přirozeně škálovatelné
- Pracuje bez vyhrazeného serveru

Taxonomie P2P systémů, stručně charakterizovat každou kategorii.

Taxonomie:

- Centralizovaný - server poskytující různé služby, typicky pomáhají najít požadované zdroje - StarCraft, Jabber
- Decentralizovaný - každý peer má stejné práva a povinosti - Gnutella, FreeNet
    - Flat vs Hierarchical
        - Flat - funkcionalita i zátěž jsou rozloženy rovnoměrně
        - Hierarchical - více vrstev směrovacích uzlů
    - Structured vs unstructured
        - Structured - data jsou strukturována dle určitých pravidel

        - Unstructured - každý peer je zodpovědný pouze za svoje data
- Hybridni - určitá kombinace dvou předchozích

Co jsou overlay networks a kde se nacházejí.

Overlay networks

- Virtuální síť postavená nad transportní vrstvou
- Využívá pro svůj provoz TCP/UDP
- Může (a nemusí) respektovat rozložení peerů v transportní vrstvě
    - Peery které jsou blízko na overlay networku nemusí být blízko sebe v reálné síti

Směrování CHORD v P2P, popsat jak a kde sa používá. Jak v něm probíhá směrování?

CHORD:

- Každý uzel spravuje část dat
- Používá hashovací tabulky - jsou zahashovaná data
- Spojení je jednocestné (do kruhu)
- Získání/uložení položek znamená nalézt peer s adresou zahashovaných dat

Kde:

- Používá se ve strukturalizovaných P2P sítích

Jak probíhá směrování:

- Simple lookup alg
    - Každý peer potřebuje znát jenom své bezprostřední následníky
    - Uzel který hledá data jej pošle svému následníkovi
    - Ten se podívá, zda má data, pokud ne, tak zkontroluje, zda ID následníka není větší než hash dat
        - pokud ano, hledání neúspěšně ukončeno
        - pokud ne, odešle následníkovi
- Scalable lookup alg
    - Každý peer si drží finger table
        - tabulka obsahuje adresy na 2 na *n* peery
    - Pokud peer obdrží dotaz, tak v tabulce vyhledá největší menší ID peeru a odešle jej (plus kontrola zda on není požadovaný peer či ID není již větší)

Popište P2P sítě využívající PRR stromy a vyhledávání v nich.

Popis sítě:

- Každý uzel má jako ID m-bitové číslo, které je rozděleno na sekvence číslic se základem 2 na b
- Každý peer si drží 2D tabulku pro směrování
    - ID řádku - délka prefixu společného s cílovým uzlem

    - ID sloupce - další možný krok
- Peer si drží i leaf sety - slouží jako spádové uzly, pokud není kam směrovat

Vyhledávání:
- Pastry
    - Data jsou v uzlu, který s identifikátorem dat sdílí nejdelší prefix
    - V každém kroku je vybrán další uzel s o jedna větším prefixem
- Tapestry
    - Obdobné pastry, ale používá suffix

Popište P2P systémy BATON a P-Grid. Jaké grafové struktury využívají a čím se liší?

P-Grid:
- Virtuální binární strom (může být nevyvážený)
- Každý peer je je zodpovědný za data, jejich prefix je roven ID peera
- Každý peer si udržuje routovací tabulku
- ID peeru může být duplicitní (za účelem tolerance chyb)
- Routování:
    - Při obdržení dotazu peer zkontroluje, zda jeho ID je prefix klíče dat
        - pokud ano, tak vyhledá lokálně data u sebe
        - pokud ne, podívá se do routovací tabulky, aby našel nejbližšího souseda a přepošle dotaz

BATON:
- Používá stromovou strukturu
- I v interních uzlech jsou peery
- Peer si má odkazy na
    - rodiče
    - potomky
    - sousedy
    - adjacent links - nejbližší vyšší ID
- Routování
    - Peer dostane dotaz s klíčem dat
    - Pokud je peer prefixem klíče - prohledá lokální úložiště
    - Pokud není prefixem - odešle dotaz na peer s největším menším ID než je klíč

Čím se liší
- Jiná routovací tabulka

Popište heuristické směrovací strategie používané v P2P sítích a alespoň jednu z nich podrobněji. Základní problém heuristik?

Heuristické směrovací strategie:
- Iterative Deeping

    - BFS po úrovních
    - Na začátku úroveň 1 - sousedi
    - Pokud není výsledek nalezen, zvýší se úroveň
    - Existuje úroveň, za kterou se nepokračuje a hledání je ukončeno
- **Directed BFS (rádoby podrobněji)**
    - Každý peer odesílá dotaz jenom části svých sousedů dle interních statistik
    - Příklad statistiky: počet zodpovězených dotazů, výsledků,...
    - Výhody - počet query dotazů je výrazně redukován
    - Nevýhoda - uzly jsou povinné udržovat statistiky, které mohou být zavádějící
- Intelligent Search
    - Každý peer odesílá dotaz jenom části svých sousedů dle relevantnosti odpovědí na dotazy
- Local indices Search
    - Každý uzel spravuje indexy pro lokální data a data sousedů ve vzdálenosti *k* hopů (k = 0 je BFS)
    - Dle globální politiky je pak specifikována hloubka vyhledávání a zpracování dotazu
- Random Walk
    - Náhodný výběr souseda
    - *k-random walk* = na začátku se vybere k náhodných sousedů - pak random walk
- Random Breadth First Search
    - Random k-walk i v peerech, kteří neinicalizují
- Adaptive Probabilistic Search
    - Kombinuje random k-walk a probabilistic search
- Interest Based Shortcuts
    - Každý peer si přidává do své tabulky peer se stejnými zájmy

Základní problémy heuristik:

- Není zaručeno, že data (i když se v P2P vyskytují) budou nalezeny
- Flooding - zahlcování sítě
- Není zaručena žádná efektivita

CAN

Content Addressable Network:

- D-dimenzionální prostor
- Systém rozloží data do tohoto prostoru (za pomocí hash table)
- Peery jsou spravují určený prostor
- Routing table - odkazy na peer spravující sousední prostory
    - routing - je vždy vybrán peer s bližšími souřadnicemi ke klíči
- Pokud existuje výsledek, měl by být uložen v patřičné zóně

Připojení uzlu:

- Nový uzel musí najít libovolný peer připojený k síti
- identifikuje zónu na rozdělení

- Požádá vlastníka o rozdělení zóny
- Vytvoření vlastní routing table
- Aktualizování routing table sousedních uzlů

Odpojení uzlu:

- Požádání o sloučení zón
- Ostatní si musí aktualizovat routing table

Co je to VANET a jaké jsou rozdíly oproti mobilným ad-hoc sítím?

Verticular Ad hoc Network:

- Automobilové ad-hoc sítě - auta se využívají jako uzly
- Interakce mezi zařízeními na silnici jsou docela přesně popsána - můžeme používat specifičtější protokoly

Rozdíly oproti MANET

- Uzly se nepohybují náhodně
- Není třeba se tolik zaobírat energií

MANET, co to je, porovnání s P2P.

Mobile Ad-Hoc Network:

- Ad hoc síť
- samoorganizující se
- samokonfigurující se
- bez infrastruktury
- wireless
- nody se pohybují v čase a prostoru

Podobnosti s P2P

- samoorganizující se
- samokonfigurující se
- bez infrastruktury

Rozdíly (MANET / P2P)

- wireless / wired
- pohybující se nody / nody se nepohybují
- fyzická struktura = logická struktura / v P2P logická struktura nekopíruje fyzickou
- reaktivní i proaktivní routing / pouze reaktivní routing

Porovnání reaktivního a proaktivního ad-hoc směrování, příklady protokolů.

Reaktivní:

- Cesta se nachází až je potřeba
- Nižší overhead - nižší spotřeba energie
- Vyšší latence

- Protokoly: Dynamic Source Routing (DSR), AdHoc on Demand Dostance Vector (AODV)

Proaktivní

- Cesty mezi peery jsou udržovány v routing tables
- Uzly si pravidelně vyměňují své tabulky
- Velká routovací zátěž
- Nižší latence
- Protokoly: Destination Sequence Distance Vector (DSDV), Opminalized Link State Routing (OLSR)

Jak pracuje reaktivní ad-hoc směrování (Reactive On demand Ad-hoc Routing)? Uveďte příklady konkrétních protokolů se stručným popisem.

Reaktivní:

- Cesta se nachází až je potřeba
- Nižší overhead
- Vyšší latence

Dynamic Source Routing:

- Používají se PREQ a PREP pakety pro objevení cesty
- Iniciátor odešle PREQ pateky všem naslouchajícím
- Ti provedou to samé s tím, že připojí svoje ID
- Jakmile source dostane PREQ odešle PREP s IDs všech nodů
- Ustanoví se cesta

Ad-hoc on Demand Distance Vector (AODV)

- Podobný proces jako DSR
- Každý node si zapíše do své routing table vytvořenou cestu v PREQ
- Pokud dojde PREQ na cestu, kterou node už zná, odešle správný PREP

Přístup k médiu pro WSN a Ad-hoc sítě. Identifikujte hlavní kritérium použitelnosti pro tyto protokoly; uveďte jejich klasifikaci a pro každou skupinu zástupce.

Wireless Sensor Network

- Hlavní kritérium je plýtvání energií
- Interakce s okolím (měří/ovlivňují okolí)
- Sítě jsou zakomponovány do okolí
- Bezdrátová komunikace
- Omezení:
    - Dostupná energie
    - Paměť - malý senzor = malá paměť
    - Šířka pásma - vzhledem k energii relativně malá šířka pásma
    - Spolehlivost
    - Adresovatelnost - dynamická alokace adres

    - Škálovatelnost využívaných metod

Klasifikace

- Connection based - MACA, BTMA
- Connection based with reservation mechanism - MACA/PR
- Connection based with scheduling mechanism - LEACH, SMACS

Co jsou to multimediální data a jaké typy těchto dat rozlišujeme? Uveďte protokoly, které multimediální data zpracovávají a ve zkratce je popište.

Multimediální data

- data, které jsou složené z více typů/forem médií, které jsou nějakým způsob integrovány dohromady (text, obraz, zvuk)

Rozlišení

- Realtime
    - Discrete
        - text, chat,.. (nedovoluje chyby)
        - weather updates (dovoluje chyby)
    - Continuous
        - Delay intolerant
            - Remote desktop (nedovoluje chyby)
            - Videochat (dovoluje chyby)
        - Delay tolerant
            - Stream (dovoluje chyby)
- Non-realtime
    - Text, Data (nedovoluje chyby)
    - Obraz (dovoluje chyby)

Protokoly

- HTTP - web
- SMTP - email
- FTP - data
- RTP - streams

Komunikační protokoly pro přenos Multimédií s ohledem na Realtime přenos.

Protokoly

- Session Description protocol
    - Jedná se o formát popisující parametry streamovacího média
    - <tag>=<value> kde tag je předdefinovaná jednopísmená zkratka
- Session Announcement protocol
    - Používáno pro oznamování multicast konferencí/session
    - zajišťuje integritu, autentifikaci a šifrování
- Real-Time protocol
    - Běží nad UDP

        - Přenáší části dat
        - Nezajišťuje kvalitu, ale dodává informace aplikacím, díky kterým to lze
        - Poskytuje
            - Sequencing
            - Identifikace payloadu
            - Frame indicator
            - Source identification
            - Intramedia synchronization
- Real-Time Control Protocol
    - Kontrolní protokol spolupracující s RTP
    - Sbírá statistiky o aspektech kvality
- Real-Time Streaming protocol
    - Nadrámcový kontrolní protokol
    - Pracuje s RTP
    - Umožňuje kontrolovat přehrávači přenos média streamu
    - “Stavové http”

Jak probíhá digitalizace zvuku, 3 formáty zvukového záznamu.

Digitalizace zvuku

- Sampling - bereme diskrétní hodnotu zvuku v pravidelných časových intervalech
- Kvantování - bereme diskrétní hodnotu zvuku dle jeho křivky

3 formáty

- mp3, wav, webm

Popište přenosové a funkční požadavky multimediálních síťových aplikací + protokoly.

Přenosové požadavky

- Delay
- Jitter
- Bandwidth
- Reliability

Funkční požadavky

- podpora multicastingu (IGMP)
- bezpečnost (IPv6)
- Mobilita (IPv6)
- Session management (RTP, SAP, SDP, RTCP, RTSP)

FEC, BEC a Interleaving

Forward error correction

- Vyžaduje, aby k paketům byly přidány extra informace – tyto informace jsou použity pro obnovu ztracených paketů.

- Media-independent FEC – využívá blokové nebo algebraické kódování k produkci dodatečných paketů, které pomáhají při obnově ztrát.
    - Kódování berou kódové slovo n datových paketů a generují tak m dodatečných kontrolních paketů
    - Parity Coding – operace XOR je aplikována na skupinu paketů za účelem generování paritních paketů
    - Reed-Solomon Coding – polynomy s určitými číselnými základy
    - Nevýhoda – způsobuje dodatečné zpoždění a zvyšuje využití šířky pásma
- Media-dependent FEC – využívá charakteristiky médií
    - Každá datová jednotka je poslána ve více paketech – primární šifrování + sekundární šifrování (může být nižší kvality než primární šifrování)
    - Nemusí vyžadovat přenos FEC pro každý paket, díky povaze média
    - Výhoda – nízká odezva => vhodné pro interaktivní aplikace

Backward error correction

- Pokud je chyba neopravitelná (nebo používáme jen detekci chyb bez oprav), příjemce požádá odesílatele o opětovné odeslání dat = Automatic Request for Retransmition (ARQ) – vhodné pro málo ztrátová přenosová média: sudá/lichá parita, CRC, …

Interleaving

- Může být využito jen tehdy, když velikost jednotek v médiu je menší, než je velikost paketu (např. audio jednotky). End-to-end zpoždění není důležité.
- Na základě znovuobnovení jednotek v médiu před síťovým přenosem (původně přilehlých jednotek oddělených garantovanou vzdáleností) a navrácení do původního pořadí u příjemce – rozptýlení efektu ztráty paketů
- Ztráta jednoho paketu způsobí mnoho malých mezer v původním médiu (jednodušší k vyřešení)
- Výhoda – nezvyšuje využití šířky pásma
- Nevýhoda – zvyšuje se odezva => nevhodné pro interaktivní aplikace