

Protokollarchitektúrák

Fizikai réteg

- Bitsoportok továbbítása, bitszinkronizáció

Adatkapcsolati réteg

- Bitsorozatok keretezése, fizikai (MAC) címek kezelése, közeghozzáférés vezérlése (Medium Access Control)

Hálózati réteg

- Egyedi linkek összekötése végpontok közti csatornává
- Logikai címezés: hálózati eszközök közti kapcsolásokhoz
- Útvonalkeresés a hálózaton belül

Szállítási réteg

- Végpontok közti megbízható kommunikáció
- Hibamentes összeköttetés (hibás/duplikált csomagok kezelése, sorrend helyreállítása)
- Forgalm szabályozás

Viszonyréteg

- Kapcsolat irányának kezelése (duplexitás)
- Összeköttetés kezelése (kapcsolatépítés és -bontás)
- Manapság a szállítási vagy alkalmazási rétegben

Megjelenítési réteg

- Felhasználói adatok: adatábrázolás, tömörítés, titkosítás

Alkalmazási réteg

- Csak a felhasználót szolgálja ki, végpontokon futó programokhoz
- Kommunikációs partnerek azonosítása, hálózati erőforrások elérhetősége, szinkronizáció felhasználók közt, formátum, biztonsági egyeztetés

Ez volt a szabványos OSI referenciamodell. A gyakorlatban a fizikai, adatkapcsolati, hálózati, szállítási, és alkalmazási réteg valósult meg.

Többszörös hozzáférés

Fix csatornamegosztás

- **Frequency-Divided Duplex (FDD)**: megosztás up/downlink irányba
- **Frequency-Divided Multiplexing (FDM)**: több kis sáv szélességű csatorna egy nagyobbon
- **Frequency-Divided Multiple Access (FDMA)**
 - Frekvenciasávot oszt szét a felhasználóknak, interferencia miatt védősávok.
- **Time-Divided Multiple Access (TDMA)**
 - Időablakokat oszt szét, szinkron gondok = szinkronrések.
- **Code-Divided Multiple Access (CDMA)**: egy időben, egy frekvencián, más kóddal

Véletlenszerű hozzáférés

Egyszerű ALOHA

- Két frekvencia (up/downlink)
- Hub -> kliens: csomagok, címezve
- Kliens -> hub: nyugtázott, különben random idő után újraküldés
- Rossz kihasználtság, instabil, de fair

Réselt ALOHA

- Azonos hosszúságú csomagok időréshatárokon (szinkronjel)
- Dupla kihasználtság, fair, de instabil

Helyfoglaló ALOHA

- Igénybejelentés, majd az igénylők sorban küldenek

Carrier Sense Multiple Access (CSMA), vivőérzékelés

- Szabad csatorna: igénybevétel
- Foglalt csatorna:
 - nemperzisztens: random idő múlva újra
 - 1-perzisztens: ahogy felszabadul, újra
 - p-perzisztens: random idő után p valószínűséggel újra, időrés elején

CSMA with Collision Detection (CSMA/CD)

- Ütközésnél leállítás, jam signal
- Csak félduplex vezetéken
- Újraadás: exponenciális backoff
- Legrosszabb eset: A-B közt A-nál, 2T a detektálás

CSMA with Collision Avoidance (CSMA/CA)

- Szabad csatorna: szól mindenkinek és ad, vagy vár, és ha utána is szabad, ad
- Foglalt csatorna: exp. backoff
- Rádió is jó, de problémás:
 - Rejtett terminál: árnyékolt felhasználó két terminál közt, nem érzékelt adást zavar
 - Exponált terminál: két csatornát lát a felhasználó, nem meri használni a sajátját, mert ütközéstől tart
 - Megoldás: igénybejelentés (RTS), engedély (CTS) jelzés

Bit mapped protocol (Bit-térkép módszer)

- N időrés, j. terminál a j.-ben mondja, ha adna
- Sorrendben ad, aki akart
- Alacsony forgalomnál nem hatékony

Binary countdown (Bináris visszazámlálás)

- A küldeni akaró ID-jét körbeküldi, ha bitenkénti VAGY után 1-et látnak, visszavonulnak
- Nagyobb ID-k jobb helyzetben vannak

Capetanakis-algoritmus, adaptív fa

Ütközésnél két csoport, rekurzív.

Központi vezérelt módszerek

- **Roll-call polling (lekérdezés):** körbekérdez, aki akar, küld
- **Probing (csoportos lekérdezés):** egyszerre többet pollol, ha több küldene, egyesével kéri
- **Reservation (helyfoglalás):** csatornamegosztás foglalás és használat közt
- **Token passing (vezérjelátadás):** a használati jog azé, akié a token, ezt küldik körbe

Exponenciális backoff

$[CW * RND()] * Slot_Time$

- Contention Window (CW): 31, majd 63, körönként $*2+1$
- RND: random 0-1 közt
- Slot_Time: résidő, ezalatt az állomás biztos észlelhessen foglalást

Lokális hálózatok (Ethernet, Kapcsolt Ethernet)

Hálózatok osztályozása

Wide Area Network

Metropolitan Area Network

Local Area Network

Personal Area Network

Body Area Network

Ethernet

- Logikailag busz topológia
- CSMA/CD (mindenki hall mindent, minimum méret és csomaghossz összerendelve)
- Jelölés: sebesség Mbitben + Base/Broad + közeg/szegmenshossz
- Nincs kapcsolatfelépítés, nincs nyugta

Ethernet jelismétlő (repeater)

- Szegmensek összekötése
- Ütközés: minden porton jam signal
- Sokkapus ismétlő (hub): ütközéskezelés (pl. porttiltás)

Minimális csomaghossz (résidő)

- Ütközések biztos elkerülése
- Legkedvezőtlenebb esetben is mindkét állomás érzékeli: $T = 2L/C$
 - résidő = $2 * \text{szegmenshossz} / \text{jelterjedési sebesség}$

Kapcsolt Ethernet

- Nagyobb forgalmat kezel buszsegesség növelése nélkül
- Bridge (híd) és switch (kapcsoló) bevezetése: MAC cím alapján irányítják a forgalmat
- A híd LAN-szegmenseket köt össze, a kapcsoló munkaállomásokat is tud
- Több, eltérő sebességű szegmens összekapcsolása
- 10 Gbit: full duplex switch, nincs CSMA/CD

LAN-ok kiterjesztése

- LAN-korlátok: távolság, állomások száma és típusa
- Átjátszó segítségével
- Nem minden réteg szükséges minden csomópontban = különböző átjátszók
 1. repeater (jelismétlő) / hub (többportos jelismétlő)
 2. bridge (híd) / switch (kapcsoló) = store and forward
 3. router (útválasztó)
gateway (átjáró)

Switch extra

- A végpontok nem látják, transzparens
- Plug-and-play, self-learning (switching table, MAC helyét megjegyzi)
- Nincs ütközés, full duplex
- 2-2 végpont közt kapcsolat akár egyszerre

Vezetéknélküli LAN-ok

WLAN

- Párszáz méter, 1 Mbit - 1 Gbit, ISM sávban 2.4 és 5.8 GHz (engedélymentes)
- Access Point és WLAN kártyák közt
- Ad-hoc mód: eseti peer-to-peer hálózat, csak kliensek, pl. WiFi Direct
- Infrastruktúra mód: központ az AP, vezetékre kötve, csak AP-kliens beszél
- Csatlakozás: állomás szkenneli a csatornákat beacon keretek után, bennük AP SSID és MAC, választ egy AP-t, DHCP-vel kap egy IP-t.
- CSMA/CA, ütközést detektálni pl. rejtett terminál miatt nem lehet

Csatornák

- 2.4 GHz: 13 db 22 MHz-es csatorna, egymástól 5 MHz-re a középfrekvencia
- Spektrális maszk minden csatornára, átlapolódás miatt, -30 dB +/- 11 MHz-re
- 1, 6, 11 pl. működik átlapolódás nélkül, de interferencia és közel-távolság probléma lehet
- 5 GHz-es sávban 23 nem átlapolódó csatorna

Topológia

- Basic Service Set (BSS) - AP és a kliensei (nem a lefedett terület)
- Extended Service Set (ESS) - több BSS, közös SSID
- Distribution System (DS) - elosztóhálózat, gerinc
- BSS-ek közti mozgás switch-ben öntanulással megoldva

Wireless Access Point (WAP) - brigde

- 802.11 keretben, fontos almező: Frame Control: 2 bit típus, 2 bit to DS - from DS
- To DS - from DS MAC mezők: cél-forrás-cél-forrás (előbbi cél az AP, 00-nál a 3. BSS ID)
- Vezeték nélküli híd 11-es eset, vezeték nélküli ismétlő és végpont közt 01/10

Distributed Coordination Function (DCF) hozzáférés

- CSMA/CA
- Különböző értékű IFS-ek (inter-frame space)
 - Short IFS (SIFS): rövid vezérlőüzenetek, fontos adáskor először férnek csatornához
 - pl. ACK/CTS üzenetek, konstans hossz, reduced IFS (RIFS) még rövidebb
 - DCF IFS (DIFS): adatkereteknek, SIFS + 2 * résidő
 - PCF IFS (PIFS): PCF-es AP várakozása, SIFS + résidő
- Szabad csatornán állomás folyamatosan figyel, vár, hogy DIFS ideig szabad-e, majd random idő múlva ad, amire ACK választ vár

Network Allocation Vector (NAV)

- RTS keretben csatornafoglalási idő, a többi állomás eddig vár, mielőtt csatornát ellenőriz
- Fizikailag foglalt közeg: állomás szerint foglalt a csatorna
- Virtuálisan foglalt közeg: állomás RTS/CTS-t kap, foglalt lesz a csatorna, NAV-ot indít
- RTS/CTS opcionális, rejtett állomás ellen, de csökken az átvitel, késleltetés nő

Point Coordination Function (PCF)

- Opcionális, DCF-fel, felette, egyetlen AP vezérli a hozzáférést, üzenetére nincs több DCF
- Sorban kérdez az AP, a kliens csak akkor ad, ha kérdezik
- Priorításokat lehet kliensekhez rendelni

Kapcsolás, jelzés, címzés

Azon módszerek összessége, amik összekötnek két pontot

Áramkörkapcsolás

- Fizikai kapcsolat, minden információ ugyanazon a hálózaton halad
- Fel kell építeni, le kell bontani (jellemzően nem állandó)
- Valósídejű átvitelre kiváló, torlódás csak összeköttetéskor lehet
- Továbbítás alatt csomópont adatot nem tárol

Csomagkapcsolás

- Egész üzenet, egy egységben, két szomszédos csomópont közt
- Megvalósításához az üzenetben címrész, csomópontban tárolás (store and forward) kell
- A küldő tördeli üzenetét csomagokra, egymás után (sorszámozva) hálózatra küldi
- Különböző útvonalon, eltérő sorrendben is célba érhetnek
- Csomópontok eszközei: router, switch
- Összeköttetés-mentes mód: datagram-kapcsolás
- Összeköttetéses mód: virtuális áramkörkapcsolás
- Előnyök: több felhasználó egyszerre, prioritás, üzenetszórás
- Hátránya: késleltetés, nem valósídejű

Datagram-kapcsolás

- Minden csomag önálló egység, és tartalmazza a rendeltetési hely teljes, egyedi címét
- Két végpont közt megvizsgálják a fejléct, majd útvonalat választanak neki
 - Választás: merre gyorsabb? merre szabad az út?

Virtuális áramkörkapcsolás

- Két pont közt szakaszokból álló összeköttetés, minden csomag ott megy
- Kapcsolatépítés, adatátvitel, kapcsolatbontás
- Csomópontokban virtuális áramkör azonosító (VCI)
- Kétféle jelzésátvitel: in-band (HTTP), out-of-band (FTP): jelzések külön csatornán

Elnevezés és címzés

- Egyedi név (google.com) -> egyedi cím (12.34.57.69) = névfeloldás
- A nevek hierarchikusak (subdomain.domain.top-level-domain)
- A neveket a Domain Name System oldja fel
- A címzés is globálisan egyedi és hierarchikus, egyszerűbb az útválasztás
- Többszintű a címzés (pl. hálózaton belül MAC)

Útvonalválasztás

Hálózati réteg

- Szegmens átvitele a feladótól (ráadott IP fejléccel) a címzettig (szállítási rétegnek)
- Hálózati rétegbeli protokoll minden csomópontban (pl. router: fejlécvizsgálat alapján)

Routing

- Bridging: adatkapcsolati rétegben MAC alapján, nem tud különbséget tenni hálózatok közt, elárasztást használ: csak helyi hálózaton jó
- Routing: Hálózati rétegben IP alapján, skálázható
- Útvonalválasztó módszerek, algoritmusok, és azokat megvalósító protokollok
- Probléma: a hálózat mérete nem állandó, és túl nagy
- Összeköttetés alapon útvonalkijelölés, összeköttetés nélkül útvonalválasztás
- A valóságban elosztott, Bellman-Ford (távolságvektor, decentralizált, a szomszédok elmondják egymásnak, ki milyen távol van tőlük) vagy Dijkstra (linkállapot, globális, mindenki elmondja mindenkinek a szomszédait) algoritmus

Feladat

- Megismerni a hálózat felépítését: csomópontok, linkek, útvonalak
- Összeköttetéses esetben a csomópontok információi alapján az útvonal kiválasztása, feljegyzés a csomópontnál, végpontok értesítése az elkészült útvonallról
- Összeköttetés nélkül a csomagtovábbításakor választódik útvonal
- Áramkörkapcsolt eset: állandó csatorna az átvitel idejére

Útvonaltáblák (forwarding table)

- Útvonalmeghatározás a csomópontok táblái alapján (kitölthető manuálisan vagy automatikusan (centralizált/elosztott))
- Két oszlop: az érkező csomag fejlécének értéke → kimenő link
- Centralizált: egy ponton minden infó a hálózatról, ami meghatározza és elküldi a csomópontokhoz a tábláikat: konzisztens táblák, de sérülékeny
- Elosztott: a csomópont készít saját táblát, nem sérülékeny, de nem is egységes, és eltérő nézetek lehetnek a csomópontokban
- Követelmények: minél kisebb tábla (olcsóbb, gyorsabb), robusztusság (hiba esélyének (hurok/oszcilláció) minimalizálása), optimalitás (idő, költség, megbízhatóság)
- Általában bináris fával implementálják

Távolságvektor

- Legegyszerűbb esetben az ugrások száma, de súlyozható a link sebességével, sorbanállás hosszával, vagy költséggel
- Szomszéd költsége: $d_x(y) = \min_v \{c(x,v) + d_v(y)\}$, v : x -nek minden szomszédja
- Amelyik szomszéd lesz a minimális, táblába kerül
- Aszinkron és iteratív, iterációt egy költségváltozás vagy vektor átvétele vált ki
- Csak vektor megváltozásakor értesítenek szomszédot

- Alapprobléma a végtelenségig számolás: meghibásodás és téves számolások lehetnek, egy el nem érhető ponthoz a végtelenségig növelhetik a távolságukat, ettől egymásnak küldik a csomagot, és túlterhelik a linkeket
- Javítások: split horizon (visszafelé nincs útvonalhirdetés), route poisoning (elérhetetlen útvonal hirdetése), holddown timer (egy ideig nem foglalkozik kiesett pontokkal)

Linkállapot módszer

- Továbbadva: link állapota és költsége, elárastással, kivéve visszafelé
- Minden csomópont ismeri a topológiát, így kiszámolhatják a költségeket mindenkire
- N iteráció után ismeri a legrövidebb távolságot N állomás felé
- Dijkstra algoritmus: legrövidebb útvonalakból fa, majd minden $D(v)$ cseréje arra, hogy $\min(D(v), D(W) + c(v, w))$, vagyis a legrövidebb útvonal egy másik ponton keresztül, ahonnan ismert oda a távolság
- Hatékony implementációval akár $O(n \cdot \log n)$
- Gyakorlatban: hierarchikus linkállapot routing protokollok
- Oszcilláció lehetséges, ha a link költsége a pillanatnyi forgalom

Autonóm rendszerek

- A világháló egy egységben nagy falat lenne az algoritmusoknak, szegmentálni kell
- Autonóm rendszer (AS): önállóan old meg routing feladatokat, a külvilágnak egy pont
- AS-en belül egységes routing irányelv, egyetlen hálózat (pl. egyetlen) közös adminnal
- Gyakran routing domain néven
- Globálisan egyedi azonosító a IANA-tól: Autonomous System Number (ASN)
- Határroutereken (gateway router) keresztül kapcsolódnak, mint egy bejegyzés
- Multihomed AS: több, mint egy AS, hiba esetén sem lesz elvágva, viszont nem enged átmenő forgalmat más AS-ek közt
- Stub (csonk) AS: csak egy másik AS-sel van összekötve
- Tranzit AS: csak átmenő forgalom, ilyen egy ISP
- Multihomed és tranzit AS esetén több útvonal van más AS felé
- Sok esetben nem a linkkapacitás vagy a költség számít, hanem az üzleti kapcsolat a szomszédos AS-sel
- Hot-potato elv: minél rövidebb út saját AS-en belül, összességében lassabb lehet
- Cold-potato elv: minél tovább saját AS-en belül, minőségi garanciát nyújthat
- Mobil végpont: átmehet másik AS-be

Multicast (többesadás) routing

- Nem egy célpont van (pl. konferenciabeszélgetés)
- Broadcast: mindenkinek, multicast: egy csoportnak, anycast: csoportból a legközelebbinek, unicast: egy pontnak
- Feladatok: címzés, csoportkezelés, útválasztás segítése
- A csoportot egy csoportcím azonosítja
- Sűrű elhelyezkedés esetén legrövidebb útvonalra, elárastás és lemondással, amúgy explicit csatlakozás, elhelyezkedésfüggetlen esetben mindkettő

IP - Internet Protocol

Az IP feladata és jellemzői

- Hálózati protokoll: adattovábbítás végpontok közt
- Fő funkciók: címzés (addressing), útvonalválasztás (routing), tördelés (fragmentation)
- Csomagkapcsolt, összeköttetés-mentes (datagram)
- Nincs garancia: a csomagok elveszhetnek, duplikálódhatnak, sorrendjük megváltozhat, meghibásodhatnak (nincs hibajavítás, csak a fejléc ellenőrzése)
- Más, ami nincs: torlódáskezelés, ütemezés, titkosítás és hitelesítés
- IPv4 cím: 4 bájt, hálózatazonosító + egyedi azonosító, végpont/router interfészéhez
- Interfész: kapcsolat a végpont (egy interfész) vagy router (több), és a fizikai link közt

Címosztályok

- Különböző méretű hálózatok más osztályban
- A hálózati címeket egy kezelő szervezet (IANA) osztja ki, alatta 5 regionális kezelő
- A (első bájt) és B (második bájt) osztályokat országok, ISP-k, egyetemek kapnak
- A, B, és C osztályok unicast-ra, D osztály ([224.0.0.0, 240.0.0.0]) multicast-ra
- E osztály fenntartva (240.0.0.0-tól)
- Mivel a host ID csupa 0-ra a hálózat, csupa 1-re multicast cím, -2 terminál lehet
- 127.*.*: loopback interfész, helyi interfész, localhost, pl. vonaltesztelésre
- A címosztály nem skálázható, kihasználatlan címeket hagynak, mind elfogyott
- Az osztályokat eltörölték, lett helyette alhálózati maszk (<IP>/<host ID bitjei>)
- Hierarchikus címzés, útvonal aggregáció: hatékonyabb routing

Network Address Translation (NAT)

- Helyi hálózaton nem kell globálisan egyedi IP, így kifelé minden egy IP-ről megy
- Késleltette az IPv6-ot, megsértette a végpont-végpont elvet (pl. P2P), a routerek elvileg csak a hálózati rétegig dolgozhatnak

Alapértelmezett útvonal (default route)

- Erre megy a csomag, ha nem ismeri a célhálózatot
- 0.0.0.0/0: minden címet tartalmazó hálózat
- Alapértelmezett átjáró, default gateway: a felfelé következő csomópont IP-je
- Végpontokon gyakran csak két bejegyzés: helyi hálózat, alapértelmezett útvonal

Metrikák szerepe az útvonalválasztásban

- Metrika (mérték): egy számérték, amely a hálózati utak közötti preferenciát adja meg
- Metrika alapja lehet pl: elérhetőség, terheltség, késleltetés
- Lehet manuális vagy dinamikus (a hálózat állapotától függ)
- A jobb metrikájú kapcsolaton küldünk csomagot
- Közvetlenül kapcsolódó (helyi) hálózaton fizikai cím ismeretében közvetlen küldés
- Nem közvetlenül kapcsolódó (távoli) hálózaton küldés az útválasztónak, de az IP-t módosítani tilos, csak az adatkapcsolati rétegben megy neki, ehhez szükség van az adatkapcsolati címére

Address Resolution Protocol (ARP)

- "Kié az IP-cím?" üzenet broadcast (ARP Request), a tulajdonos válaszol (ARP Reply)
- Közvetlenül az adatkapcsolati réteg protokolljának megy, nem IP-csomag
- ARP táblában tárolódnak az adatkapcsolati rétegbeli és IP-címek, statikus (manuálisan felvitt) vagy dinamikus (feloldott, cache-elt, idő után elévülő) formában
- ARP Probe: IP felderítése, hogy használja-e más, 0.0.0.0 forrásból magára kérdez
- ARP Announcement: ha változik a MAC vagy IP, értesíti a többieket
- RARP: Reverse ARP, MAC-ből IP-t, hálózatmenedzsmenthez vagy permanens tárnélküli eszközökkel használták, de ma már nincs, helyette BOOTP és DHCP

Útválasztó protokollok

- Feladatok: útvonal-irányítási információk begyűjtése, hurokmentes útvonal-irányítás, csatlakozások és leválasztások kezelése
- Osztályozás: Interior Gateway Protocol (IGP, AS-ek, kisebb hálózatok), Exterior Gateway Protocol (EGP, AS-ek közt, az internet routing protokollja), Ad-hoc (kis és gyorsan változó hálózatok, szenzorok, vezeték nélküli hálózatok)
- Ad-hoc protokollok osztályozása: működési mód szerint proaktív (folyamatosan karbantartott táblák), reaktív (igény szerinti címfelderítés), hibrid (az előző kettő), alkalmazási terület szerint hierarchikus, földrajzi alapon, multicast, energiatakarékos
- IGP: távolságvektor vagy linkállapot módszer
- Egy autonóm csoport egy bejegyzés

Interior Gateway Protocol (IGP)

- Távolságvektorosan: Routing Information Protocol (RIP), Interior Gateway Routing Protocol (IGRP), Enhanced IGRP (EIGRP)
- Linkállapotosan: Open Shortest Path First (OSPF), Intermediate System to IS (IS-IS)

Routing Information Protocol (RIP)

- Metrika: hopszám
- Lassan konvergál: RIP response (advertisement, 30s-enként) az AS-en belül
- Nem skálázódik jól: nincs hierarchia, de könnyen konfigurálható
- Hopszám limit korlátozza a hálózat méretét (max 15)
- Végtelenig számolás ellen: split horizon, route poisoning, holddown timer

Enhanced Interior Gateway Routing Protocol (EIGRP)

- IGRP a RIP javítása (255 hop, többféle metrika, 90s update, deprecated)
- Az EIGRP ezt javítja, Variable Length Subnet Mask használatával gyorsabb konvergencia és hurokmentes működés, 5 metrika, de alapból 2 kombinációja (min. sávszél + késleltetés)

Open Shortest Path First (OSPF)

- Link State Database (LSDB) üzenetek elárasztással (változáskor, periodikusan)
- Minden csomópontban topológia térkép (gráf), ebből legrövidebb útvonalú fa Dijkstrával minden alhálózatához
- IP üzenetekben, többféle metrika, autentikált, hierarchikus, gerinc - routing tartomány

- IS-IS: nagyobb hálózatokra (ISP), nem IPv4-specifikus, mint az OSPF

Border Gateway Protocol (BGP)

- Sokáig az EGP az internet EGP-je, de már a BGP
- Címaggregáció (supernet): kisebb routing táblák; gyorsabb keresés és terjesztés
- Routerek (BGP peer-ek) közt TCP kapcsolatok: BGP session
- AS2 hálózati prefix-et hirdet AS1-nek: AS2 megígéri, hogy kézbesít minden, a prefixnek megfelelő csomagot: AS2 aggregálhatja a hálózati prefixeket a hirdetésben
- A prefixek egy AS-en belül elárasztással terjednek
- Gateway router: import policy alapján dönti el, elfogadja-e az útvonalat
- Ha egy BGP több útvonalat kap egy prefix-et, a döntési sorrend: helyi preferencia érték (policy), legrövidebb AS-PATH (olyan AS sorozat, ahol áthalad a prefix), legközelebbi NEXT-HOP router (hot-potato, a következő AS-hez vezető AS-en belüli egység), más

Tördelés

- Maximum Transmission Unit (MTU): maximális keretméret, adatkapcsolati törzsben
- Eltérő technológiák miatt eltérő MTU-k (Etherneten 1500B): tördelni kell
- Tördeléskor minden töredéknek saját fejléce van: más töredék ID, ofszet, és flagek
- Tördelés után változik a total length, a checksum, az MF bit (more fragments, utolsót kivéve mindenhol 1), offsetet kell állítani, ha nem volt ID, azt is, adattördelés (8 bájtos)
- Csak a címzett rakhatja újra össze (kivéve NAT), ha nem érkezik meg egy, mind kuka

Internet Control Message Protocol (ICMP)

- Jelzés- és menedzsmentüzenetek (hiba, kérdés, válasz, pl. echo + reply = ping/tracert)
- IP-be ágyazva, azé után jön a fejléce, majd egy checksum (+hibánál a hibás head+8B)
- Típuson belüli kód (pl. címzett elérhetetlen, benne letiltott hálózat)
- Tracert: TTL = 1, majd 2,..., routerek folyamatosan eldobják, ICMP üzenetek alapján kilistázható, hogy merre megy a csomag
- IGMP: Internet Group Management Protocol, főként multicast csoportok kezelése, általában csak helyi hálózaton (TTL = 1)

IPv6

Az IPv4 problémái

- Elfogytak a címek, erőforrásigényes (felesleges mezők, tördelés), nem biztonságos (hitelesítés/titkosítás nem támogatott), nehéz konfigurálni, mobilitás-támogatás külön
- Eddig privát tartományokkal, DHCP-vel, NAT-tal, stb-vel húztuk ki.

Az IPv6 koncepciója

- Megnövelt címtartomány, előreláthatólag elég
- Egyszerűbb, rugalmasan bővíthető fejléc, checksum sincs, de lehet next header
- Erőforrás-allokáció, biztonságos kommunikáció, mobilitás, továbbfejlesztési lehetőség
- Neighbor Discovery Protocol (TCP-n): automata hostkonfiguráció, IPv6 címet, átjárót, DNS-t választ, duplikált címet észlel, link paramétereit határozza meg, címet old fel
- Path MTU Discovery: az egész úton meghatározható MTU miatt csak feladó tördel
- IPsec: titkosítás és integritásvédelem a hálózati rétegben

A szolgáltatásokat nyújtó eszközök

- "Okos" routerek: hálózati beállítások hirdetése hostoknak
- Anycast: szolgáltatás elérése ("valamelyik router mondja meg, hogy...")
- Multicast: azonos szolgáltatások eszközei egymás közt ("én már nem vagyok router")
- ICMPv6: pl. NDP-hez

Címzés

- 128 bit, 8 darab 16 bites hexaként, vezér 0 nem kell, egy helyen több 0 csoport sem
- Ha IPv4-ből származik, visszaírható az a rész, pl. ::127.0.0.1
- Prefixek jelölése: <prefix>::/48 (vagy a szabad bitek), hivatkozások [és] közt
- Kanonikus, ajánlott forma: vezérnullákat el kell hagyni, dupla kettőspont a max helyen, vagy több max esetén az elsőt, hexa számokban kisbetűk

Multicast címzés

- Broadcast nincs, első 2 bájttal 1: multicast prefix, majd 1B flagek, 1B group: cím érvényességének hatóköre, 12B group ID: csoportazonosítók
- Solicited-node multicast address: leginkább a keresett csoport hallgatja, de más is, képzése: ff02::1:ff00:0/104 + a kérdéses IPv6 utolsó 24 biteje, pl. Neighbor Discovery esetén így lehet broadcast nélkül megtalálni valakit

Anycast címzés

- Ugyanazt a címtartományt több helyen is alkalmazzák, és hirdetik BGP-vel
- Az IP datagramok a legközelebbi célhoz fognak megérkezni
- pl. DNS-ek: ugyanolyan IP-jű névkiszolgálóból több van, 6to4, tartalomszolgáltatók
- ::ff:0:0/96: IPv4 címek elérése IPv6-on

Neighbor Discovery Protocol (NDP)

- Állapotmentes automatikus címkonfig (Stateless Address Autoconfiguration, SLAAC)

- Duplicate Address Detection (DAD): ICMPv6 Neighbor Solicitation üzenettel, érvénytelen (::) forráscímről, a vizsgált címre, csak a multicast csoportot terheli

Szállítási protokollok

A szállítási réteg

- Alkalmazások közötti megbízható logikai kapcsolatok a hálózati réteg szolgáltatásaival
- User Datagram Protocol (UDP) és Transmission Control Protocol (TCP)
- Közös képességek: multiplexelés portokkal
- A TCP összeköttetés-alapú, az UDP nem

Socket

- Interfész az alkalmazás és hálózat közt
- Jellemzői: protokoll, forrás és cél IP-port páros
- Lehet datagram (UDP), stream (TCP), vagy raw (IP): közvetlenül az alkalmazásnak
- TCP-n a szerver létrehoz egy hallgatót, amihez a kliensek csatlakoznak, mindegyikhez külön szál indul, ami a kliensének párja, UDP-n nincs dedikált socket mindenkinek

User Datagram Protocol (UDP)

- Nincs kapcsolatépítés vagy -bontás, a megbízhatóságot az alkalmazásra bízza
- Multiplexálást és opcionálisan adatintegritás ellenőrzést nyújt
- Kis késleltetés, egyszerű, kis fejléc, gyorsan eléri a maximális adatátviteli rátát

Transmission Control Protocol (TCP)

- Megbízható protokoll az IP nem megbízható datagram-szolgáltatásán
- Virtuális összeköttetések, kézfogás épül fel és marad fenn a kommunikációra
- Sorrendhelyes, puffert, duplex, piggybacking módon küld vezérlő információt
- Pont-pont: nincs multicast
- Maximum Segment Size (MSS): maximum ennyit küld egy adatrészben, fejlécek nélkül, MTU-val kell egyeztetni, kapcsolatfelépítéskor megbeszélni
- Sorszámozott