Fizikai szintű kommunikáció

Bitfolyamok továbbítása hírközlő csatornákon

Mi az, hogy fizikai szintű átvitel?
- A hálózati rendszernek az a része, amely két végpont között bitek továbbításával foglalkozik
- A bitekből az adó szimbólumokat (jelalakokat) csinál
- Ezek továbbítódnak a csatornán, ennek során torzulnak, zajok ülnek rájuk
- A vevő feladata, hogy a kapott szimbólumsorozatot kiértékelje és az a lehető legjobban megfeleljen a leadottnak

Bitfolyamok továbbítása hírközlő csatornákon
- alapfogalmak
- átvitel sávhatárolt csatornán
- átvitel zajos csatornán

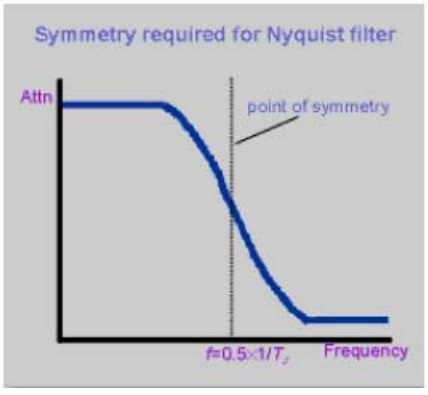
Digitális modulációs eljárások
- ASK, FSK, PSK

Többcsatornás átvitel multiplexeléssel
- FDM, TDM

Hírközlő csatornák a gyakorlatban
- Rézvezetékes csatornák
  - Sodrott érpáras kábelek, strukturált kábelezés
  - Koaxiális kábelek
- Fényvezetős (üvegszálas) csatornák
- Vezetéknélküli csatornák

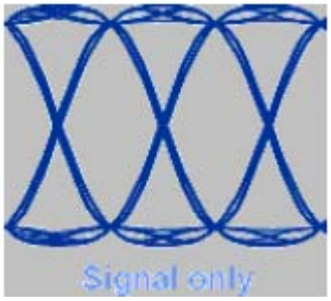
Alapfogalmak
- bit, bitsebesség: bit/s
- szimbólum-sebesség, jelzési sebesség: baud, Bd
- összefüggés: hány bitnyi információt hordoz egy szimbólum?
  - Bináris átvitel esetén a két sebesség egyenlő
  - Többszintű átvitel esetén a bitsebesség többszöröse lehet a szimbólumsebességnek. Például: 8-szintű átvitel esetén $8=2^3$, tehát ha a jelzési sebesség 2000 szimbólum/másodperc, akkor a bitsebesség ennek háromszorosa

Az átviteli szintek csak elméletben növelhetők tetszés szerint nagyra, a gyakorlatban problémát jelent, hogy sávkorlátozott csatornán visszük át a jelet, ezért minél kevesebb harmonikust továbbítunk, a jel annál jobban elkenődik és annál nehezebb a vevőnél a döntés. Impulzussorozat esetén a szomszédos impulzusok egymásrahatnak, ez a **szimbólumközi áthallás (ISI: Inter Symbol Interference)**. Megoldás: lehet ISI, de tartsuk kézben – mintavételkor a többi jel értéke legyen zérus. A jel spektruma a döntés előtt legyen szimmetrikus a jelzési frekvencia (Nyquist frekvencia) felére.

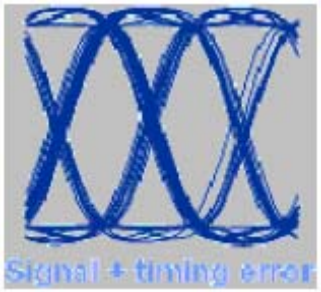


Nyquist törvénye miatt a szükséges legkisebb sávszélesség tehát a szimbólum-frekvencia felének felel meg, például: 1MBaud-os átviteli sebességhez 0,5MHz-es elvi sávszélesség tartozik; a telefonvonal 3100 Hz-es sávszélessége mellett 6200 Bd-dal lehet kommunikálni.
Nyquist tétele: ha az átviteli függvényt eltoljuk a szimbólum-frekvencia egész számú többszöröseire és ezeket összegezzük, konstanst kell kapnunk.

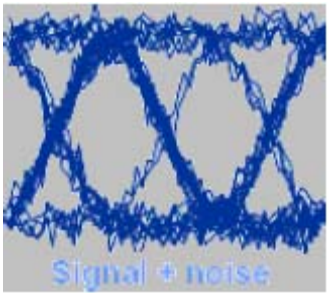
Szemábrák:



csak hasznos jel



jel és időzítési hiba



jel és zaj

Vonali kódolások (hibavalószínűség minimalizálására, hogy ne legyenek pl. hosszú azonos bitsorozatok):

- NRZ, NRZ inverted
- Manchester, Diff. Manchester
- MLT-3, FM-0
- 4B/5B kódolás: minden 4 bitet összefogunk és 5 bittel helyettesítünk, csak a „jókat” használjuk, a többi jelzésre használatos vagy nem használt

Fizikai szintű kommunikáció

Bitfolyamok továbbítása hírközlő csatornákon
2. rész: modulációs eljárások

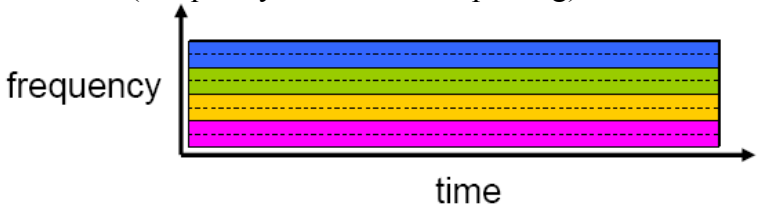
„Moduláció”: a szimbólumsorozat továbbítására egy a jelzési sebességnél általában nagyobb frekvenciájú szinuszos vivőt használunk. A vivő valamely tulajdonságát változtatjuk a szimbólumnak megfelelően:

- ASK: Amplitude-Shift Keying: amplitudómoduláció (ki-bekapcsolásos moduláció)
- FSK: Frequency-Shift Keying: frekvenciamoduláció
- PSK: Phase-Shift Keying: fázismoduláció
    - Többszintű PSK: QPSK (Quadrate PSK), 16QAM

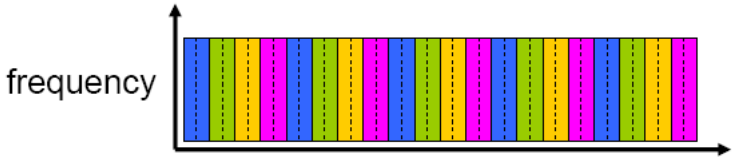
Az eljárás eredményeképpen a jel spektruma áthelyeződik az „alapsávból” a vivő környezetébe.

Többcsatornás átvitel multiplexeléssel: FDM és TDM

- FDM (Frequency Division Multiplexing): frekvenciaosztású nyalábolás



- TDM (Time Division Multiplexing): időosztású nyalábolás



További osztási típusok:

- WDM (Wavelength DM): Hullámhossz-osztású nyalábolás – fényvezetőn
- CDM (Code DM): Kódosztású nyalábolás: az egyes csatornák jele sem frekvenciában, sem időben nem különül el

Fizikai szintű kommunikáció

Bitfolyamok továbbítása hírközlő csatornákon
3. rész: gyakorlati kérdések

Hírközlő csatornák a gyakorlatban
- (Réz)vezetékes csatornák
- Fényvezetős (üvegszálas) csatornák
- Vezetéknélküli csatornák
    - Szabadtéri fényátvitel
    - Infravörös átvitel
    - Rádiós átvitel
        - Földfelszíni
        - Műholdas
        - Ezen belül mobil

Fémvezetős jeltovábbítás
- Két fémvezető és köztük dielektromos szigetelés
- Szaknév: TEM-hullámvezető (Transzverzális Elektromos-Mágneses)
    - Mivel a vezetők távolsága a jel hullámhosszához képest kicsit, csak TEM-alapmódus terjed
- Fő típusai
    - Szimmetrikus érpár
        - Sodrott érpár: UTP (Unshielded Twisted Pair)
    - Koaxiális kábel

Strukturált kábelezés
- Döntően UTP-kábelezés
- A végpontról nem kell előre tudni, mi csatlakozik majd rá (telefon, számítógép, …)
- Központi elosztókból (rendezőkből) minden végponthoz külön kábel megy
- Elemei
    - Főrendező: az épület központi rendezője, itt csatlakozik pl. a telefon-alközpont
    - Gerinckábelezés
    - Alrendezők (szintenkénti kábelezés)
    - Vízszintes kábelezés
    - Csatlakozók

Többszörös hozzáférés

Elvek és technikák

Többszörös hozzáférés szerepe
- Takarékoskodás az átviteli közeggel
- Rugalmas hálózati elérés biztosítása

A rugalmas, kötetlen, akár mobil elérés rádiócsatornán valósítható meg.

A közös használat, a megosztás elvi lehetőségei
- A csatorna átviteli képességének megosztása
    - FDMA: ortogonális de technikailag hátrányos, alkalmazása elsősorban valósidejű környezetben
    - TDMA: ortogonális, rugalmas megosztásra kiváló
    - CDMA: nem ortogonális, de elvileg a legjobb

A hozzáférési módszerek teljesítőképességének osztályozása

- Átvitel (throughput): kiszolgált információ, a fellépő igény függvényében
- Kiszolgálási késleltetés: igény jelentkezése és kiszolgálás közötti idő
- Igazságosság (fairness): teljesül-e a jogosultág szerinti kiszolgálás
- Stabilitás: reakció a túlterhelésre, forgalom dinamikus változására

Körbefordulási idő:
$a = D/T$ ahol D: terjedési idő két állomás között, T: átlag-hosszú csomag továbbítási ideje

Többszörös hozzáférés fajtái

- Közösen használt erőforrás igénybevétele:
  - Szabad: igény szerint
  - Vezérelt: engedély szerint
- Vezérlés módja:
  - Centralizált: egy vezérlő felügyel
    - Lekérdezés (polling): a vezérlő kérdése jelenti a csatornahasználati jogot
      - Körbekérdezés: akinek van csomagja, az elküldi
      - A csatorna információátvitelre használt a csomagtovábbítás alatt, egyébként a hozzáférés szervezése folyik
      - Kihasználtság: fenti két időszak aránya
      - Kiszolgálási késleltetés: a körbejárási idő fele
      - A módszer stabil és fair
    - Próba-szerencse (probing): a felhasználók nagyobb csoportját kérdezi a vezérlő – több igény esetén kezelni kell az ütközést
      - Csoportos lekérdezés, ütközés esetén részekre bontás
      - Kihasználtság javul, kiszolgálási késleltetés csökken, stabilitás megmarad
      - Igazságosság biztosítható
    - Foglalás (reservation): a vezérlő az igények alapján csatornahasználati jogosultságokat oszt ki. Igények gyűjtése: egyedi „csatornákon” vagy „versenyben”.
      - Ha nagy a körbefordulási idő, a lekérdezés hatékonysága rossz
      - Ezért célszerű megosztani az átviteli csatornát foglalási (kisebb hányad) és átviteli részre (nagyobb hányad)
      - A vezérlő a beérkező igények alapján küld engedélyeket
    - Használat: terminálhálózatokban (master-slave)
  - Elosztott: a résztvevők felügyelnek
    - A vezérlés szétosztása miatt:
      - Csökken a szervezési forgalom, tehát nő a kihasználtság
      - Megváltozik a működés biztonsága: kedvező, hogy nincs kritikus pont, de kedvezőtlen a résztvevők megbízhatósága
    - Használat: általános célú LAN-ok (peer-to-peer); ki vezérelje a hozzáférést: önjelölt/mindenki
    - Módszerek:
      - Lekérdezés: explicit kérdés nélkül
      - Polling: explicit kérdés nélkül, de merev időkiosztással. Mint a TDM, de itt a felhasználók maguk dolgoznak
      - Probing: explicit kérdés nélkül; a felhasználók csoportjai együtt kísérlik meg a csatornahasználatot; ha nem kapnak nyugtát, akkor a csoport részenként folytatja, akár addig, amíg egyedül maradnak. A csoportok és a tördelésük előre rögzített.
      - Vezérjel (token) átadás: jogosultság átadása egymás közt
        - A csatornahasználat jogát egy speciális üzenet (token) birtoklása jelenti
        - Megfelelő szabályok alkalmazásával nagyon rugalmas kiszolgálást biztosít
        - Állomások együttműködése szükséges

    - Jó kihasználtság, korlátozott késleltetés
    - Biztosítható az igazságos csatornamegosztás
- Vivőérzékelés (carrier sensing): ellenőrizzük a csatorna foglaltságát. Szabad csatorna esetén használjuk a csatornát, foglalt csatorna esetén „majd később megpróbáljuk”, vagy várakozunk a csatorna felszabadulására, s ekkor vagy rögtön igénybe vesszük, vagy még egy kicsit (véletlen ideig) várakozunk.
    - Egyszerű
    - Nagyon hatékony
    - Érzékeny a terjedési késleltetésre
    - Túlterheltség instabillá teheti
    - Biztosítható az igazságos kiszolgálás

  Fajtái:
    - CSMA/CD (Carrier Sensing Multiple Access / Collision Detection) – vivőérzékelés ütközésdetekcióval, ütközés esetén leállás. Csak vezetékes csatornán használt, rádiós csatornán nem használható.
    - CSMA/CA (Carrier Sensing Multiple Access / Collision Avoidance) – vivőérzékelés ütközéselkerüléssel, készülünk az ütközésveszélyes helyzetekre.
- Foglalt „hang”: segítség a csatorna foglaltságának érzékelésében
    - A vevő kiad egy „foglalt” jelzést egy (célszerűen frekvenciában) elkülönített részcsatornán (ennek észlelésére külön vevő kell)
    - Egy igénybejelentés (RTS) és egy nyugta (CTS) párbeszéd után történik információ-átvitel
    - A két üzenet tartalmazza az átvitel hosszát
- Szabad hozzáférés (Aloha): minél kevesebb szervezés
    - Egyszerű (pure) Aloha: teljesen kötetlen hozzáférés
        - Rossz kihasználtság
        - Instabil
        - Nem korlátos késleltetés
        - Hosszútávon egyenlő (fairness)
    - Réselt Aloha:
        - Azonos hosszúságú csomagok időréshatárokon
        - Ütközésnél teljes fedés
        - Jobb kihasználtság, de még mindig instabil, a késleltetés alig változik
        - Ugyanúgy egyenlő hosszútávon (fairness)
    - Helyfoglaló Aloha:
        - A csatorna egy részén igénybejelentés
        - A felhasználók „visszahallják” az igényeket, mely alapján mindenki egységes döntést hoz

- Kiszolgálás kötöttsége:
  - Merev: „ami jár, az jár”
  - Rugalmas: igény szerinti

Többszörös hozzáférés előnyei, hátrányai:

- Előnyök (nagyban függ a használt közegtől)
  - Gazdasági – kevesebb vezeték
  - Technikai – jobb teljesítőképesség
  - Rádiócsatorna esetén szinte nélkülözhetetlen
- Hátrányok
  - Bonyolultabb algoritmusok
  - Illetéktelen hozzáférés az információhoz

Összefoglalás

- Ez egy másik módszer, mint a multiplexelés
- Fajtái: centralizált és elosztott vezérlésű
- Rádiócsatorna használata esetén meghatározó szerepe van
- Vezetékes csatorna esetén akkor jelentős, ha a felhasználókat felfűzzük (busz, gyűrű topológia)

Kapcsolás

Áramkörkapcsolás, virtuális áramkörkapcsolás, hullámhosszkapcsolás, csomagkapcsolás

Kapcsolás:
- Definíció: azon eljárások/technikák összessége, melyek a kapcsolt hálózatokban két, nem szomszédos csomópont között összeköttetést hoznak létre, mely nem feltétlenül közvetlen, és nem feltétlenül fizikai.
- Számítógép-hálózatban az éppen aktív állomás (csomópont) az adatokat/üzeneteket továbbíthatja:
  - Mindenkihez (broadcasting)
  - Egy/néhány állomáshoz (kapcsolt hálózat)
- Magának a kapcsolt hálózatnak kell gondoskodnia az üzenet kézbesítéséről

Kapcsolás fajtái:
- Áramkörkapcsolás
- Üzenetkapcsolás
- Csomagkapcsolás
- Virtuális áramkörkapcsolás
- Hullámhossz-kapcsolás

Összeköttetés-alapú hálózat: a kommunikáló csomópontok a tényleges adatátvitel előtt a végpontok között end-to-end összeköttetést létesítenek.
Összeköttetés-mentes hálózat: nincs előzetes összeköttetés-létesítés.

Osztályozás:
- Számítógép-hálózatok
  - Kapcsolt
    - Áramkörkapcsolt
      Fizikai kapcsolat a küldő és a fogadó között, mely nem állandó (fel kell építeni, le kell bontani). Minden adat ugyanazon a dedikált fizikai útvonalon halad, a működés valós idejű, a csomópontok nem tárolnak adatokat, torlódás csak az összeköttetés felépítésekor lehet, adatátvitel alatt nem.
      - Távbeszélő hálózat
      - Hullámhossz-kapcsolt hálózat (WDM – Wavelength Division Multiplexing). Megvalósítás: fénytörésen alapuló multiplexelés.
        Fajtái:
        - CWDM (Course WDM) – kissűrűségű, legfeljebb 16 különböző hullámhossz egy üvegszálon.
        - DWDM (Dense WDM) – nagysűrűségű,

      Kapcsolók általános felépítése: kapcsolóelem, ami a tényleges kapcsolást végzi és kapcsoló-vezérlő, ami a kapcsolóelemeket választja ki. Kapcsolóelemek megvalósítása multiplexeléses, fajtái:
      - Térosztásos – SDM (Space Division Multiplexing) – legegyszerűbb ebből a crossbar, bonyolultabb a többfokozatú térosztásos kapcsoló.
      - Időosztásos – TDM (Time Division Multiplexing): N db azonos sebességű csatornáról érkező adatok ráhelyezése egy N-szeres sebességű csatornára. A kapcsolás időréscserélővel (TSI – Time Slot Interchanger) történik.
      - Idő-térosztásos (TSDM)
      - Idő-tér-időosztásos (TSTDM)
    - Üzenet- és csomagkapcsolt
      Üzenetkapcsolt: nincs közvetlen kapcsolat, azaz összeköttetés-mentes, gráfban két pont közti útként képzelhetjük el. Előny, hogy javul a csatorna kihasználtsága a megosztott használat miatt, a csomópontok bufferelési képessége csökkenti a torlódásra való érzékenységet, az üzenetekhez prioritás rendelhető és a broadcasting támogatott. Hátrány viszont, hogy a késleltetések miatt nem

alkalmas valós idejű átvitelre.
Csomagkapcsolt: az üzenetet csomagokra bontja szét a küldő, mely tartalmazza a küldő és a címzett csomópont azonosítóját, ill. a csomag helyét az üzenetben. A címzett állítja össze a csomagokból az üzenetet.
Hálózati eszközök: switch (helyi hálózaton belüli kapcsoló), router (hálózatok közti kapcsoló).

- Összeköttetés-alapú (virtuális áramkörkapcsolás)
  Csomópontok gráfjában két pont közt létesít utat (tehát itt is van felépítés, átvitel, lebontás), minden csomag ezen az úton fog haladni. A virtuális áramköröket egy helyi, az adott csomóponton érvényes azonosítóval (VCI – Virtual Circuit Identifier) azonosítjuk.
  Csomagtípusok:
  - CR (Call Request), fejrésze: […|VCI|…|DA (Dst. Addr.)|…|SA (Src. Addr.)|…]
  - CC (Call Confirm), fejrésze: ugyanez
  - Adatcsomagok, fejrésze: […|VCI|…]

  Kapcsolat felépítése
  - CR csomag továbbítása a csomópontokon az NRT (Network Routing Table) alapján
  - Egy NRT bejegyzés tartalma: [DA|…|next hop|interface]
  - Felépítéshez (CR csomag továbbításához) a csomópont:
    - Keres egy szabad logikai csatornát
    - Bejegyzést készít a kimenő porthoz tartozó virtuális áramkörtáblába, amibe feljegyzi a csomaggal együtt érkezett bemeneti VCI-t, a kimeneti port számát és a kimeneti VCI-t.
    - A csomagban felcseréli a be- és kimeneti VCI-t
    - Elküldi a csomagot a kimeneti porton át
  - VC-tábla egy bejegyzése: [bemeneti port|VCI_{in}|kimeneti port|VCI_{out}]

  Kapcsolat alatti adatátvitel
  - Adatcsomagok továbbítása a kapcsolat felépítésekor kialakított VC-táblák alapján:
    - A kapcsoló megkeresi a bementi porthoz és VCI_{in}-hez tartozó bejegyzést
    - Be- és kimeneti VCI cseréje a csomagban
    - Továbbküldés a kimeneti porton

  Virtuális áramkörkapcsolás fajtái:
  - X 25
  - ATM
  - Frame Relay
  - MPLS
- Összeköttetés-mentes (datagram kapcsolás)
  Minden csomag önálló entitás, tartalmazza a cél teljes címét. Csomópontban a kimeneti port megválasztásának alapja a routing-tábla, mely minden lehetséges célcímhez tartalmazza a kimeneti portot és az ahhoz tartozó „költség” értékét.
  - IP-hálózat

- Broadcast
  - Ethernet LAN
  - Csomagkapcsolt rádióhálózat
  - Műholdas hálózat

Hívásvezérlés; címzés

Hívások felépítése, jelzésrendszerek áramkörkapcsolt hálózatokban; elnevezés, címzés

Hívásvezérlés (Call Processing)

- A hívások (kapcsolatok) felépítése, fenntartása, lebontása
- Az ehhez szükséges jelzések rendszere
  - Sávon belüli (in-band) – jelzésátvitel, hagyományosan az analóg telefonvonalon

    - Sávon kívüli (out-of-band) – külön csatornákon történő jelzésátvitel
      közös csatornás – CCS (Common Channel Signaling)
        - Közös fizikai/virtuális jelzéscsatornák
        - Rugalmas, jobb sávszélesség-kihasználás
        - IDSN-ben: külön digitális csatornákon
- Hívásvezérlő protokollok

ISDN

- Mi az ISDN (Integrated Services Digital Network):
    - Végpontok közötti átlátszó digitális csatornák
    - Közös csatornás jelzésrendszer
    - Univerzális interfészek
- CCS az ISDN-ben:
    - Felhasználó és hálózat közötti jelzésátvitel az UNI-n – User-Network Interface
      UNI:
        1) BRI (Basic Rate Interface): 2B+D
        2) PRI (Primary Rate Interface): 30B+D
        (B = 64 kbit/s, D = 16, 64 kbit/s)
      Protokollja: ITU Q.931
        Protocol discriminator
        Length of Call Reference
        Call Reference: 1-15 byte hosszú azonosító
        Message Type: 1 byte hosszú, megadja a jelzésüzenet típusát. Példák: Alerting,
            Call Proceeding, Connect, Connect ACK, Setup, Setup ACK, Disconnect
            Status Enquiry, Status
        Information Elements: az adott jelzésüzenethez szükséges információk
    - Hálózaton belüli jelzésátvitel az NNI-n – Network-Network Interface

Elnevezés és címzés

- Elnevezés: egyedi név hozzárendelése (pl. internetcím)
- Címzés: egyedi cím hozzárendelése (pl. IP-cím)
- Név-cím átalakítás: címfeloldás
- Hierarchikus szervezés a könnyebb útvonalválasztás érdekében: mivel alhálózatok alakíthatók ki, csak a határokon kellenek routingtáblák
- A telefonhálózat címzési rendszere: szabványa: ITU E.164
- ENUM (tElephone NUmber Mapping): lehetővé teszi, hogy telefonszámokat DNS-ekkel kapcsoljunk össze

Az Internet címzési rendszere

- IP-cím
- Végpontok helyett interfészek címzése
- Címek hierarchiája:
    - A osztály: 8+24: [0-network|host]
    - B osztály: 16+16 [10-network|host]
    - C osztály: 24+8 [110-network|host]
- Alhálózatokra osztás (subneting)
- Osztálynélküli tartományközti irányítás (CIDR – Classless InterDomain Routing)
- DHCP (Dynamic Host Configuration Protocol)
    - A végpont csak akkor kap címet, amikor aktív; nem mindig ugyanazt kapja
    - Ezért ugyanaz a cím több hostra kiosztható, ha nem egyszerre aktívak
    - A címallokálást a DHCP-protokoll végzi

Névfeloldás

- Névszerverek
- DNS (Domain Name System) végzi

Adatkapcsolati rétegbeli címfeloldás
- a DNS leképezi a címet egy hálózati címre
- ha viszont a végpont egy LAN-on van, Ethernet-címre kell továbbfordítani, ezt a végponthoz legközelebbi router teszi meg; kifelé ugyanez kell
- ARP (Address Resolution Protocol), RARP (Reverse ARP) végzi ezeket az átalakításokat

Routing

Útvonalkijelölés, -választás, routing

Útvonal-kijelölés és –választás a csomópontok routing táblái alapján. Ennek kitöltése lehet:
- manuális
- automatikus
    - centralizált:
        - tapasztalatok alapján előre becsült forgalmi viszonyok szerint
        - folyamatos figyelés
    - elosztott
        - distance-vector: a csomópontok elmondják szomszédjaiknak a hálózatról alkotott elképzeléseiket (melyik csomópont milyen távol van). Problémát jelenthet linkszakadás esetén a végtelenig számolás, ezért tárolni kell azt is, melyik csomóponton keresztül érvényes a távolságvektor.
        - link-state: a csomópontok elmondják mindenkinek a szomszédjaikról nyert tapasztalataikat (linkek aktuális állapota). Küldés: felügyelt elárasztással.

Autonóm rendszerek (AS – Autonomous System; Routing Domain): olyan egység, melyen belül egységes routing policy van. Egyetlen hálózat, vagy hálózatok csoportja; egyetlen szervezeti egységhez tartozik. Globálisan egyedi azonosítót kap: ASN (AS Number).

Feladatütemezés, csomagkezelés

Scheduling

Sokszor van véges erőforrással dolgunk, melyet néha nagyobb mértékben kellene igénybevenni, mint arra képes, máskor meg nincs eléggé kihasználva, viszont hosszú távon átlagban képes az igények kielégítésére. Tehát időnként várakozni kell az erőforrásra – különböző elvek, stratégiák alapján képezhetünk várakozási sort úgy, hogy az adott kiszolgálási feltételek, elvárások a lehető legjobban teljesüljenek.

Véges erőforrás:
- linkek átviteli képessége
- csomópontok tárolási képessége
- csomópontok feldolgozási képessége

Témakörök:
- Bevezetés
    - Verseny van az erőforrásokért, jó okkal nem használunk mindig FCFS-t
    - Feladatütemezési módszer kell az igazságos megosztáshoz és a kiszolgálási minőség garantálásához
    - A módszer összetevői
        - Kiszolgálási sorrend meghatározása: késleltetés
        - Kiszolgálásra várakozók túlcsordulásánál igény-eldobási stratégia: vesztési arány
    - Megőrzési törvény: $\text{sum}(p_i * q_i) = \text{konstans}$: átlagos késleltetések forgalom-részarányokkal súlyozott összege állandó, azaz valakinek előnyt biztosítani csak mások rovására lehet

- Követelmények
  - Egyszerű megvalósíthatóság
  - Igazságosság: részesedés a költségviselés arányában
    - Gyakran egyenlő jogosultságok de eltérő igények: logikus, hogy a kicsiknek adjunk, amennyit kérnek, a maradékot osszuk szét a nagyok közt
    - Ez a max-min igazságos megosztás elve
      - Erőforrás-kiosztás a növekvő igények szerint
      - Senki sem kap többet a kértnél
      - A kielégítetlen igények egyenlően osztoznak a maradékon
  - Védelem: a többiek védelme azzal szemben, aki nem tartaná be a szabályokat
  - Teljesítménykorlátok biztosítása (garantált kiszolgálásnál)
    Kiszolgálási garancia és használati kötelezettség-vállalás
    - Determinisztikus: az összeköttetés minden csomagjára teljesülnie kell – egyszerű ellenőrzés, rossz kihasználtság
    - Statisztikus: a csomagok adott hányadára teljesülnie kell – bonyolult ellenőrzés, jó kihasználtság

    QoS-paraméterek (teljesítmény-korlátok):
    - Sávszélesség: garantált minimális, az összeköttetésre
    - Késleltetés
      - Legrosszabb eset: minden más összeköttetés a lehető legrosszabbul viselkedik
      - Átlagos érték
      - Csomagok adott hányadára vonatkozó jellemző
    - Késleltetés-ingadozás: kiegyenlítési lehetőség a vevőben, nem lehet akármekkora
    - Csomagvesztés
  - Egyszerű és hatékony beengedés-szabályozás (garantált kiszolgálásnál)
    - A QoS-paraméterek csak beengedés-szabályozás (Admission Control) mellett biztosíthatók
    - Gyorsan kell eldönteni, hogy az új igény kiszolgálható-e
    - Nem eredményezhet kihasználatlanságot
- Lehetőségek
  Négy alapvető szabadsági fok a tervezésnél
  - Prioritási szintek száma
    n szint esetén a k-ik szintű igényt csak akkor elégítjük ki, ha nincs magasabb prioritású igény. Egyszerű, de éhezés léphet fel. Megoldás: megfelelő beengedés-szabályozás.
  - Az egyes szinteken
    - Munkamegőrző
      Csak akkor üres a kiszolgáló, ha nincs várakozó csomag
    - Nem munkamegőrző mód
      Vannak akkor is üres időszakok, ha van várakozó csomag, csak az „esedékessé” válókat továbbítja. Így nem halmozódnak fel börsztök, csökken a tárolóigény és a késleltetés-ingadozás, egyszerűsödik a vállalható teljesítmény-korlát meghatározása. Korrekt forgalomjellemzést kíván meg a forrásoktól és azt, hogy ehhez tartsák is magukat.
  - Igények csoportosítási mértéke az egyes szinteken belül
    - Összevonás (aggregation), összeköttetések összevonása, közbenső eset a két véglet között
    - Két véglet
      - Minden igény együttes jellemzése – ugyanazt a QoS-t kapják
      - Minden összeköttetésre saját QoS
    - Csomagkapcsolt hálózaton technikailag nem lehet erőforrással győzni az egyedi igények kezelését
    - Közbenső eset: osztályokba sorolás – az adott osztályba soroltak ugyanazt a QoS-t kapják, az ütemező nem tud különbséget tenni a csoport tagjai közt, ezért „együtt sírnak, együtt nevetnek”.
  - Kiszolgálási sorrend az egyes szinteken belül

        - FCFS: egyszerű, de
            - Nem enged meg kivételt pl. késleltetés-érzékeny csomagokra
            - Nem biztosít védelmet, nem max-min elvű
            - Erőszakosságra sarkall
        - Nem-FCFS: előnyös, de bonyolult – meg kell határozni és jelezni a sorrendet (tagging)
- Best effort ütemezők
    - Általánosított processzor-megosztás: GPS (Generalized Processor Sharing)
        - Elve: max-min megvalósítása
        - Alapelv: úgy leszünk igazságosak, hogy mindenki feladatának egy 0-hoz tartó szeletét végezzük el
        - Nyilván ez ilyen formában csak elvileg működik, a gyakorlatban ehhez viszonyítunk
        - Megvalósítás:
            - Logikailag minden csomag külön várakozási sorban
            - RR kiszolgálás
            - Akinek nincs igénye, kimarad
            - Prioritás kezelése az időszelet méretének változtatásával
            - Ez max-min értelemben fair szolgáltatás
    - Súlyozott Round-Robin
        - Jó, ha azonos csomaghosszak és azonos súlyú összeköttetések vannak
        - Kiszolgálás körben csomagonként
        - Átlagos csomaghossz jó közelítésű ismerete kell
        - Rövidtávon nagyon igazságtalan lehet
    - Deficit RR
        - Előre ismeretlen átlagos csomaghosszra
        - Definiálunk egy kiszolgálási adagot (byte-okban) és egy felhasználói hitelszámlálót
        - A sor elején álló csomagot akkor szolgáljuk ki, ha az nem hosszabb, mint az adag. Ha hosszabb, az adagot hozzáadjuk a hiteléhez és a következő körben ennek alapján döntünk.
    - WFQ (Weighted Fair Queuing), PGPS (Packet-by-packet GPS)
        - Alapötlet: kiszámítjuk a csomagok távozási időpontját, mintha GPS-szel szolgáltuk volna ki őket és ezt a sorrendet alkalmazzuk a kiszolgálásra. Nem a távozási időpont, hanem a sorrend érdekes, ezért a távozást jellemző értéket befejezési számnak nevezzük.
        - Bitenkénti kiszolgálás
        - Ha ismerjük a ciklushosszt (arányos az aktív felhasználók számával) és a ciklusszámot, a befejezési szám értéke: $F(i,k,t) = \max(F(i,k-1,t),R(t)) + P(i,k,t)$
          $F(i,k,t)$ – az i. felh. bef. száma a t. időpontban
          $P(i,k,t)$ – az i. felh. bef. t-ben beérk. k-ik csomagjának hossza
          $R(t)$ – ciklusszám t-ben
    - WFQ javított változatai: SCFQ (Self-Clocked FQ), STFQ (Start-Time FQ)
- Ütemezés garantált kiszolgálás esetén
    - Súlyozott igazságos sorképzés (WFQ)
    - Egyéb módszerek, pl. virtuális óra, legkorábban esedékes ütemezők (EDD)
- Csomageldobás

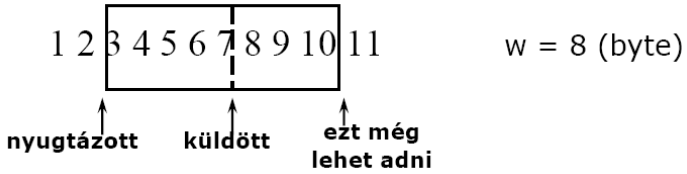
Forgalomszabályzás (flow control)

Forgalomszabályzás (flow control)

- Definíció: olyan módszerek, melyek lehetővé teszik, hogy egy forrás az aktuális átviteli sebességét igazítsa hozzá a vevőhöz és a hálózatban rendelkezésre álló kiszolgálási sebességhez
- Elvárások
    - Egyszerű megvalósíthatóság
    - Kis hálózati erőforrásigény (átviteli képesség, csomóponti tárolás)
    - Hatékonysága független legyen a szabályzott források számától, azaz O(1) legyen O(n) helyett

    - Igazságos erőforrás-megosztás
    - Stabilitás
- Fajtái
    - Nyílthurkú (vezérlés)
        - Kommunikáció előtt a felhasználó és a hálózat forgalmi paramétereket egyeztet
        - A hálózat dönt a beengedésről – beengedésszabályozás (admission control)
        - A hálózat ennek megfelelően erőforrásokat dedikál
        - A működés során felügyel
    - Forgalomleírók
        - Paraméterkészlet, jellemzi az adó viselkedését
        - Alapját képezi a szolgáltatási szerződés forgalmi részének
        - Bemenő adata egy forgalomszabályzónak (regulator, a túlzott forgalmat késlelteti) és egy felügyelőnek (policer, a túlzott forgalmat beszűnteti)
        - Egyszerű példa: csúcssebesség, átlagsebesség
        - Követelmények
            - Megjelenítési képesség (representativity) – hosszútávú információt adjon a forgalomról
            - Ellenőrizhetőség (verifiability) – a hálózat gyorsan és olcsón ellenőrizhesse a forgalom megfelelőségét
            - Megőrizhetőség (preservability) – az út mentén
            - Használhatóság (usability) – a felhasználó képes legyen megmondani, a hálózat tudjon mérlegelni
    - Zárthurkú (szabályozás)
        - Muszáj használni, ha
            - Nincs erőforrásfoglalás
            - Túlfoglalást alkalmazunk
        - Típusai
            - Első generációs módszerek: csak a nyelő képessége
                - On-off: a nyelő engedélyezi az adást
                - Stop-and-wait: a küldő egy csomag után vár a nyugtára
                  Kihasználtság: $U = (L / R) / (RTT + L / R)$, ahol
                  RTT: round-trip time, oda-vissza idő
                - Statikus ablak: a küldő az ablak méretének megfelelő számú csomag küldése után vár nyugtára – az adónak lehet több, adásban lévő, még nem nyugtázott csomagja
                    - Sorszámozás kell
                    - Tárolás kell az adóban

                  Kihasználtság: $U = 3 * U_{\text{stop-and-wait}}$, ha 3 az ablakméret
                - Csúszóablakos forgalomszabályzás



            - Második generációs módszerek: a nyelő és a hálózat képessége
    - Hibrid

Torlódásvezérlés (congestion control)

- Linkek és csomópontok időszakos túlterheltsége megszűntetésének módszerei
    - Ez szólhat a torlódás megelőzéséről is – ilyen értelemben a forgalomszabályzás az eszköz a torlódásvezérléshez

Forgalommenedzselés (traffic control)

Forgalommenedzselés (traffic control)

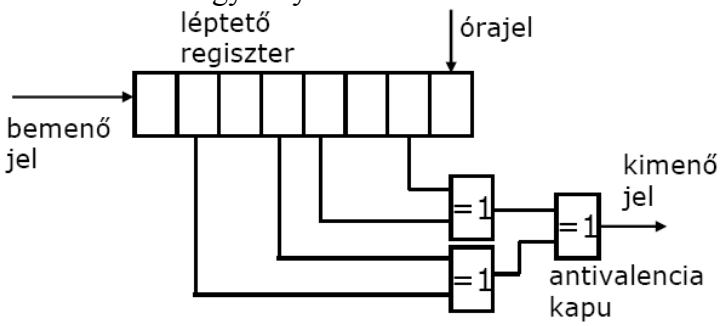
- Szabályok és intézkedések, melyek lehetővé teszik a különféle kiszolgálási igények hatékony kielégítését
- Forgalommodellezés
  - A modell egy alkalmazás összegzett viselkedésének várható jellemzőit tartalmazza
  - Ismerni kell az egyedi igényeket és azok tipikus viselkedését
  - Fajtái
    - Tapasztalati modell
    - Matematikai modell
  - A forgalommodelekről
    - Telefon-forgalommodell
      - Hívásérkezési modell
      - Hívástartási modell
    - Internet-forgalommodell – szempontok:
      - Session-ök közötti beérkezési idő
      - Egy-egy session (összeköttetés) időtartama
      - Egy-egy session adatforgalma
      - Egy-egy session-ön belül a csomagok közti időköz
- Példák forgalomosztályokra
  - Két fő osztály → két fő kiszolgálási típus
    - Garantált
    - Best effort
  - Alosztályok
    - ATM Forum alosztályok:
      - Garantált: CBR, VBR
      - Best effort: ABR, UBR
    - IETF alosztályok
      - Intolerant: Guaranteed service
      - Tolerant: Controlled-load
      - Best effort: interactive burst, -bulk, async bulk
- Forgalommenedzselés időskálája és eszközei
  - < RTT – feladatütemezés, szabályozás és ellenőrzés, routing (ö.k. mentes hál.), hibakezelés
  - k * RTT – flow control, ismétlés, újratárgyalás
  - session – jelzés, admission control, tarifálás, routing (ö.k. alapú hál.)
  - egy nap – csúcsidőszak tarifálása
  - >= egy hét – kapacitástervezés

Hibakezelés (error control)

A hibák fajtái és keletkezésük okai

- Végpontok közti átvitel során
  - Bithiba – átállítódásos, törléses
    Okai:
    - Véletlen zaj – normáleloszlású – termikus zaj – független bithibákat okoz
    - Impulzuszaj – nem normáleloszlású – forrásai: erősáramú berendezések – hibacsomókat okoz
    - Hiba a szinkron elvesztése miatt – túl hosszú azonos minták miatt – hibacsomókat okoz
      - Megoldások
        - Kódolási technikák, pl. Manchester-kód

    - Bitkeverés a bemenet léptetőregiszterbe-vezetésével és egyes bitek összekombinálásával – vételi oldalon ugyanilyen módon dekódolható.



      Ez nem tökéletes megoldás, mindig lehet csupa 0 vagy csupa 1 sorozatot kapni; ill. hibásan vett bit hibacsomót okoz.
  - Bithibák mobil hálózatokban
    - Cellás mobilhálózatokban a cellaváltás fading-et okoz – megelőzhető a frekvenciakihasználtság-romlásának árán (előbb váltunk, utána engedünk el)
    - Wireless átvitel során a terjedés útjába eső közeg, tereptárgyak visszaverődést és fading-et okoznak
  - Csomaghiba
    - Csomagvesztés
    - Csomagtöbbszöröződés
    - Csomagsorrend felborulása
- Hibakezelés: bármely szinten észlelhető és javítható legyen a hiba

Alapvető hibajavítási stratégiák – alapötlet: redundancia bevitele
- Visszirányú hibajavítás (BEC – Backward Error Correction), azaz automatikus ismétlés-kérés (ARQ – auto repeat request)
- Megelőző hibajavítás (FEC – Fwd Err Corr) – hibajavító kodolás; a vételi oldalon javítás
- Hibakezelő kódolás (ECC – Error Control Coding)
  - Blokk-kódolás
  - Konvolúciós kódolás

Csomaghibák kezelése
- Csomagvesztés
  - Okok
    - Wireless hálózatokban burst-ös bithibák
    - Vezetékes hálózatokban átmeneti csomópont-túlterheltség
- Csomagtöbbszöröződés
  - Okok
    - Csomagvesztés miatti újbóli elküldés, amire az adó nem kap nyugtát az időkorláton belül
    - Mert a nyugta el sem indult, vagy elveszett
- Csomagsorrend felborulása – átsorrendeződés és beszúrás
  - Ugyanazon kapcsolat csomagjainak sorrendje felborulhat, ha azok különböző utakon mennek
  - Csomagbeszúrás történhet, ha a csomag fejrésze észrevehetetlenül hibásodik meg
    - Egy vevő az 1-es és 2-es VCI-n vár csomagokat
    - Egy csomag fejrészében a 2-es VCI 1-be íródik, nem evhető észre
    - Ez az 1-es VCI-nél egy beszúrt csomagot eredményez
- Csomaghibák észlelése – sorszámozás
  - Minden csomag fejrészébe egy növekvő számláló értéke a küldő oldalán
  - Alsó korlát a sorszám méretére (*n* hosszára bitekben mérve), tényezők
    - MPL (Max Packet Life)
    - T_{max} idő, ameddig a küldő a nyugtát várja, ezen túl ismétel
    - A max *A* idő egy csomag vétele és a rá következő nyugta küldése között

- A küldő *R* csomagtovábbítási sebessége (csomag / s)

Így: $2^n >= (2 * MPL + T_{max} + A) * R$

Példa:

- MPL = 120 s, T_{max} = 60 s, A = 0,5 s, csomagméret = 40 byte, adatsebesség = 2Mbit/s
- Így: $R = 2 * 10^6 / 40 * 8$ csomag/s
- Ekkor n >= 21 bites sorszámozás kell!

o Az észlelés történhet

- Időkorláttal – minden csomag elküldése után timeout, ha a lejáratig nincs ACK → ismétlés
  - Problémák
    - Ha túl kicsi: felesleges ismétlés
    - Ha túl nagy: vontatott hibajavítási folyamat
  - Hossz
    - Rögzített: RTT 1-2-szerese
    - Változó: a mért RTT-től függően
- Negatív nyugtázással (NACK)
  - Hibás csomag vagy hézag esetén a vevő NACK-ot küld, erre az adó ismétel
  - Probléma:
    - a NACK is elveszhet
    - csomaghiba torlódáskor szokott lenni, a NACK küldése tovább terheli a hálózatot

- Csomagismétlési módszerek
  - ARQ (auto repeat request) körébe tartozó módszerek
  - Csomagvesztésnél a csomagismétlési stratégia dönt arról, hogy melyik csomagot kell ismételni
  - Stratégiák:
    - Stop-and-wait – egyszerű, de nem hatékony
      - Az adó minden csomag után nyugtát vár, csak annak fogadása után küld újra
      - A vevő ACK/NACK üzenettel minden csomagot nyugtáz
    - Go-back-n – egyszerű, biztonságra törekszik, de túlterhelés miatti hibáknál csak ront a helyzeten, külső ellenőrzés nélkül ez odáig fajulhat, hogy a hálózaton csak csomagismétlés van
      - Csúszóablak-típusú, az ablakban az elküldött, de még nem nyugtázott csomagok sorszámai vannak
      - Minden elküldött csomag megnöveli az ablak méretét
      - Minden pozitív nyugta csökkenti az ablak méretét
      - A küldés és ACK-fogadás elcsúsztatja az ablakot
      - Ismétléskérésnél az ablakban levő összes csomagot újraküldjük

      Hatékonyság
      - *p* csomaghiba-valószínűség és W max ablakméret mellett az adó legfeljebb (1-p)/(1-p+Wp) százalékban használja a sávszélességet nem-ismételt csomagok továbbítására
      - példa: p=0.01, W=250 → (1-0.01)/(1-0.01+0.01*250) = 28.3%, ha $p=10^{-5}$, akkor 99.7%
    - Szelektív ismétlés – hatékony, de bonyolult és pufferigényes
      - A küldő csak a kért csomagokat ismétli
      - A vevő csak a hibás csomagokat dobja el
      - A hibásan vett csomag utáni jó csomagokat bepuffereli

Összefoglalás

- Hibák okai: bit- és csomaghibák
- Hibajavítási stratégiák: visszirányú hibajavítás és hibajavító kódolás
- Hibajavító kódolás módszerei: paritáskód, Hamming-kód, CRC, Reed-Solomon kód, konvolúciós kódok
- Csomaghibák kezelése: go-back-n és szelektív ismétlés

ATM

Példa az eddig megismert elvek megvalósítására

Mi az ATM?
- Átviteli és kapcsolási módszer, és az ezen alapuló távközlőhálózati rendszertechnika
- Összeköttetés alapú, azon belül ún. gyors csomagkapcsolási módszer, virtuális összeköttetések épülnek fel
    - Gyors: rövid csomagok, nincs forgalomszabályozás, nincs linkenkénti hibajavítás
    - Rövid, fix hosszúságú adatcsomagok
- Célkitűzései:
    - Különböző típusú forgalmak átvitele: beszéd, kép, videó, adat
    - Tág átvitelisebesség-tartomány: néhányszor 64kbit/s ~ 2.4Gbit/s
- Ma a távközlő hálózatokban használt (pl. 3G mobil rendszerek gerinchálózatánál)
- Elnevezés: a távközlésben addig egyeduralkodó, SDH-n alapuló STM (Synchronous TM) ellentéte
- Minden összeköttetéshez specifikus QoS-t képes biztosítani

Működése: kétszintű virtuális kapcsolatok:
- virtuális csatorna
- virtuális útvonal

Használt funkciók
- Hívásvezérlés (Call Control): mert összeköttetés-alapú, vannak ATM jelzésrendszerek
- Címzés
- Routing: mert ahhoz, hogy a csomópontok kezelni tudják a virt. kapcsolatok csomagjait, előzetesen útvonalat kell kijelölni és menedzselni
- Scheduling: fontos a QoS biztosításához
- Forgalommenedzsment: a különböző típusú szolgáltatásminőség-igények kielégítéséhez
- Forgalomszabályozás NINCS (linkenkénti), hogy gyors legyen
- Hibakezelés NINCS (linkenkénti), hogy gyors legyen és ma már elég megbízhatóak az összeköttetések

<u>Az ATM-elv, a csomagok (cellák) felépítése</u>
A cellamultiplexálás elve:
- A bemeneti adatfolyam bájtjaiból rövid, állandó hosszúságú adategységeket, ATM-cellákat képzünk
  [fej (5 byte) | payload (48 byte)]
- A multiplexer egy bufferben tárolja az aszinkron módon, eltérő sebességgel érkező, különböző jellegű adatfolyamokból képzett cellákat
- Ezeket aztán FCFS vagy más eljárás alapján illeszti be a kimenő szinkron ATM adatfolyamba, 2 Mbit/s .. 2 Gbit/s között választható sebességgel

A cella fejrészének felépítése
[GFC (4) | VPI (8) | VCI (16) | PT (3) | CLP (1) | HEC (8)] UNI
[VPI (12) | VCI (16) | PT (3) | CLP (1) | HEC (8)] NNI
- GFC (Generic Flow Control) – általános áramlásvezérlés: nem használt, nincs megfelelő protokoll
- VPI (Virtual Path Identifier) – virtuálisútvonal-azonosító: két ATM-csomópont közötti útvonalhoz
    - 2^8 virtuális út az UNI-n (8 bites mező)
    - 2^{12} virtuális út az NNI-n (12 bites mező)
- VCI (Virtual Circuit Identifier) – virtuáliscsatorna-azonosító: két ATM-csomópont között vagy egy virtuális útvonalon belül
    - 2^{16} VCI (16 bites mező)
- PT (Payload Type) – hasznos rész típusa: hasznos adatot hordozó és menedzseléshez szükséges cellatípusok megkülönböztetése

- CLP (Cell Loss Priority) – cellavesztési prioritás
  - = 0: magas prioritás (nem dobható el – adatátvitel)
  - = 1: alacsony prioritás (eldobható, ha torlódás van – video, hang)
- HEC (Header Error Check) – fejrész-hibaellenőrzés: CRC képzése a fejrészre, egyszeres hiba javítható, többszörös jelezhető (ekkor eldobjuk a cellát)

A kétfajta virtuális kapcsolat (VPI és VCI)

A VPI/VCI pár csak együtt értelmes, nevezik címkének is. Lokális érvényűek két szomszédos csomópont között. Az ATM kapcsológépek kapcsolótáblákat tartanak fenn, melyek minden összeköttetésre vonatkozóan összerendelik a bejövő és kimenő VPI/VCI értékeket és a bejövő/kimenő portokat.

Összeköttetés típusai:
- PVC (Permanent VC) – állandó VC, rendszermenedzsment állítja be, hosszú ideig fennmarad
- SVC (Switched VC) – kapcsolt VC, az ATM-jelzésrendszer segítségével építi fel a hálózat, valós időben, tetszőleges időtartamra

Az ATM-kapcsolás

Az ATM-címkekapcsolás (ATM label switching)
- A kapcsoló beolvas egy bejövő cellát egy adott bemeneti porton
- Kiolvassa a fejrészből a VPI/VCI értékeket, ezek és a bemeneti port alapján kikeresi a kimeneti port számát és az új VPI/VCI értékeket
- A bemeneti címkeértékeket felcseréli a kimenetiekkel
- Továbbküldi a cellát a címkéhez tartozó porton

SVC kapcsolat felépítése
- jelzési csatornák
  - default pont-pont jelzési csatorna, előzetesen VPI=x / VCI=5-re konfigurálva
  - dedikált jelzési csatorna, melyet a default metajelzési csatornával (VPI=x / VCI=1) hoznak létre
- jelzésrendszer:
  - jellegzetes hívásüzenetek a kapcsolat felépítésekor: setup, call proceeding, connect, connect ack
  - bontáskor: release, release complete

Az ATM átviteli és kapcsolási mód fő funkciói:
- összeköttetés-alapú csomagkapcsolás
- nincs linkenkénti hibavédelem és flow control, mert a hibavalószínűség kicsi, ha pedig mégis van elvesztett vagy hibás cella, a helyreállítás egy magasabb rétegbeli protokoll (pl. TCP) feladata
- címzés
  - minden ATM végkészüléknek és kapcsolónak egyedi ATM címe van
  - a magán- és nyilvános hálózatokban eltérő címzés
- QoS biztosítása
  - Minden ATM-összeköttetéshez QoS kategória kapcsolódik
  - Az ATM-hálózat garantálja a megállapodás szerinti QoS-t minden összeköttetéshez

Az ATM által a QoS-hez használt forgalomszabályozás

Forgalom jellemzése
- PCR (Peak Cell Rate): csúcs-cellasebesség
  A forrás által az ATM-hálózatba bebocsátható maximális cella/sec sebesség. A PBR (Peak Bit Rate) is használható a PCR helyett.
- SCR (Sustained Cell Rate): tartósan fennálló cellasebesség
  - Kiszámítjuk az egymást követő rövid T hosszú időszakokra az átlagos cellaszámokat. Ezen átlagok maximuma adja az SCR-t.
  - T nem definiált szabványosan, gyakorlatban 1 sec szokott lenni

    - Az SCR nem azonos a forrás átlagos cellasebességével (csak ha T azonos a teljes adási idővel)
      Average cell rate <= SCR <= PCR
- MBS (Maximum Burst Size): max cellaszám, melyet a forrás csúcs-cellasebességgel adhat
- Burstiness: burst-összég – milyen mértékben csomósodik a forrás által kibocsátott cellafolyam
- Inter-arrival times: beérkezési időközök, valószerű, hogy ezek korreláltak
- CDVT (Cell Delay Variation Tolerance)
- BT (Burst Tolerance)

Szaványosított forgalomleírók:
- ATM Forum: PCR, SCR, MBS, CDVT
- ITU-T: PCR

QoS paraméterek
- CLR (Cell Loss Rate): ATM kapcsológépek méretezéséhez és hívásengedélyező algoritmusokhoz
- CTD (Cell Transfer Delay): küldőtől a fogadóig tartó továbbítás ideje
    - Fix cellaátviteli késleltetés: terjedési késleltetés, a rendszer jellemzője, belső késleltetése
    - Változó cellaátviteli késleltetés: sorbanállási késleltetés a kapcsológépekben
- CDV (Cell Delay Variation) = jitter, cellakésleltetés ingadozása: azt jellemzi, mennyire ingadoznak a beérkezési időközök a cellánál (fontos a beszéd és video továbbításakor)
- Peak-to-peak CDV (max CDV)
- Max CTD
- CER (Cell Error Rate): payload-hibás és hibátlan cellák aránya a forrás által leadott összes cellára
- CMR (Cell Misinsertion Rate): tévesen kézbesített cellák aránya adott időszakra

ATM szolgáltatási kategóriák
- CBR (Constant BitRate): az állandó bitsebességű szolgáltatás
  Forgalomleírók: PCR, CDVT
  QoS jellemzők: maxCDV, maxCTD, CLR
    - realtime alkalmazásokhoz, amelyek szigorúan rögzített késleltetést és késleltetés-ingadozást igényelnek, pl. beszéd és áramkör-emulációs programok, állandó bitsebességű videó, minőségi hangátvitel
    - ha a források állandó sebességgel adnak
- rt-VBR (realtime Variable BR)
  Forgalomleírók: PCR, CDVT, SCR, MBS
  QoS jellemzők: maxCDV, maxCTD, CLR
    - realtime alkalmazásokhoz: videó, beszéd
    - a források változó bitsebességgel, burst-ösen adnak
- nrt-VBR (non-rt-VBR)
  Forgalomleírók: PCR, CDVT, SCR, MBS
  QoS jellemzők: CLR
    - a források változó bitsebességgel, burst-ösen adnak, de nem igényelnek realtime jellegű korlátokat
- ABR (Available BR): visszacsatolás-alapú, adási sebességüket tekintve adaptív forrásokhoz
  Forgalomleírók: PCR, CDVT, MCR
  QoS jellemzők: CLR (lehetséges, hálózattól függően)
- UBR (Unspecified BR): késleltetést tűrő alkalmazásokhoz, nem garantál QoS-t
  Forgalomleírók: PCR specifikálva van, de nem használja a CAC és a policing
  QoS jellemzők: nincs
- GFR (Guaranteed FrameRate): egy minimális cellasebességet igénylő forrásokhoz, a hálózat ennél többet nem garantál, habár tud. „Frame”: nagyobb egységekre működik a szabályozás.
  Forgalomleírók: PCR, CDVT, MCR, MBS, MFS
  QoS jellemzők: CLR (lehetséges, hálózattól függően)

Torlódásvezérlés ATM-hálózatokban

- Preventív: megelőzni a torlódást
  Új összeköttetés kérésekor minden, a tervezett útvonalon levő switch beleegyezése szükséges. Eldöntendő, hogy az új kapcsolat befolyásolja-e a switch által már kezelt kapcsolatok QoS-ét, és hogy képes-e a kapcsoló az új összeköttetés által igénylet QoS nyújtására.
  - CAC (Call Admission Control) – hívásengedélyezés, beengedés-szabályozás
    A switch ezt használja annak eldöntésére, hogy beengedi-e az új kapcsolatot. A legtöbb CAC algoritmus a CLR-en alapul. Az új összeköttetés elfogadást nyer, ha a kapcsoló képes tartani a kért CLR-t anélkül, hogy az hatással lenne meglevő összeköttetésekre. A jittert és CTD-t nem nézzük. Az újabb algoritmusok már a CTD-n alapulnak.
  - Policing
- Reaktív: a hálózat által adott visszacsatoláson alapul, szabályozza az adási lehetőséget
  - ABR (Available BitRate) szolgáltatás
    - Az összeköttetés felépítésekor az adó MCR-t kér, megadja a maxCR-t is, ami a PCR-je
    - A hálózat elfogadja, ha tudja teljesíteni a kért MCR-t
    - A forrás túllépheti a kért MCR-t, ha a hálózatban van ehhez szabad kapacitás
    - Torlódáskor az adónak csökkenteni kell az adási sebességét

Protokollok

Kialakulása, jelölések
Megvalósítás
Szerepe a hálózatok leírásában

Réteg: interface-elv, megvalósítás elrejtése:
Réteg teteje és alja: interfészek, rajtuk SAP-k (Service Access Point)

Protokoll réteg: két, azonos szinten, de különböző oszlopban lévő réteg virtuális kapcsolata

Az ISO-OSI referenciamodell: („A Pisti Szokott Tévét Nézni, Leginkább Pihenésképpen.”)

Alkalmazási	(7. Application)
Megjelenítési	(6. Presentation)
Viszonylati	(5. Session)
Átviteli	(4. Transport)
Hálózati	(3. Network)
Adatkapcsolati	(2. Data Link)
Fizikai	(1. Physical)

ISO OSI

Alkalmazási	(5. Application)
Átviteli	(4. Transport)
Hálózati	(3. Network)
Adatkapcsolati	(2. Data Link)
Fizikai	(1. Physical)

TCP/IP

Application layer: széles körben használt további protokollok (http, levelezési rendszerek), felhasználó programok és alkalmazások.
Presentation layer: az átvitt információ szintaktikai és szemantikai ellenőrzése, szükség szerinti konvertálása (adatábrázolás, op. rendszer miatti különbségek).
Session layer: megbízható, hibamentes (és gazdaságos) összeköttetés létrehozása és fenntartása a végpontok között; szinkronizáció a közös erőforrások kezelésében.
Transport layer: hibamentes összeköttetés létrehozása, a csomagsorrend helyreállítása; globális címrendszer lokálisra konvertálása; forgalomirányítás, útvonalkeresés.
Network layer: hálózati eszközök közötti kapcsolásokhoz a megfelelő címek és egyéb információk összegyűjtése; útvonalkeresés az alhálózaton belül; forgalomirányítás, csomagjavítás.

Data Link layer: csomagok összeállítása, hibaellenőrzéshez szükséges adatok előállítása, vétel esetén ellenőrzése, esetleg javítása; alhálózati címek kezelése.
Physical layer: bitek, bitcsoportok továbbítása a fizikai csatornán; egyéb jelzések küldése és fogadása ugyanitt.

Borítékolás: [fej | payload | (farok)]
Megvalósítás: minden réteg a felette levő rétegtől kapott adatot payload-nak veszi, hozzácsatolja saját fej-farok részét

Adatkapcsolati rétegbeli kommunikáció

Az adatkapcsolati réteg (Data-Link Layer):
- szolgáltatásokat nyújt a hálózati rétegnek (Network Layer)
- használja a fizikai réteg szolgáltatásait (Physical Layer)
- nagykiterjedésű hálózatok két szomszédos csomópontja, illetve helyi hálózatok csomópontjai közötti adatátvitelt biztosítja
- biztosítja
    - az adatátvitel funkcionális és eljárási eszközeit
    - a hibadetektálást, esetleg hibajavítást funkciókat a fizikai rétegbeli hibák kezelésére
- néha két alrétegre oszlik:
    - LLC (Logical Link Control): logikai kapcsolat vezérlés
    - MAC (Media Access Control): közeghozzáférés-vezérlés
- Protokolljai:
    - HDLC (High-level Data Link Control): magasszintű adatkapcsolat-vezérlés
    - SDLC (Synchronous DLC): szinkron adatkapcsolat-vezérlés
    - LAPB (Link Access Protocol – Balanced): kapcsolathozzáférési protokoll – kiegyenlített
    - LAPF (Link Access Protocol – Frame mode service): kapcsolathozzáférési protokoll kerettovábbítás számára

HDLC
- Szabványos, bit-orientált, szinkron adatkapcsolati protokoll
- Támogatja az összeköttetés-alapú és összeköttetés-mentes hálózatokat is
- Adategysége a keret (frame)
- HDLC protokollt alkalmazó hálózat csomópontjai (állomásai)
    - Elsődleges, ami a kapcsolat vezérlője
        - Vezérli az összes többi csomópontot
        - Szervezi az adatátvitelt
    - Másodlagos, melynek léteznie kell, ha van elsődleges; az elsődleges felügyeli
        - Nem csak az elsődleges kérésére aktiválódik
        - Nem felel a kapcsolat vezérléséért
    - Kombinált, mely egyesíti az elsődlegest és a másodlagost
- Az állomások konfigurációi
    - Kiegyenlítetlen
        - 1 elsődleges, 1..* másodlagos állomás
        - Elsődleges vezérli a többit
        - Half-duplex vagy full-duplex
        - Pont-pont vagy pont-multipont hálózatokban
    - Kiegyenlített
        - 2..* kombinált állomás
        - Egyenrangú állomások
        - Half-duplex vagy full-duplex
        - Pont-pont közötti kapcsolaton
    - Szimmetrikus

        - Minden fizikai állomás két logikai állomásból áll, egy elsődlegesből és egy másodlagosból
        - Külön vonal köti össze a logikai állomáspárokat
        - Ritkán használt
- Működési módok (a két adatcserét folytató állomás közötti viszony; meghatározza, hogy ki vezérli az adatkapcsolatot)
    - NRM (Normal Response Mode) – ez a szabályos elsődleges-másodlagos viszony megvalósulása, melyben a másodlagos állomás csak az elsődleges engedélyével adhat és egy vagy több, adatot tartalmazó keretből álló válasz továbbítását kezdeményezheti
    - ARM (Async RM) – a másodlagos állomás az elsődleges engedélye nélkül is kezdeményezhet átvitelt, ha a vonal tétlen. Az állomások közti viszony nem változik meg, az elsődleges állomás minden üzenete először a másodlagoshoz jut, s csak ezután kerülhet további eszközökhöz.
    - ABM (Async Balanced Mode) – minden állomás egyenrangú, csak kombinált állomások között használatos, pont-pont kapcsolatban. Bármelyik kombinált állomás kezdeményezhet átvitelt a másik engedélye nélkül.
- Kerettípusok
    - I (Information) – információs, felhasználói adatok és az ezekre vonatkozó vezérlési információk
      [Flag | Address | Control | Információ – felh. adatok a felső rétegből | FCS | Flag]
    - S (Supervisory) – felügyeleti, az átvitel vezérléséhez
      [Flag | Address | Control | FCS | Flag]
    - U (Unnumbered) – számozatlan, a rendszermenedzsment számára fentartott
      [Flag | Address | Control | Információ – hálózatirányítási mező, elhagyható | FCS | Flag]
    - A keretek mezői
        - Flag
            - Rögzített mintázat: 01111110
            - Minden keret elején és végén
            - A vevő szinkronizálására szolgál
            - Adatok között nem fordulhat elő, az adó az adatokban minden egymást követő 5 db 1-es után automatikusan beszúr egy 0-t, ezt a vevő törli

            7..14 egymás utáni 1-es: forgalom megszakítása, ha egy fontosabb keretet kell sürgősen átvinni

            15..* egymás utáni 1-es: tétlen csatorna jelzése, a HDLC vevő ilyenkor keretre vár, figyeli a csatornát
        - Address
            - 8 bit vagy annak többszöröse, hálózatfüggő
            - 8 bites cím utolsó bitje mindig 1
            - Több byteos cím legutolsó bitje 1, többi byte vége 0
            - Minden állomásnak egyedi címe van
            - Kiegyenlítetlen konfiguráció: parancs- és válaszkeretben is a másodlagos állomás címe
            - Kiegyenlített konfiguráció: parancskeret: célállomás címe, válaszkeret: küldő állomás címe
            - A cím első bitje:
              0: egy állomásra vonatkozik
              1: több állomásra vonatkozik
        - Control
            - I-keret: [0 | N(S) (3 bit) | P/F (1 bit) | N(R) (3 bit)]
                - P/F (Poll/Final): lekérdezés/végső bit; csak akkor értelmes, ha =1
                    - ha parancsban van, akkor poll-t jelent
                    - ha válaszban van, akkor állapotot tartalmazó keretet jelez (normálválasz módban a másodlagos állomásezzel jelezheti adásának végét is)
                - N(S): az elküldött keret sorszáma
                - N(R): a következő keret várt sorszáma
            - S-keret: [1 | 0 | Kód (2 bit) | P/F (1 bit) | N(R) (3 bit)]
                - Kód: S-típusazonosító

            - 00: RR (Recieve Ready): pozitív nyugta az N(R)-1 számú kerethez, vételi készség az N(R) számú kerethez
            - 01: REJ (Reject): n-nel történő visszalépés kérése, azaz a vevő kéri N(R)-től a keretek ismétlését
            - 10: RNR (Recieve Not Ready): pozitív nyugta az N(R)-1 számú kerethez, vételi szünetelési kérés
            - 11: SREJ (Selective Reject): szelektív ismétlés kérése, a vevő kéri az N(R) számú keret ismétlését
        - U-keret: [1 | 1 | Kód (2 bit) | P/F (1 bit) | Kód (3 bit)]
            - Kód: U-típusazonosító
                - Adatkapcsolati vezérlőfunkciókat tartalmaz
                - Példák:
                    - SNRM (Set NRM)
                    - SARM (Set ARM)
                    - SABM (Set ABM)
                    - DISC (DISConnect)
                    - UA (Unnumbered Ack)
                    - FRMR (FRaMe Reject)
    - Információ
        - Nincs az S-keretben
        - Tényleges adatbiteket tartalmaz
        - Mérete hálózaton belül állandó, egyébként hálózatfüggő
        - Lehet I-keretben vezérlési információt is vinni, ez a hátonvitt (piggyback) módszer
    - FCS (Frame Check Sequence)
        - A HDLC hibadetektáló mezője
        - Cím-, vezérlési- és információs mezőkre vonatkozik
        - 16 vagy 32 bites CRC
- HDLC-ből származó protokollok
    - SDLC
    - LAP (Link Access Protocol), LAPB (Balanced), LAPD (D channel), LAPF (Frame mode services)
    - PPP (Point-to-Point Protocol)
    - MTP-2 (Message Transfer Part 2)

SDLC (Sync Data Link Control)
- Jellemzői:
    - Az első bitorientált szinkron adatátviteli protokoll
    - Half-duplex vagy full-duplex átvitel
    - Topológiák:
        - Pont-pont
        - Pont-multipont
        - Hurokba szervezett: az elsődleges állomás az első és utolsó másodlagoshoz csatlakozik
        - Középponti (hub) szervezésű
    - Kapcsolt vagy kapcsolásmentes hálózatokban
- Lényegében megfelel a kiegyenlítetlen konfigurációjú normálválasz-módú HDLC-nek
- Eltérések a HDLC-től
    - Csak NRM átviteli mód
    - Csak 16 bites CRC
    - HDLC nem támogatja a hurokba szervezett és a hub-szervezésű topológiákat

LAPB
- X.25 protokollcsalád tagja

- Keretekbe szervezett adatokat továbbít egy adatvégberendezés (DTE – Data Terminating Equipment) és egy adatkapcsolati végberendezés (DCE – Data Circuit Terminating Equipment), pl. egy modem között
- Működése megfelel az aszinkron kiegyenlített módú HDLC-nek
- LAPB kapcsolatot akár a DTE, akár a DCE kezdeményezhet – a kezdeményező lesz az elsődleges állomás
- Kerettípusok
    - I-keret: felsőbb rétegekből származó, ill. vezérlési információk
        - Funkciók (pl.):
            - Sorrend biztosítása
            - Áramlásvezérlés
            - Hibaészlelés és –javítás
        - Elküldött és vett keretszámot egyaránt tartalmaz
    - S-keret: vezérlőinformációk továbbítására
        - Funkciók (pl.):
            - Átvitel kérése és leállítása
            - Állapotjelentés
            - I-keret nyugtázása
        - Csak vett keretszámot tartalmaz
    - U-keret: vezérlőinformációk továbbítására
        - Funkciók (pl.):
            - Kapcsolatlétesítés és –lebontás
            - Hibajelentés
- Érvényes LAPB címek: 2 db létezik, az átvitel irányát is meghatározzák
    - DTE cím (0x03)
    - DCE cím (0x01)
- LAPB parancsok:
    - S-keretben: mint a HDLC-nél, csak itt nincs SREJ
    - U-keretben:
        - Parancsok
            - SABM (Set ABM)
            - DISC (Disconnect)
        - Válaszok
            - UA (Unnumbered Ack)
            - DM (Disconnected Mode)
            - FRMR (Frame Reject)

LAPF

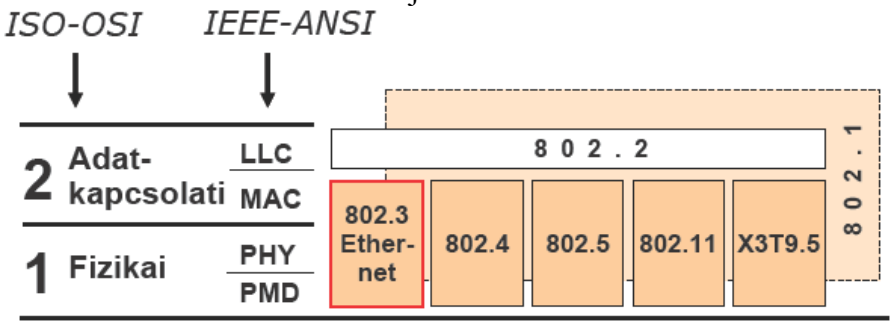
- Legfontosabb funkciók:
    - Kerethatárolás és –igazítás
    - Transzparens átvitel
    - Virtuális áramkörök nyalábolása és kibontása
    - Bájtok/oktettek határra igazítás (nulla beszúrás előtt egész számú bájt)
    - Keret méretének ellenőrzése
    - Hibakezelés
    - Torlódásvezérlés
- A LAPF protokollt a kerettovábbításban végpontok közötti jelzésre használják
- Keret, cím- és vezérlésmező
    - Keret: [Flag | Address / Control | Információ | CRC | Flag]
        - Address/Control: [DLCI (6)|C/R (1)|EA (1)|DLCI (4)|FECN (1)|BECN (1)|DE (1)|EA (1)]
            - DLCI (Data Link Connection Identifier)
            - C/R: nem használt
            - EA (Extended Address)
            - FECN (Forward direction Collision Notification)

    - BECN (Back direction Collision Notification)
    - DE (Disposable frame)
- Áramlásvezérlés
    - Garantált átviteli sebesség (keret/sec) alatt mindent továbbít
    - Efölött, de a maximális sebesség alatt a keretek DE bitjét 1-be írjuk, és amit lehet, továbbítunk
    - A maximális sebesség felett minden keretet eldobunk

Lokális hálózatok

Az Ethernet (IEEE 802.3)

A lokális hálózatok architektúrája



Alrétegek:
- LLC (Logical Link Control)
- MAC (Medium Access Control)
- PHY (Physical)
- PMD (Physical Media Dependent)

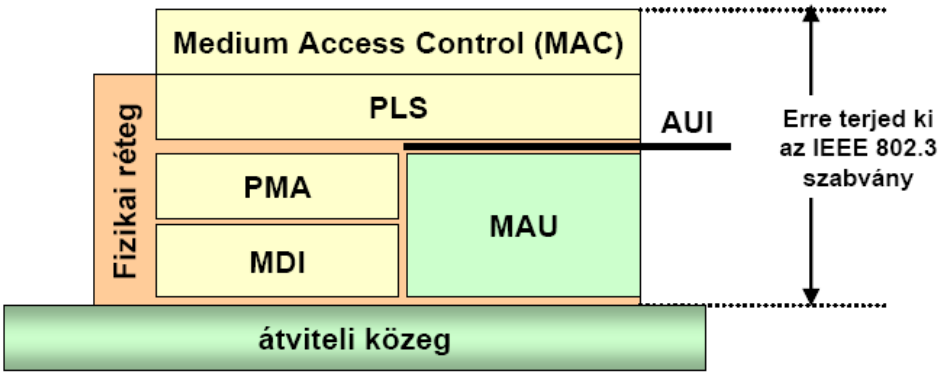
802.1: közös funkció minden LAN-ra és MAN-ra

Az Ethernet két változata – különbségek elsősorban a MAC keretben
- Ethernet version 2 (DIX)
- IEEE 802.3

Topológia: logikailag busz

A fizikai réteg feladatain
- bitfolyamok adása/vétele
- vivőérzékelés (Carrier Sensing)
- ütközésdetektálás (Collision Detection)
- jelkódolás és –dekódolás
- előke (előtag) (preamble) generálása
- órajelgenerálás a szinkronizáláshoz

A fizikai réteg architektúrája

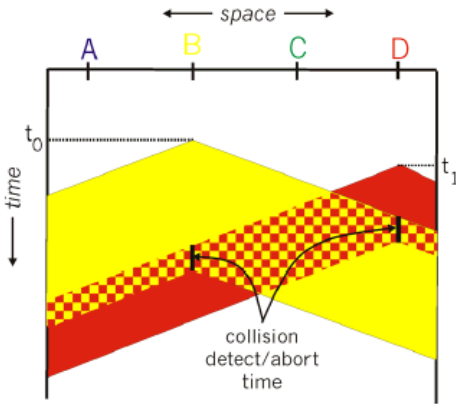


PLS (Physical Signalling Sublayer)
AUI (Attachment Unit Interface)
PMA (Physical Medium Attachment)
MDI (Medium Dependent Interface)
MAU (Medium Attachment Unit)

MAC – az Ethernet keretek felépítése (zárójelben: byte-okban mért hossz)
[előtag (7) | SFD (1) | Dst Addr (6) | Src Addr (6) | Type/Length (2) | Data (46..1500) | CRC (4)]
---------- Kerethossz: 64..1518 ----------

- Előtag: 1010101
- SFD (Start Frame Data)
- Dst Addr, Src Addr: cél és forrás fizikai címe (MAC address)
- Type/Length: az adatmező típusa és hossza

Ütközésdetektálás

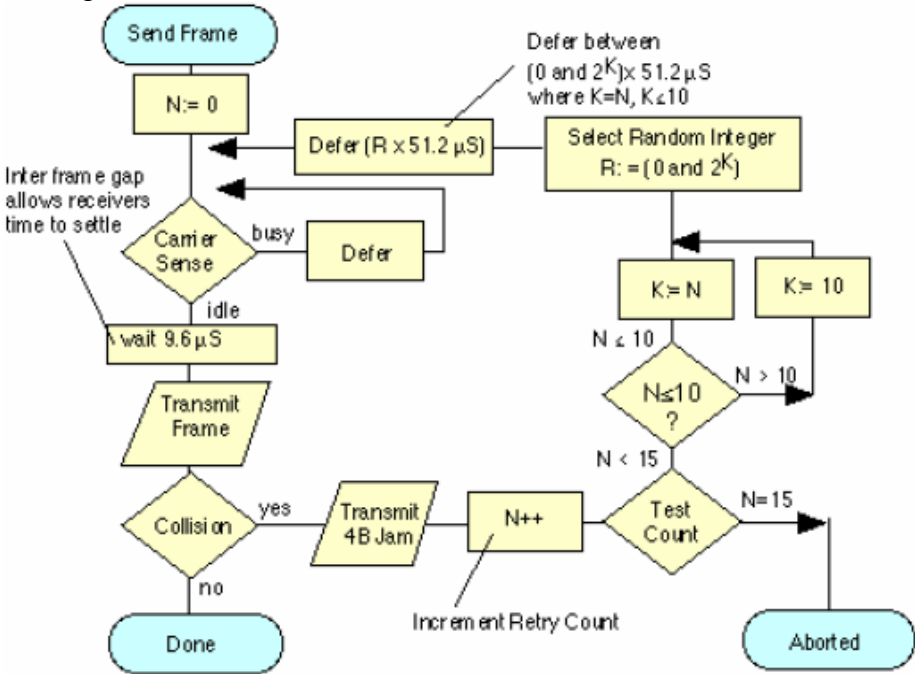


- Legkedvezőtlenebb esetben is (busz két végén van az adó és a vevő) minden állomás érzékelje az ütközést: T = C / 2L
  - T: résidő
  - C: jelterjedési sebesség
  - L: szegmens (busz) hossza
- Például: L = 500 m, C = 2 * 10^8 m/s➔ T ~= 51,2 µs. Ha 10 Mbit/s, akkor 51,2 µs → 512 bit = 64 byte

MAC – CSMA/CD

- CSMA/CD
  - Az állomás figyeli a csatornát, a „vivőt” (CS – Carrier Sense)
  - Ha nem érzékel adást, küldeni kezd
  - Ha több állomás ad, mindkettő abbahagyja (CD – Collision Detection), zavaró jelet adnak (jam)
  - Valamekkora (véletlen) idő múlva (backoff time) újra megpróbál adni
- Fentiek miatt CSMA/CD-hez kell, hogy
  - Adás előtt érzékeljük a csatornát, a „vivőt” (CS)
  - Adás alatt érzékeljük az ütközést (CD)

A MAC-protokoll:



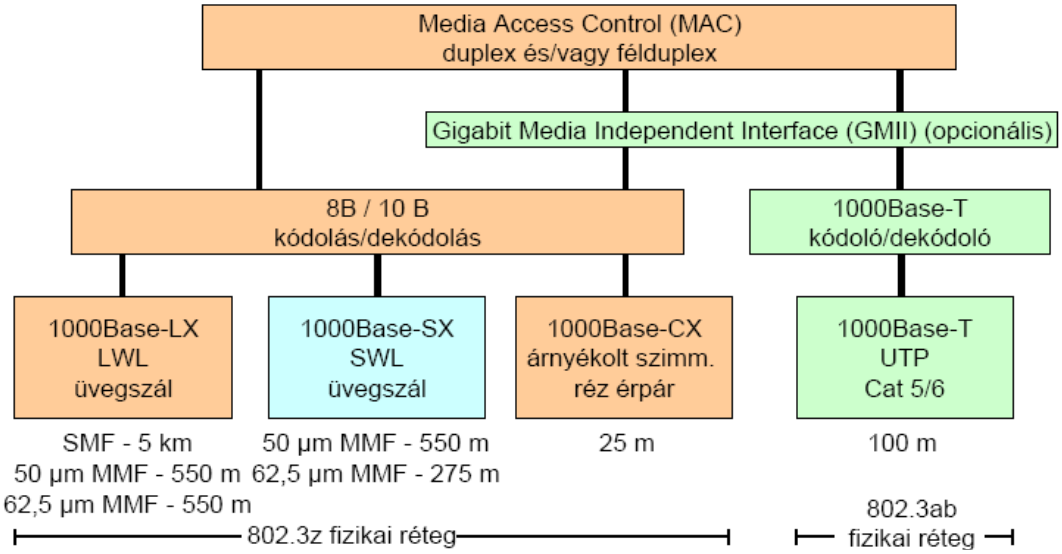
Interframe gap: 96 bit, 9,6 µs 10 Mbit/s-nál
Résidő: 512 bit, 51,2 µs 10 Mbit/s-nál

Kapcsolt Ethernet

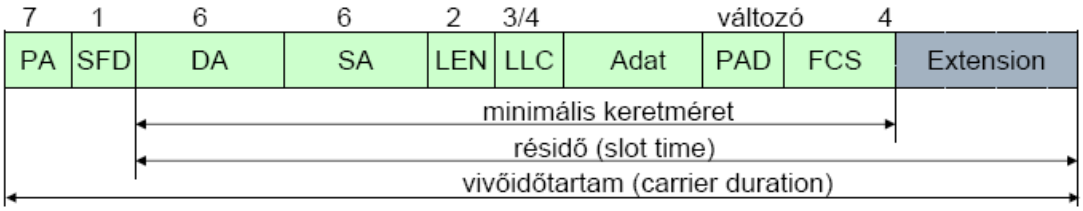
- Nagyobb forgalom kezelése a buszsebesség növelése nélkül
- Ethernet-kapcsoló (switch) több vonali kártyával
- A kártyák portjaira 10BaseT-n csatlakoznak a végpontok
    - Adott portra csatlakozó szegmensen ütközéses kommunikáció
    - A kapcsolón belül nincs ütközés
    - Pufferelt portok, duplex működés
    - Egy port egy állomás is lehet (dedikált sávszélesség)

Fast Ethernet

- Minden gyors Ethernet kapcsolt, UTP vagy üvegszál
- IEEE 802.3z Gigabit Ethernet („GbE”)
    - Keretformátum változatlan (lefelé kombatibilis)
    - Rézvezeték és üvegszál
    - Manchester helyett 8B/10B kódolás
    - Half-duplex: még mindig CSMA/CD
    - Full-duplex: nincs ütközés
    - Használat: nagyforgalmú dedikált állomások (szerverek), gerinchálózat
    - Újdonságok
        - Flow Control (forgalomszabályozás)
        - 802.1Q szerinti VLAN (Virtual LAN) kezelése itt jelent meg
            - Virtuális hálózat létesítése logikai azonosítók alapján (nem csak fizikai címek)
            - Eltérő keretformátum
    - Funkcionális elemek

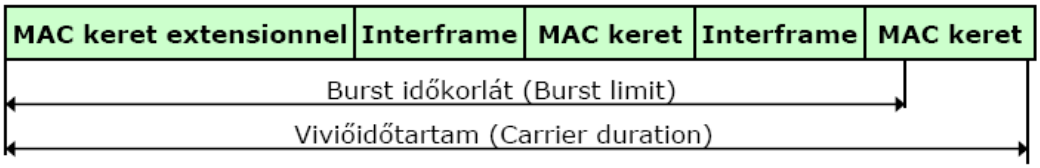


- Megnyújtott keretformátum
  - „Félduplex” üzemmód:
    - Mint a klasszikus Ethernet (CS, CD), de sokkal rövidebb keretidők
    - Két megoldási lehetőség:
      - Megnövelt kerethossz
      - „Carrier-extension” bitek hozzáadása a keretekhez
        - Ezt választották, mert ezzel nem változott a szabvány



PA	Preamble	LLC	Logical Link Control
DA	Destination Address	PAD	Padding
SA	Source Address	FCS	Frame Check Sequence (CRC-32)
SFD	Start Frame Delimiter	LEN	Length

- Frame bursting



  - Ez egy másik lehetőség az adási időszak megnyújtására
  - Az állomás rövid csomagok sorozatát küldheti el egy adott burst időkorlátig anélkül, hogy elengedné a csatornát („jumbo” keret)
  - A keretek közé interframe-eket kell helyeznie
  - Az időkorlát leteltekor az utolsó keretet még befejezheti

IEEE 802.3ae – 10 Gbit/s Ethernet (XGE)
- Csak duplex, nincs CSMA/CD
- Főleg üvegszál
- 7 különböző fizikai réteg

Összefoglalás
- A különböző 802.3 szabványokban közös:
  - Keretformátum
  - Címzés
- A különböző 802.3 szabványokban eltérő lehet:
  - A közeghozzáférés – CSMA/CD fokozatos kivonása
  - A fizikai közeg – koax kábeltől a monomódusú üvegszálig

Lokális hálózatok 2.

Token bus (IEEE 802.4), Token ring (IEEE 802.5), FDDI (ANSI), FiberChannel (ANSI)

További LAN-ok
- Token bus – a legjobb MAC-protokoll, de bonyolult; kihalt
- Token ring – alig használt
- FDDI (Fiber Distributed Data Interface) – gyűrű topológia; kihalóban

Ezek igen érdekes témák, ezért foglalkozunk velük. – *Mégpedig az 584-601 dián (LAN_1.pdf 40-57. dia). Én inkább kihagynám.*

Lokális hálózatok 3.

A közös réteg: IEEE 802.2 LLC – Logical Link Control

BWA (Broadband Wireless Access)

WPAN (Wireless Personal Area Network), IEEE 802.15.1 (BlueTooth)
- Célkitűzés:
  - Olcsó eszköz
  - Kis hatótávolság (10 m)
  - Max 1 Mbit/s

Nagysebességű PAN-ok: 802.15.3
- Célkitűzés
  - Médiakommunikáció – tv, MP3, videójátékok
  - Kis hatótávolság (10 m)
  - Max 55 Mbit/s
  - Másik munkacsoport: 110, 200, 480 Mbit/s – házimozi, játékok

Nagyvárosi vezetéknélküli hálózat: WMAN (802.16), WiMAX

WiMAX
- Fizikai réteg: OFDM (Orthogonal Frequency Division Multiplexing)
  - Többvivős modulációs/multiplexálási technika
  - A rendelkezésre álló sávszélesség alvivőkre osztása
    - Ezek ortogonálisak egymásra
    - Ahol az egyiknek maximuma van, ott a többi eltűnik
    - ISI nélküli átvitel
  - Digitális jelfeldolgozás IFFT/FFT
  - Többutas terjedés (ISI) ellen védőidő alkalmazása
  - A több vivő miatt ellenáll a frekvencia-szelektív fading-nek
  - Változtatható adatsebességek
  - TDD – FDD
    - TDD (Time Division Duplex): félduplexnek is hívják, egy csatorna áll rendelkezésre, ezt használják közösen megosztva a kommunikáló felek
    - FDD (Freq Div Duplex): két, egymástól eltérő csatornát (frekvenciát) használunk, ez valódi full-duplex mód
- MAC réteg
  - DLC (Data Link Control)
    - Biztonsági alréteg
    - Közös alréteg
      - Topológia: kétirányú pont-multipont
      - Kapcsolatorientált: 16 bites kapcsolatazonosító, 48 bites MAC-címmel azonosított előfizetők
    - Szolgáltatás-specifikus alréteg
      - Két alternatív alréteg: ATM-konvergencia alréteg és csomag-konvergencia alréteg (csomagkapcsolt protokollok továbbítására, pl. IP, PPP, Ethernet)
- Közeghozzáférés: QoS biztosítása
  - Forgalmi paraméterek és előírások
    - MIR (Max Information Rate), MaxRTR (Max Reserved Traffic Rate), MSTR (Max Sust Traff Rate), EB (Excess Burst): felülről korlátozza egy forgalom adatsebességét, hogy a csatornán más forgalom is mehessen

        - CIR (Committed Information Rate), MinRTR, CB (Comitted Burst): az adott forgalom átlagos adatsebessége bit/s-ban
        - CT (Comitted Time), PTI (Polling Time Interval), UP (Unicast Polling): max ilyen időközönként kerül frissítésre a sávszélességigény – csatorna idejének/frekvenciájának felosztása – a tényleges forgalomnak megfelelően, általában 500-1000 ms
        - Prioritás – Traffic Priority: 0-7 közötti egész, azonos forgalmi osztályokon belüli priorizálás
        - Késleltetésingadozás – NGR (Normal Grant Jitter), TJ (Tolerated Jitter); jitter = delay variation: megadja, max mekkora késleltetésingadozás megengedett
        - Max késleltetés (max latency): biztosítandó max késleltetés
        - Megengedett méret (unsolicated grant size): tipikusan mekkora egy csomag
    - Forgalmi osztályok
        - UGS (Unsolicated Grant Service), CG (Continuous Grant): konstans adatsebességet igénylő valósidejű alkalmazásokhoz, pl VoIP telefonbeszélgetés
        - rtPS (realtime Polling Service): nem konstans adatsebességű valósidejű szolgáltatásokhoz, pl MPEG videó
        - nrtPS (non-rtPS): nem kell valósidejűség, de garantált sávszélesség igen, pl. internetböngészés
        - BE (Best Effort): hasonló az nrtPS-hez, de semmilyen garancia nincs, a többi QoS által meghagyott sávszélességet kapja
    - Osztályok és paraméterek

Paraméter	*QoS osztály*			
	UGS	rtPS	nrtPS	BE
MIR	(✓)	(✓)	✓	✓
CIR	✓	✓	✓	
CT		✓	✓	✓
Tolerated jitter	✓			
Maximum latency	✓	✓		
Traffic priority			✓	✓
Unsolicited grant size	✓			

- Összefoglalás:
    - WiMAX = WiFi nagyban
    - Nagy távolságok (48 km) áthidalása
    - Közvetlen rálátás nélkül is működik
    - Többutas terjedés ellen véd
    - QoS támogatása

Lokális hálózatok 4.

LAN-ok összekapcsolása

Korlátok: távolság, állomások száma és típusa. Áthidalás: átjátszóval.
Átjátszó elvi lehetőségei attól függően, hogy melyik ISO-OSI rétegben van:

- 1. rétegben: repeater (ismétlő)
- 2. réteget ismeri/szűri: bridge/switch
- 3. réteget ismeri, 2. réteget újragenerálja: router
- Több réteget újragenerál: gateway

Bridge és switch

- Majdnem ugyanaz: LAN-szegmenseket kötnek össze az adatkapcsolati rétegben
- A bridge elvileg LAN-szegmenseket köt össze, a switch-re végpontok is csatlakozhatnak
- Mára a switch maradt:
  - Adatkapcsolati rétegbeli
    - tárolja és továbbítja az Ethernet-kereteket
    - Keretfejrészt vizsgál és szelektíven továbbít a MAC célcím szerint
    - Ha saját szegmensére kell továbbítani, CSMA/CD-t használ
  - Transzparens: a végpontok nem tudnak a kapcsolók jelenlétéről
  - Plug-and-play: nem kell konfigurálni
- Switch jellemzői:
  - Felépítés:
    - Kapcsolómátrix
    - Gbit-es hátlap
    - Vonali kártyák (4-32 db)
    - Kártyánként 1-8 port
  - Működés
    - A portok belső LAN-t alkotnak, mindegyik egy CSMA/CD ütközési tartomány
    - A kapcsoló belsejében nincs ütközés
    - A portok pufferelteк, duplex működést tudnak
  - Kerettovábbítás szegmensek között (honnan tudja, hova kell küldeni?)
    - Öntanuló
      - Van kapcsolótáblája, bejegyzése: {MAC, Interface, Timestamp}, régieket eldobja
      - Megtanulja, hogy melyik végpontokat melyik interfészen át éri el
      - Egy keret vételekor megtanulja, melyik szegmensen van a küldő
    - Szűrés/továbbítás pszeudokód:

      if (van bejegyzés az adott MAC cél-címre) {
      if (cél azon a szegmensen van, ahonnan jött a frame)
      keret eldobása
      else
      keret továbbítása a megadott interfészre
      } else { elárasztás }
    - Feszítőfás algoritmus: védekezés az ellen, ha több switch van párhuzamosan kapcsolva és ez végtelen ciklust eredményezne

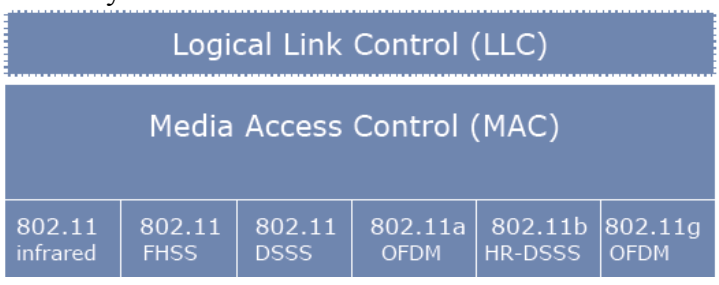
Virtuális LAN-ok (VLAN), IEEE 802.1Q
[Dst MAC addr (6 byte) | Src MAC Addr (6 byte) | „Tag protocol ID” (2 byte) | User priority (3 bit) | CFI (1 bit) | VLAN ID (12 bit) | Type/Length (2 byte)]

Lokális hálózatok 5.

WLAN (IEEE 802.11)

WLAN

- Pár 100 méter, 1-2 Mbit/s..10 Mbit/s
- Szabványok:



- 802.11a: 5 GHz
- 802.11b: 2,4 GHz
- 802.11g: a 802.11b feljavítása 54 Mbit/s-ra
- 802.11n: 100 Mbit/s felett
- 802.11e: QoS
- 802.11i: adatbiztonság, titkosítás
- 802.11s: mesh-üzemmódú működés
- 802.15: PAN
- 802.15.1: BlueTooth
- 802.16: Wireless MAN

Wireless transmission
- IR (Infra Red)
- RF (Radio Freq)
  - SS (Spread Spectrum)
    - FHSS (Freq Hopping): több frekvenciát használ, az egymás utáni biteket (-csoportokat) más-más frekvencián adja. Legalább 74 frekvencia használata, lassú és gyors frekvenciaugrások (a bitsebességehez képest)
    - DSSS (Direct Sequence)
    - OFDM (Orthogonal Freq Div Mpx)

WLAN topológiák
- BSS (Basic Service Set) – egy cella
- ESS (Extended Service Set) – több cella
- DS (Distribution System) – elosztóhálózat (gerinc)

802.11 keretformátum
[Frame Control (2) | Duration ID (2) | Addr1 (6) | Addr2 (6) | Addr3 (6) | Sequence Control (2) | Addr4 (6)]
[Frame body (0-2312) | FCS]

	To DS	From DS	Addr1	Addr2	Addr3	Addr4
	0	0	Dest Addr	Src Addr	BSSID	-
Lan->wlan	0	1	Dest Addr	Sending AP	Src Addr	-
Wlan->lan	1	0	Recieving AP	Src Addr	Dst Addr	-
Wlan->wlan	1	1	Recieving AP	Sending AP	Dst Addr	Src Addr

BSSID: Basic Service Set ID
AP: Access Point

802.11 MAC réteg, hozzáférési módszerek
- CSMA/CA – vezetéknélküli LAN-ban nem lehet ütközést detektálni
- Két hozzáférési módszer:
  - DCF (Distributed Coordination Function)
    - A MAC alsó alrétege
    - Különböző értékű IFS-ek (InterFrame Space)
      - Short IFS – vezérlőüzenetekhez
      - PIFS (PCF IFS)
      - DIFS (DCF IFS) – adatkeretekhez

      Reláció: DIFS > PIFS > SIFS
    - DCF algoritmus:
      - Ha szabad a csatorna, az állomás még IFS ideig vár, hogy szabad marad-e
      - Ha foglalt, vagy IFS alatt azzá válik, tovább figyel
      - Ha szabaddá válik, vár IFS + random ideig, majd ad
    - RTS/CTS

        - Opcionális eljárás
            - RTS (Request To Send)
            - CTS (Clear To Send)
        - Erőforrásigényes és nagy késleltetést visz be
        - Használat: ha nagy a verseny a hálózaton
    - NAV (Network Allocation Vector)
        - Minden RTS keret tartalmazza a tervezett csatornafoglalási időt
        - NAV: számláló a többi állomásnál, amelyeknek NAV ideig várniuk kell, mielőtt megnéznék, szabad-e a csatorna
        - Amikor egy állomás RTS-t vagy CTS-t küld, a többiek elindítják a NAV-ot
        - Rejtett állomás problémája: ketten akarnak ugyanannak adni. Megoldás: egyikük RTS-ét visszautasítja a másik NAV-jával
    - Foglalt közeg
        - Fizikailag foglalt: az állomás foglaltnak érzi a rádiócsatornát
        - Virtuálisan foglalt: az állomás RTS-t/CTS-t vesz, mely jelzi, hogy NAV ideig foglalt lesz a csatorna

- PCF (Point Coordination Function)
    - Opcionális, ha van, akkor a DCF felett van
    - Egyetlen AP vezérli
    - Az AP jelzőüzenetére (beacon) az állomások beszüntetik a DFC működést
    - Az AP sorban lekérdezi az állomásokat (polling): garantált max késleltetés
    - Egy állomás csak akkor adhat, ha kérdezik
    - Lehet prioritást is hozzárendelni az állomásokhoz, így kezelhetők időérzékeny alkalmazások

Szolgáltatásminőség WLAN-okban (802.11e szabvány)

- HCF (Hybrid Coordination Function)
- Kétféle MAC-módszer, az eredetihez hasonlóan
    - HCCA (HCF controlled channel access)
    - EDCA (enhanced distributed channel access)
- Mindkettőnél: forgalomosztályok és a protokoll biztosítja, hogy a magasabb prioritású jobb kiszolgálást kapjon

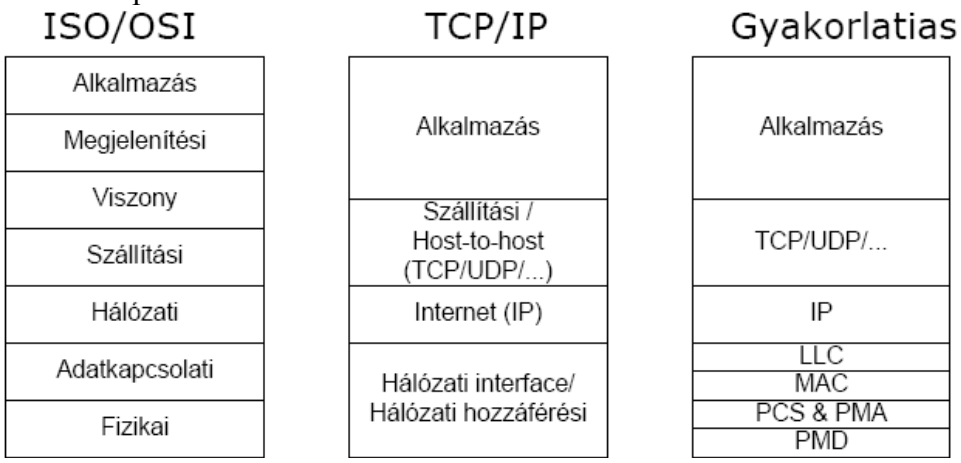
IP – Internet Protocol

IP címzés, routing, IPv6, IP mobilitás

Tematika

- Bevezetés
    - Az Internet és az IP története

- A TCP/IP protkollarchitektúra



  - IP: Internet Protocol
  - TCP: Transmission Control Protocol
  - UDP: User Datagram Protocol
  - LLC: Logical Link Control
  - MAC: Medium Access Control
  - PCS: Physical Coding Sublayer
  - PMA: Physical Medium Attachment
  - PMD: Physical Medium Dependent
- Az IP feladata és jellemzői
  - Hálózati protokoll: adattovábbítás a hálózat végpontjai között
  - Funkciói:
    - Címzés és forgalomirányítás (routing)
    - Tördelés (fragmentation)
  - Jellemzők
    - Csomagkapcsolt és összeköttetés-mentes, tehát datagram-típusú
    - Best Effort, a csomagokra igaz, hogy:
      - Elveszhetnek
      - Duplikálódhatnak
      - Megváltozhat a sorrendjük
      - Meghibásodhatnak (nincs hibaészlelés és –javítás)
    - Nincs:
      - Torlódáskezelés
      - Ütemezés
      - Titkosítás és hitelesítés

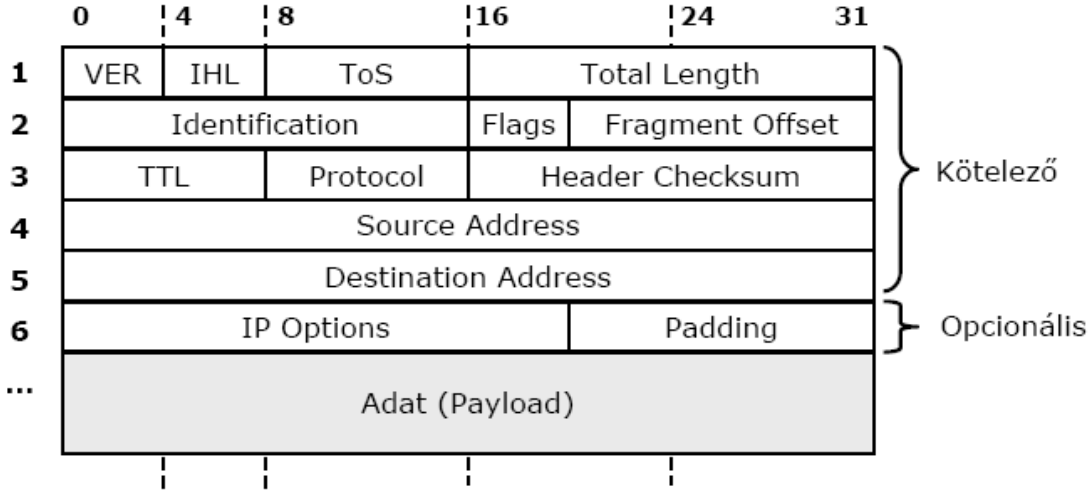
- Címzés
  - Felépítés: 32 bites: [hálózati azonosító | hálózaton belüli azonosító]
  - Címosztályok
    - A, B, C: egyedi címzés (unicast)
    - D: multicast, 224.0.0.0 – 239.255.255.255
    - E: fenntartott, 240.0.0.0 – 255.255.255.255
    - Speciális címek:
      - HostID csupa 0: hálózat címe, eszközök opcionálisan kezelhetik
      - HostID csupa1: broadcast cím, mindenkinek szól
      - 127.0.0.0 – 127.255.255.255: loopback cím, a helyi gépet azonosítja
      - Privát címtartományok
        - Csak helyi hálózaton (Interneten nem)
        - 10.0.0.0 – 10.255.255.255
        - 172.16.0.0 – 172.31.255.255
        - 192.168.0.0 – 192.168.255.255

- Címosztályok általánosítása
  - Subnetting: alhálózatokra osztás
    - 1 db A osztályú ↔ 256 db B osztályú
    - 1 db B osztályú ↔ 256 db C osztályú
    - Prefix alapján már nem állapítható meg
  - CIDR (Classless InterDomain Routing)
    - VLSM (Variable Length Subnet Mask): osztályok eltörlése, a cím 32 bites és tetszőleges helyen lehet kettéosztva
    - A címből nem derül ki, hol lett kettéosztva → alhálózati maszk: 11…100…0, ahol 1, ott a network ID, ahol 0, ott a host ID

- Az IP csomag szerkezete
  - IP csomag két része:
    - IP-fejléc (header)
    - Adat (payload)
  - Az IP-csomag alsóbb rétegbeli protokollok payload részébe ágyazódik be
  - Az IP-csomag payload részébe magasabb rétegbeli protokollüzenet (PDU) kerül

↓ [Szállítási protokoll fejléc | Adat]
↓ [IP fejléc | Adat]
[Adatkapcsolati fejléc | Adat | Adatkapcsolati farok]

  - Fejléc



    - VER (Version): ertéke: 4 vagy 6 (IPv4 / IPv6)
    - IHL (Internet Header Length): a fejléc mérete DWORD-ökben, értéke: 5..(2^4-1) = 5 .. 15, tehát a fejléc mérete 20..60 byte
    - ToS (Type of Service): QoS osztályok, paraméterek jelzésére. A legtöbb router nem támogatja. Leggyakoribb felhasználás:
      - DSCP (Differentiated Services Code Point)
      - ECN (Explicit Congestion Notification)
    - Total Length: a teljes IP-csomag mérete byte-okban, értéke: 576..65535, (576: 20 fejléc + 512 adat + 44 IP-opciók és alsóbb rétegek fejlécei. Ekkora csomagot tördeletlenül kell továbbítani.)
    - Identification: az IP-töredékek azonosítója
    - Flags (3 bit):
      - 0: reserved, set to 0
      - 1: DF (Dont Fragment), 1: ha tördelni kellene, el kell dobni
      - 2: MF (More Fragment), 1: nem az utolsó töredék, 0: utolsó töredék vagy tördeletlen
    - Fragment Offset (13 bit)
      - Az eredeti csomagban levő kezdőpozíció 8 byte-os egységekben
    - TTL (Time To Live): csomag élettartama, eredetileg másodpercben, gyakorlatban hop-számban mérve (minden továbbításnál csökkentjük, ha ezután 0, eldobjuk)

        - Protocol: a payload-ban levő protocol azonosítója, pl: ICMP (1), IGMP (2), TCP (6), EGP (8), UDP (17), OSPF (89), SCTP (132)
        - Header Checksum: a fejléc minden WORD-jére számolt egyes komplemens (számításkor ez a mező csupa 0). A csomag érkezésekor ellenőrizni kell és továbbításkor újra kell számolni.
        - Source / Destination Address (2 x 32 bit): a feladó és a címzett IP-címe
        - IP Options: ritkán használt, opcionális, ezzel lehet pl. a csomag útját kijelölni
        - Padding: helykitöltő, kiegészíti az IP Options-t 4 byte többszörösére
- Routing
    - A csomagtovábbítás elve: „hot potato”: minél gyorsabban továbbítsunk, csak a következő csomópontot kell ismerni
    - Kinek küldjük tovább – routing:
        - Cél címe alapján: csomag tartalmazza
        - Saját routing-tábla alapján
    - Hogyan küldjük tovább:
        - Mekkora egységekben – fragmentation:
            - Mekkora érkezik? Csomag határozza meg.
            - Mekkora továbbítható? A következő hálózat MTU-ja (Maximum Transmission Unit) határozza meg.
        - Milyen QoS-sel – QoS:
            - Best effort – nincs garancia
            - ToS mezővel és egyéb protokollokkal
    - Routing tábla
        - Bejegyzés:

Merre megy?		Merre küldjük?		
Hálózat címe	Alhálózati maszk	Interfész	Közvetlenül kapcsolódó	Következő csomópont
<IP-cím>	</N>	<azonosító>	<igen/nem>	<IP-cím>
<IP-cím>	</N>	<azonosító>	<igen/nem>	<IP-cím>
<IP-cím>	</N>	<azonosító>	<igen/nem>	<IP-cím>

        - A cél IP-cím akkor tartozik egy hálózatba, ha a hálózatazonosító rész megegyezik
        - Keresés a táblázatban: ha több hálózati azonosítóra is illeszkedik, akkor a leghosszabb egyezésűt kell választani; a teljes táblázatot végig kell nézni. (Javítások: bináris fás tárolás; keresés csak akkor, ha nem saját cím.)
    - Alapértelmezett útvonal: erre megy a csomag, ha nem ismeri a célhálózatot
        - Ehhez tartozó bejegyzés: 0.0.0.0 – minden címet tartalmazó hálózati maszk
        - Alapértelmezett átjáró és elnevezése:
            - A fenti bejegyzéshez tartozó következő csomópont IP-címe
            - A név nem szerencsés, jobban fedi a valóságot az „alapértelmezett router”
        - Nem feltétlenül van ilyen: ha másra nem illeszkedik, akkor a célhálózat ismeretlen, a csomag eldobandó
        - A végpontokon gyakran csak két bejegyzés szerepel:
            - Helyi hálózat (helyi végpontok közvetlenül elérhető)
            - Alapértelmezett útvonal (minden más távoli hálózaton)
    - Metrikák szerepe az útvonalválasztásban
        - Metrika: tkp. élsúly a router-gráfban
        - Alapja lehet pl.: elérhetőség, terheltség, késleltetés
        - Típusa:
            - Statikus: manuálisan megadott
            - Dinamikus: a link vagy a hálózat állapotától függően adaptív
        - Értelemszerűen a jobb metrikával rendelkező kapcsolaton küldjük tovább a csomagot

- Megfelelő bejegyzés kiválasztása
  - Közvetlenül kapcsolódó helyi hálózat: a címzettnek közvetlenül küldeni, ehhez kell a címzett adatkapcsolati rétegbeli címe
  - Távoli hálózat: a routernek kell küldeni
    - Az IP-cím módosítása tilos
    - Csak adatkapcsolati rétegben szabad a routernek címezni, amihez kell az ő adatk.r.-beli címe
- Routing tábla karbantartása
  - Manuálisan: op.rendszer szintjén támogatott
  - Automatikusan: routerek kommunikációjának eredményeképpen
- Router feladatai
  - Hibás-e a csomag (fejléce)?
  - Nekem címezték-e?
  - Ismerem-e a címzett hálózatát?
  - --TTL > 0?
  - Kell-e/lehet-e tördelni?
  - Kell-e visszajelzést küldeni?

- IP segédprotkollok
  - ARP (Address Resolution Protocol): IP alapján keresünk MAC-címet
    - Működése: broadcast kérés – „kinek az IP-címe a …” → a tulajdonos válaszol
    - Közvetlenül az adatk. réteg protokolljának küldjük, nem IP-csomag
    - Fejléce:

<table>
<tr><th colspan="2">0 - 15 bits</th><th>16 - 31 bits</th></tr>
<tr><td colspan="2">Hardware Type</td><td>Protocol Type</td></tr>
<tr><td>HLen (1 byte)</td><td>PLen (1 byte)</td><td>Operation</td></tr>
<tr><td colspan="3">Sender HA (bytes 1 - 4)</td></tr>
<tr><td colspan="2">Sender HA (byte 5- 6)</td><td>Sender PA (byte 1 - 2)</td></tr>
<tr><td colspan="2">Sender PA (byte 3 - 4)</td><td>Target HA (byte 1 -2)</td></tr>
<tr><td colspan="3">Target HA (bytes 3 - 6)</td></tr>
<tr><td colspan="3">Target PA (bytes 1 - 4)</td></tr>
<tr><td colspan="3">RARP header structure</td></tr>
</table>

      - Hardware Type: Ethernet: 0x0001
      - Protocol Type: IP: 0x8000
      - HLen
        - Ethernet: 6 byte
        - TokenRing, FDDI: 2 v. 6 byte
      - PLen: IP: 4 byte
      - Operation
        - ARP request = 1
        - ARP reply = 2
        - RARP request = 3
        - RARP reply = 4
      - Sender Hardware Address: <MAC-cím>
      - Sender Protocol Address: <IP-cím>
      - Target HA, Target PA
    - ARP tábla
      - Címpárok: MAC-IP párok
      - Bejegyzéstípusok
        - Statikus: manuálisan felvitt
        - Dinamikus: ARP eredménye, elévül és törlődik
  - RARP (Reverse ARP): MAC alapján IP keresése
    - Működés: broadcast üzenettel

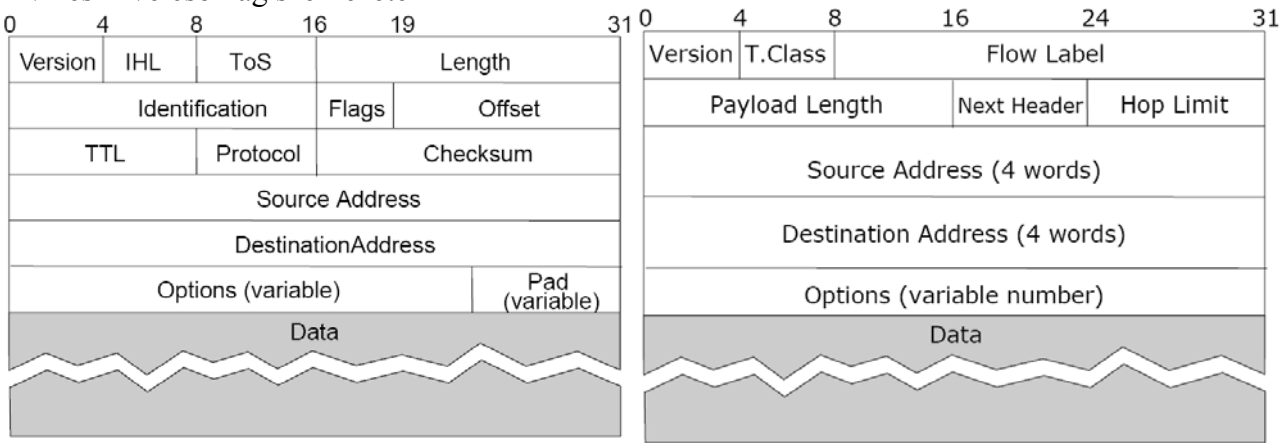
        - RARP helyett ma:
            - DHCP: IP-cím kérése
            - BOOTP: hálózatról történő betöltésre
- Routing protokollok – automatikus routing-tábla építése
    - Feladatok:
        - Routing-információk begyűjtése
        - Hurokmentes útvonalirányítás
        - Új csomópontok és hálózat csatlakoztatásának/leválasztásának kezelése
    - Funkcionális osztályozás
        - Ad hoc protokollok: kis és gyorsan változó hálózatokra, szenzor és egyéb vezetéknélküli hálózatokra
            - Osztályozás:
                - Működési mód szerint
                    - Proaktív: folyamatosan karbantartott táblákkal
                    - Reaktív: igény szerinti célfelderítés
                    - Hibrid: a kettő együtt
                - Alkalmazási terület szerint
                    - Hierarchikus
                    - Földrajzi elhelyezkedés alapján
                    - Multicast
                    - Energiatakarékos
            - Módszerek
                - Distance-vector
                - Link-state
        - IGPs (Interior Gateway Protocols): autonóm rendszereken (AS) belül, kisebb hálózatokon
            - Fajtái például:
                - IGRP (Internet Gateway Routing Protocol)
                - EIGRP (Enhanced IGRP)
                - OSPF (Open Shortest Path First)
                - RIP (Routing Information Protocol)
                - IS-IS (Intermediate System to Intermediate System)
        - EGPs (Exterior Gateway Protocols): autonóm rendszerek között – az Internet routing-protokollja
            - Fajtái például:
                - EGP: sokáig az Internet EGP-je, ma már nem használt
                - BGP (Border Gateway Protocol): BGPv4, ma is használt
            - Címaggregáció: gyorsabb keresés és gyorsabb terjesztés
- Tördelés
    - Mi az és miért kell:
        - A hálózatok alsóbb rétegei meghatározzák a keret maximális méretét, az adatkapcsolati réteg fej- és farokrészét leszámítva ez az MTU (Ethernetnél 1500 byte)
        - Az eltérő technológiák eltérő MTU-jú kapcsolatokat szülnek, tehát tördelni kell
    - Menete: a csomagot (20 byte fejléc + n byte adat) több részre bontjuk, ügyelünk arra, hogy:
        - Minden töredék önálló IP-csomag, tehát kell neki fejléc
        - A payload mérete 8-cal osztható, tehát az eredeti n byte-ot erre ügyelve kell felosztani
    - IP-fejléc tördeléssel kapcsolatos mezői: Identification, Flags, Fragment Offset
    - Fejléc változása tördelés közben:
        - Ha nem volt Identification mező érték, akkor generálni kell
        - Adat tördelése 8 byte-os egységekre
        - Fragmentation offset beállítása
        - MF-bit := 1 minden csomagra, kivéve az utolsót, ott MF := 0
    - Töredékek összeállítása:
        - Csak a címzett teheti meg

        - Ha nem érkezett be egy darab, a többit is eldobja
        - Csak teljesen összeállított csomagot továbbít a felsőbb rétegeknek
- Az IP jelzés– és menedzsment-üzenetei
    - ICMP (Internet Control Message Protocol)
        - Visszajelzés a best effort hálózattól
        - IP felett (0x01-es protokollazonosító)
        - Üzenettípusok
            - Hibaüzenetk
            - Kérdések
            - Válaszok
        - Gyakori ICMP üzenetek:
            - Echo request – echo reply → ping
            - Echo request – echo reply + TTL → traceroute
    - IGMP (Internet Group Management Protocol)
        - IP-t futtató csomópontok csoportok kezelésére
        - Főként multicast csoportok kezelésére
            - Csoportok lekérdeze
            - Csoporthoz csatlakozás
        - Általában TTL = 1 (csak a helyi hálózatban él)
- Példák
    - Hálózatok címkiosztásának tervezése
    - Egy csomag útja
- IP biztonság és egyéb technikák (NAT, IPSec, VPN)
- IPv6
    - Motivációk – az IPv4 hibái
        - Címtartomány kimerülése
        - Erőforrás-igényes – sok felesleges mező a fejlécben, tördelés a köztes csomópontokon
        - Nem biztonságos – nem támogatja a hitelesítést és titkosítást
        - Nehézkes konfiguráció – automatikusan csak megfelelő infrastruktúrával
        - Mobilitástámogatás csak külön protokollal
    - Címzés
        - 128 bites címek
        - A vezető 0-k elhagyhatók: […]:0094:[…] helyett […]:94:[…]
        - Egymást követő 16 bites csupa 0 szegmensek elhagyhatók, de csak egy ilyen tehető meg: FEDC:0000:0000:0000:000C:0000:[…] helyett FEDC::C:0:[…]
        - IPv4-es kompatibilitás: 0:0:0:0:0:0:A0:01 → 10.0.0.1
        - Hálózati címek (prefixek) jelölése: FEDB:ABCD:ABCD::/48, FEDB:ABCD:AB00::/40
        - Hivatkozásként: http://[FEDC::C:BA98:0:3210]/index.html
        - Cím prefixek: 001 – unicast address space; 1111 1111 – multicast addresses
        - Címtípusok
            - Unicast: mint az IPv4-ben. Egyedi, minden IPv6 csomópontnak legalább egy van. Típusai:
                - Globális
                - Aggregálható (hosszok bitekben értendők)
                  [FP (3) | TLA ID (13) | RES (8) | NLA ID (24) | SLA ID (16) | Interface ID (64)]
                - FP: format prefix (001)
                - TLA ID: Top-Level Aggregation ID (régió)
                - RES: reserved
                - NLA ID: Next-Level Aggregation ID (szolgáltató)
                - SLA ID: Site-Level Aggregation ID (előfizető és alhálózat)
                - Intercace ID: hossza m=64 bit megegyezés szerint, MAC címből képződik – egyediséget biztosítja, ha a HW-ből képződik a cím

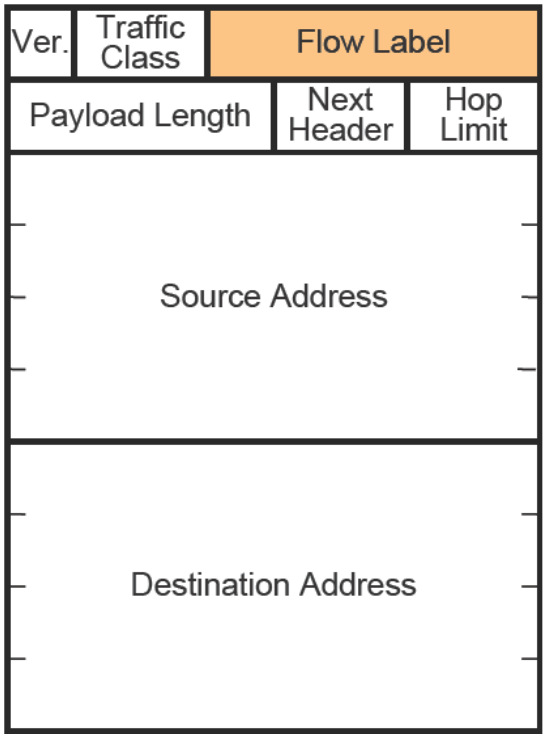
        - IPv4 kompatibilis
            - FP = 000
            - IPv4 kompatibilis IPv6 címek, pl ::10.1.4.1
            - IPv6-ra képzett IPv4 címek, pl ::FFFF:10.1.4.1
    - Link local
        - Adott linken (fizikai alhálózaton) lévő csomópontok közti kommunikációhoz
        - Formátuma: [10 bit | 54 bit | 64 bit]
        - Interface ID: EUI 64
            - U bit: 1 – univerzális, 0 – lokális
            - G bit: 1 – csoport, 0 – egyedi
    - Site local
    - Beágyazott IPv4 címet tartalmazó

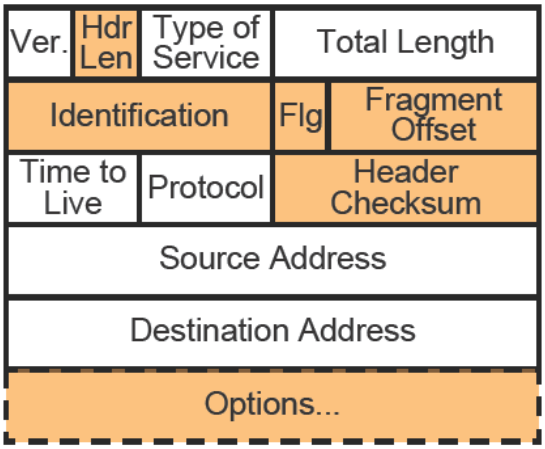
  Struktúrált cím: [a (x bit) | b (y bit) | c (z bit) | interface ID (m bit)
- Multicast: csoportot azonosít, minden csoportbeli megkapja az erre a címre küldött adatokat, boradcast helyett is ezt használjuk
    - Interfészek egy csoportját címzi
- Anycast: csoportot azonosít, biztosított, hogy egy csomópont megkapja

- IPv4 és IPv6 csomag szerkezete



  - IPv4 és IPv6 fejlécek összehasonlítása





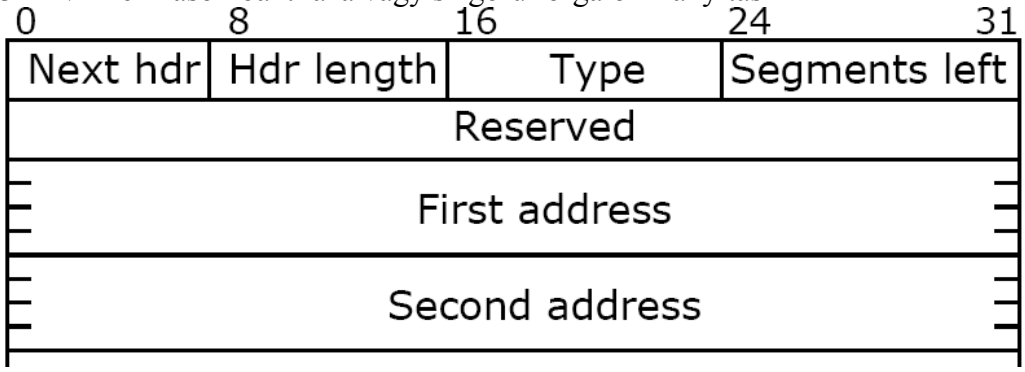
A kiemelt részek a másik verzióban nem találhatók meg!

IPv6 fejléc kétszer hosszabb (40 byte), mint az IPv4-es (20 byte)!!!

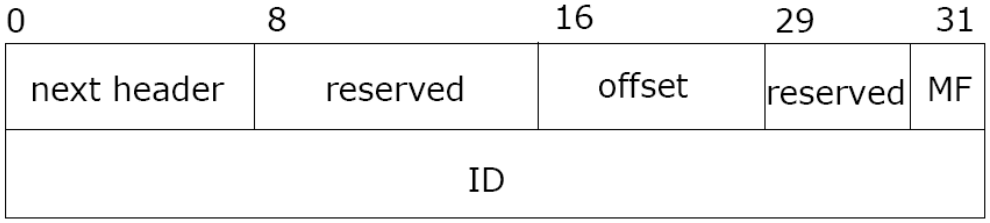
  - Az IPv6 fejléc mezői:

- Version: =6
- Traffic Class: forgalmi osztály (más néven: Priority) – QoS lehetőség biztosítása az IPv4 ToS mezőjével megegyező módon
- Flow Label: folyamazonosító címke
  - Adott kapcsolatot azonosító generált mező → nem független datagramok!
  - QoS-t és igazságos adatsebesség-megosztást tesz lehetővé
  - Virtuális összeköttetések biztosítása adatfolyamok számára
  - Egy forrás-célállomás pár esetén több adatfolyam is lehet
  - Skálázhatósági probléma a folyam-alapú eljárásoknál
- Payload Length: adathossz
  - Nem tartalmazza fejrészt
  - Max. 64 KB-os csomag (de van jumbogram opció)
- Hop Limit – ugrásszám-korlát, ugyanaz, mint IPv4-nél a TTL
- Címmezők: 2 darab 128 bites cím
- Next Header: következő fejléc. 2 lehetőség:
  - A beágyazott PDU típusát adja meg hasonlóan az IPv4 fejléc Protocol mezőjéhez
  - Az IPv6 fejléc kiterjesztését jelentő Extension mező típusát adja meg

▪ IPv6 opciók – header extensions
- Hop-by-hop options header
  - Olyan információ, melyet minden routernek meg kell néznie
  - Jumbogramok (óriáscsomagok) támogatása
  - QoS támogatása
- Routing header
  - Útbaejtendő routerek felsorolása
  - IPv4-hez hasonlóan: laza vagy szigorú forgalomirányítás

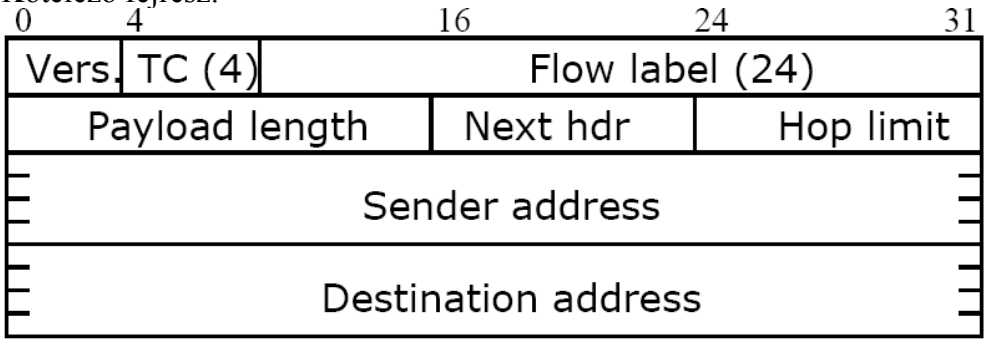


Mezők:
  - Hdr (header) length: fejléc hossza QWORD-ökben
  - Type: =0, még nem használt
  - Címek: max 24 db, következő csomópont megtalálása anycast címzéssel
- Fragmentation header: mint a v4-ben, de csak a forrás darabolhat, ehhez kell a Path MTU Discovery



Csak a feladó tördelhet, csak a címzett állíthat össze.
- Dest. options header: csak a célállomás nézheti meg, még nincs funkciója
- AH (Authentication Header): IPSec-ből
- ESP (Encapsulation Security Payload Header): IPSec-ből

- Általános fejlécformátum:
  [kötelező fejléc | extension 1 | … | extension N | data] – az extension-ök opcionálisak
  Kötelező fejrész:



  - Az IPv6 fejléc jellemzői:
    - Nincs checksum – nem kell minden routernek ellenőriznie → gyorsulás
    - Rögzített méret – gyorsabb feldolgozás
    - Nincs IHL mező – kisebb fejléc
    - Nincs ugrásonkénti tördelés → gyorsabb feldolgozás és nem kell hozzá mező a fejlécben, viszont Path MTU Discovery (útvonalon MTU-felderítés) kell!
- Biztonság az IPv6-ban: IPSec
  - Két extension header
  - Minden csomópontnak tudnia kell IPSec-et
  - AH: tényleg ő a feladó? Lett módosítva a csomag?
  - ESP: titkosított a csomag tartalma
- Infrastrukturális szolgáltatások
  - Fajtái:
    - Neighbour discovery: szomszédok feltérképezése
    - Router discovery: automatikus átjáróválasztás
    - Stateless autoconfiguration:
      - Automatikusan minden beállítást megkap
      - Duplikált címeket érzékeli
    - Path MTU Discovery: meghatározza a teljes úton az MTU-t, ezért legfeljebb a feladónál kell tördelni
  - Lehetővé teszi:
    - Okos routerek – DHCP funkcionalitás
    - Anycast címzés: „valamelyik router mondja meg, hogy…”
    - Multicast címzés: azonos szolgáltatásokat nyújtó egységek egymás közti kommunikációja: „én már nem vagyok többé router”
- IPv6 routing
  Protokoljai: RIPng, OSPFv3, IS-IS Extension for IPv6, MP-BGP, EIGRP for IPv6, Static Routing
- Áttérés IPv6-ra: 813-827 slide-ok

- Mobil IP megoldások
  - Probléma: mozgó internetező szeretné megtartani az amúgy helyhezkötött IP-címét
  - Mobil IP: módosítás az IP-rétegben – helytől függetlenül tudnak a csomópontok folyamatosan kommunikálni. A mozgó IP végpont helyváltoztatási sebessége kb. másodpercenkénti, azaz amíg a mozgás sebessége kisebb a protokoll üzeneteinek oda-vissza idejénél.
  - Fogalmak:
    - Mobile node: helyét változtató mobil eszköz
    - HA (Home agent): a mobil végpont otthoni hálózatában az a router, amely tunnelezi az adatokat
    - FA (Foreign agent): a mobil végpont aktuális tartózkodási helyéhez tartozó hálózatban egy router, aki azért felel, hogy a mobil végpont megkapja az üzeneteit
    - HoA (Home address): a mobil végpont otthoni címe
    - CoA (Care-of address): cím az idegen hálózatban

- A mobilitás megvalósításához szükséges:
  - Újracímzés otthon
  - Otthoni és idegen cím összerendelésének karbantartása
  - Datagram eljuttatása a care-of címre
  - Care-of címnél inverz újracímzés
- Regisztráció
  - Ha a node távol van, a HA-t értesítenie kell a CoA-ról
    - Közvetlenül, vagy FA segítségével
    - Regisztrációs kérelem: {HA címe | HoA | CoA | CoA élettartama}
  - FA a HA-nak továbbítja, ez
    - Elfogadja és frissíti az összerendelést, vagy
    - Elutasítja: túl hosszú igényelt időtartam, túl sok kapcsolat, stb. miatt
- CoA szerezhető
  - CoA = FA címével, ekkor a tunnel másik vége maga az FA
    - Ez jó, mert kevés címet használunk
    - És ilyenkor FA saját listán tárolja az idegen mobilok címeit
  - A távoli hálózatból kiutalunk egy IP címet a mobilnak DHCP-vel (co-located CoA), ekkor a tunnel másik vége maga a mobil node.
- Becsomagolás és alagutazás
  - Encapsulation: HA a mobil node-nak érkező csomagokat új fejléccel látja el és úgy küldi tovább
  - Tunneling: a küldő számára transzparens módon a HA továbbítja a csomagot a CoA-ra

Szállítási (transport, host-to-host) protokollok: UDP és TCP

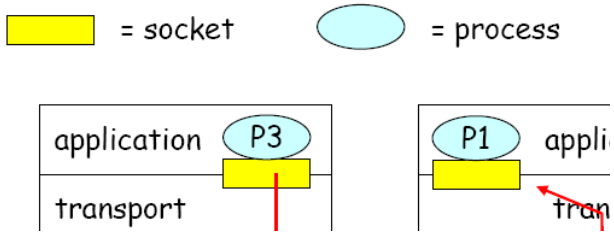
A szállítási réteg:
- Logikai kapcsolatok a végpontok alkalmazásai között
- A szállítási protokollok a végpontokban futnak, a csomópontokban nem
- Az alkalmazások adategységeit betördeljük a szállítási protokoll adategységeibe

A szállítási réteg: alkalmazások közötti logikai kapcsolatok
A hálózati réteg: végpontok közötti logikai kapcsolatok

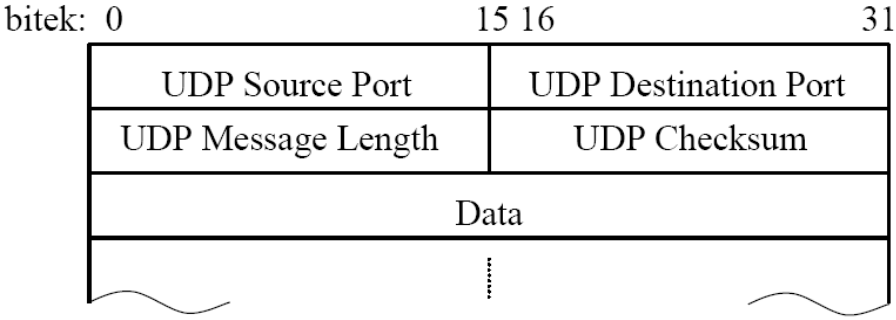
Szállítási protokollok: UDP és TCP
- UDP: User Datagram Protocol
- TCP: Transmission Control Protocol
- Közös képességek
  - Portok kezelése
  - Multiplexelési képesség
- Különbségek
  - Az UDP kapcsolatmentes transzport-szolgáltatást nyújt
  - A TCP kapcsolatalapú

UDP
- Portok kezelése
  - Az IP-rétegben a csomagok végpontnak (host-nak) vannak címezve
  - A végpontokon belül több alkalmazás is fut (és egy alkalmazás több másik alkalmazással is kommunikálhat), ezeket meg kell tudni különböztetni – erre valók a portok
  - Foglalt portok: ide mindig lehet küldeni datagrammokat, pl. 69 port: TFTP
  - Az UDP-n belül megállapításra kerülnek az alkalmazandó port-számok

- Multiplexelési képesség
  - A port-mechanizmus segítségével:



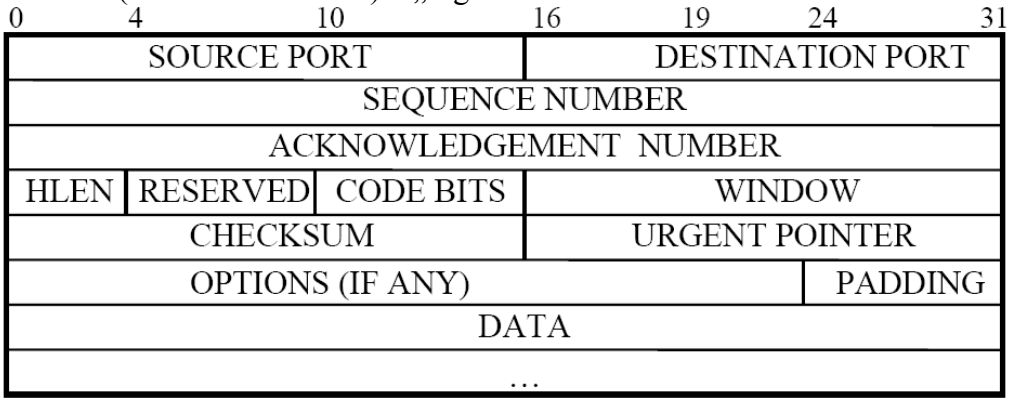
- UDP-datagramm:
  Fejrész mérete: 8 byte



  Source port: opcionális (nem használt: 0)
  Hossz: oktettben, min: 8
  Checksum: opc (nem használt: 0)
  Megj.: az IP-csomag ellenőrzése csak a fejrészre terjed ki, az UDP checksum tudja csak az egész csomagot ellenőrizni!

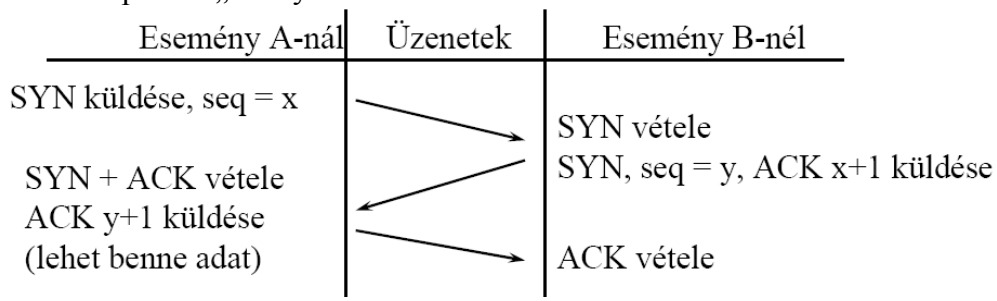
TCP

- Célja: megbízható adatszállítás az IP nem megbízható datagrammjaival
- Jellemzői:
  - Virtuális összeköttetések a kommunikáció időtartamára
  - Stream-típusú szolgáltatás: bit- (egyéb-) streamek sorrendhelyes átvitele
  - Strukturálatlan stream: delimiter-mentes streamek átvitele
  - Pufferelt átvitel: megvárja, amíg van elég elküldenő adat a stream-ből
  - Duplex kapcsolatok
  - Vezérlő információk küldése: piggyback módon (ellenkező irányban folyó stream-be ágyazva)
- Megvalósítás:
  - Pozitív nyugtázással – nem lenne hatékony
  - Csúszóablakkal (az ablak mérete = kint lévő, nyugtázatlan csomagok száma)
    - Ez a TCP-ben oktett-eken működik
    - Hatékony
    - Egyben forgalomszabályzási módszer is
- A TCP PDU (Protocol Data Unit) – „segment”

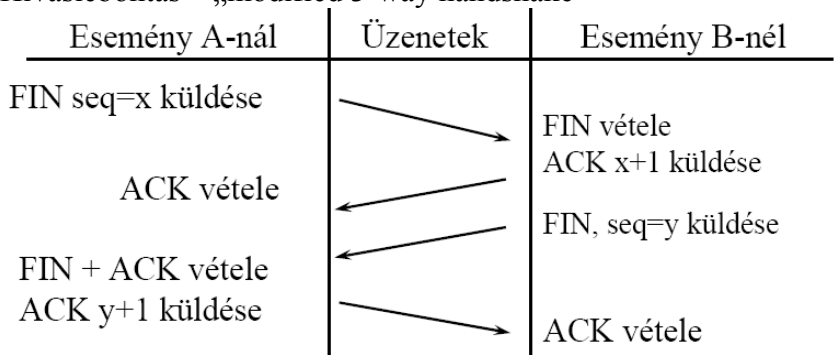


  - Seq. number: az adat helye a byte-stream-ben

    - Ack. number: a legközelebb várt byte sorszáma
    - Code bits: a szegmens tartalma
    - Window: a küldő vételi pufferének mérete
    - Checksum: mint az UDP-nél
    - Urgent pointer: out-of-band adatok küldésére
- Hívásfelépítés – „3-way-handshake”



- Híváslebontás – „modified 3-way handshake”



TCP és UDP – összefoglalás
- Mindkettő host layer / transport layer protkoll
- Mindkettő portokat kezel
- Az UDP összeköttetésmentes, best-effort szolgáltatást nyújt, gyors
- A TCP összeköttetés-alapú, megbízható transzportszolgáltatás, lassú

Multimédia továbbítása IP felett – RTP

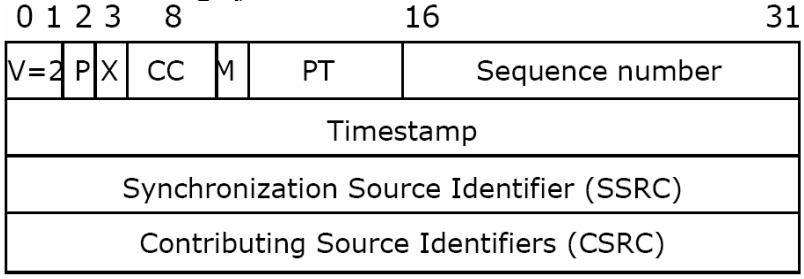
Bevezetés
- Alkalmazás-rétegbeli protokoll
- cél: média továbbítása
- ezek a protokollok vezérelnek ugyan, de nem csinálnak hívásvezérlést, az egy másik protokollcsalád dolga

RTP és RTCP
- RTP – RealTime Protocol
    - Lényege: a payload-ban média adat, pl. beszéd
    - UDP felett működik
    - Lehetséges közvetlenül IP felett is, de ez ritka
    - Nincs QoS
- RTCP – RealTime Transport Control Protocol
    - End-to-end QoS-monitoring
- Különböző UDP portokat használnak párban
    - RTP: páros számú portot
    - RTCP: páratlan számú portot

RTP szolgáltatásai
- Payload-típusok kezelése
- Sorszámozás

- Időbélyegzés

Az RTP csomagfejrész-formátum:



- Version (V, 2 bit)
- Padding (P, 1 bit): ha 1, a csomag nincs teljesen kitöltve adattal; az utolsó byte tartalmazza, hány byte-ot kell figyelmen kívül hagyni
- Extension (X, 1 bit): ha 1, a header után változó hosszúságú header extension jön, aminek az első 2 byte a hosszát adja meg, maga az extension pedig a fix fejrész utolsó érvényes mezője után van
- CC (CSRC Count) – a CSRC azonosítók száma = a multiplexelt források száma. Ha csak egy forrás van, értéke 0.
- Marker (M, 1 bit): a csomagfolyam fontos eseményeit jelöli, pl. kerethatárok; értelmezését a „profile” (PT) adja
- PT (Payload Type, 7 bit): „profile”, a médiakódolási típusokhoz payload-formátumokat rendel
- Seq. number (16 bit): minden elküldött csomag után nő 1-gyel, kezdőértéke véletlen
- Timestamp (32 bit): az első oktettnek megfelelő pozíció valós ideje, pl. beszédnél a mintavételezési időpont
- SSRC (Stream Source, 32 bit): a csomagfolyam forrása, az RTCP rendeli hozzá
- CSRC (Contributing Source, 32 bit): az „RTP mixer” által létrehozott kombinált csomagfolyam komponensét azonosítja

Payload-multiplexelés – javítja a sávszélesség-kihasználást

RTSP – RealTime Streaming Protocol
- Kapcsolat felépítése és kilépés
- Lejátszásvezérlés

RTCP – RealTime Transport Control Protocol
- End-to-end információt szolgáltat a minőségről a kapcsolat résztvevőinek: késleltetés, jitter, lost packets, …
- Nem jelzésátviteli protokoll!
- Csomagtípusai:
    - SR (Sender Report) – aktív adók statisztikái, a session minden résztvevőjét informálja
    - RR (Reciever Report) – inaktív adóktól jövő információk
    - SDES (Src Description) – helyi jellemzőket szolgáltat (hely, telefonszám, e-mail-cím)
    - BYE (close session) – egy forrás elhagyja a konferenciát
    - APP (Application-specific packet) – végpontok alkalmazásai közti kommunikáció

Összefoglalás
- RTP: a médiatranszport-protokoll a VoIP rendszerekben is
    - UDP felett működik
    - Többfajta médiakódolást támogat
    - Az átvitelért felelős, a QoS-ért nem
    - A teljes fejrész (RTP+UDP+IP) kompresszióval csökkenthető (először csak a fejrész küldése, majd ideiglenes kapcsolatazonosító használata)
- RTCP: az RTP társprotokollja
    - Nem jelzésprotokoll
    - Nem QoS protokoll
    - Hasznos segédeszköz a QoS megvalósításához

Hívásvezérlő protokollok

IP-hálózatokon működő multimédia-kommunikáció hívásvezérlése

H.323 – ITU

- Ma főleg IP-felett, használat főleg VoIP és videokonferencia-rendszerekben
- Meghatározza a csomag- és áramkörkapcsolt hálózatok közti együttműködést
- Komplett szabvány-dokumentáció
    - Audio, videó kodólás
    - Hívásfelépítés és –vezérlés, az ehhez tartozó jelzésátviteli protokollokkal
    - Regisztráció és hozzáférés-szabályozás
- Ma: multimédia kommunikáció alapvetően IP-hálózatok felett – nem-QoS hálózatokra tervezték
- Együttműködik az egyetlen élő, másik szabvánnyal, a H.320-szal, amely audiovizuális kommunikáció ISDN-en (és más, áramkörkapcsolt hálózatokon)
- Funkcionális egységek
    - Terminal (TE): felhasználói végpont
    - Gateway (GW): együttműködést biztosít a H.323 és más típusú terminálok között; konvertál a különböző jelzésrendszerek között; általában TE-be, GW-be, MCU-ba integrálják.
    - Gatekeeper (GK): opcionális, de ha van, „központi intelligencia”. Kötelező funkciók:
        - Címfordítás: LAN ↔ E164
        - Beengedés-szabályozás jogosultságok alapján
        - Sávszélesség-menedzsment
        - Opcionális funkciók továbbá: hívásvezérlés, QoS
    - Multipont Control Unit (MCU): 3 vagy több terminál közötti konferencia
        - Részei:
            - MC (Multipont Controller): hívásvezérlés 3 v. több résztvevős konferenciánál, képességegyeztetéssel
            - MP (Multipont Processor): audio- és videófolyamok kezelése, keverés: dekódolás, lineáris kombináció-képzés, újrakódolás
- Protokoll-architektúra
    - Hívásvezérlő protokollok
        - H.225
            - A H.323 jelzásátviteli protokollja
            - TCP felett működik a TPKT közbeiktatásával
        - H.225RAS
            - GK-protokoll
            - UDP felett
        - H.245 – call control signalling
            - Médiaátvitellel kapcsolatos funkciók (képesség-egyeztetés), multipont- (konferencia-) vezérlés

      Egy hívás menete
      1) Call admission – RAS – engedélykérés a GK-tól híváskezdeményezéshez/-fogadáshoz
      2) Call setup – H.225 – végpontok közti kapcsolat felépítése
      3) Képességegyeztetés – H.245 – képességegyeztetés, master-slave viszony kialakítás, logikai csatorna felépítése
      4) Stabil kapcsolat – RTP
      5) Csatorna lezárása – H.245 – logikai csatornák lezárása
      6) Kapcsolat vége – H.225 – hívás befejezése
      7) Felszabadítás – RAS – erőforrások felszabadítása
    - Médiakezelés (pl. tömörítés)
    - Médiaszállítás – RTP

    - Protokollok QoS-hez – RSVP
    - Mindez IP és TCP/UDP felett
- Problémák a H.323 első verziójával
    - Túl lassú hívásfelépítés
    - Hívás alatt nincs mód jelzésátvitelre
    - Különválik a jelzésátvitel és a hívásvezérlés
- Megoldás: H323v2: FastStart bevezetése
- Összefoglalás:
    - ITU szabvány: sok mindent átvett a távközlésből; Internet-protokollokat használ (RTP, TRCP)
    - Széles spektrumú szabvány
        - Médiák (hang, videó, adat)
        - Protokollok – hívásvezérlés, médiafeldolgozás, QoS
    - Funkcionális egységek: T, GW, GK, MCU
    - Hívásvezérlő protokollok p-p és p-mp kapcsolatokhoz
    - Állapot-alapú és bináris protokoll

SIP (Session Initiation Protocol) – IETF
- Alkalmazási rétegbeli protokoll a TCP-IP architektúra szerint
- Session-ök létrehozása, módosítása, befejezése egy vagy több partnerrel
- Különböző médiatípusokhoz különböző session-descriptorokat visz át képesség-egyeztetés céljából
- Kezeli a felhasználók helyzetinformációit, támogat pl. hívásátadást
- Támogatja a mobilitást
- MCU funkció vagy teljes mesh-kapcsolatok
- Protokollok – amikkel együttműködik, vagy amiket használ
    - RTP/RTCP/RTSP – a médiatartalom átvitelére
    - SAP (Session Announcement Protocol) – multimedia session-ök hirdetésére
    - SDP (Session Description Protocol) – multimedia session-ök leírására
    - RSVP – erőforrás-foglalásra
- Jellemzők
    - Text-alapú (hasonlóan a HTTP-hez), tehát SIP-üzeneteket könnyen generálhatnak emberek és programok (CGI, Perl, Java)
    - SIP URL-ek (Uniform Resource Locator): hasonlóak az e-mail URL-hez
    - UDP vagy TCP felett működik
- Építőelemek
    - UA (User Agent): lehet HW-alapú IP-telefon, vagy SW-alapú softphone
        - Két logikai részből állnak
            - UAC (UA Client): requestek küldése, response-ok vétele
            - UAS (UA Server): requestek vétele, response-ok küldése
        - „request”-eket kezdeményeznek, ill. azok címzettjei
        - IP-telefon, PC, konferencia-szerver
    - Proxy server: session invitation-öket továbbítja a hívott felé
        - Típusai:
            - Állapotmentes: egyszerű és gyors üzenettovábbítók
            - Állapot-alapú: forking
                - Más jelzésprotokolloknál ilyen nincs: híváskérések elágaztatása: a szerver egy beérkező reqeust üzenet vételekor 2 v. több request-et küld ki különböző címzetteknek egyidejűleg vagy egymás után
                - Ezzel valósít meg a SIP különböző emeltszintű szolgáltatásokat, pl. hívástovábbítás hangportára és automatikus hívás-szétosztás
        - Router a „request”-ekhez és „response”-okhoz
        - Az UA-k (a kliensek) megbízásából dolgoznak
    - Registrars
        - Felhasználók nyilvántartása egy domain-en belül

        - Név-cím összerendelések kezelése
    - Redirect servers
        - Request-re megadják a felhasználó címét
        - Nem kezelnek hívásvezérlést és nem továbbítanak SIP request-eket
- Üzenetek
    - Két fő kategória:
        - Request
            - INVITE – híváskezdeményezés
            - ACK – válasz nyugtázása
            - BYE – hívás befejezése
            - CANCEL – keresés és „csengetés” törlése
            - OPTIONS – a másik fél képességei
            - REGISTER – regisztráció a location service-szel
        - Response
    - Nagyon hasonlít a HTTP/1.1-hez
    - A formátum a két kategóriára ugyanaz az első sor kivételével
    - Tartalmazhat üzenettörzset
        - Session description
        - ASCII vagy HTML
- SDP (Session Description Protocol) – session-ök leírása és módosítása
    - Inkább leíróformátum, nem protokoll
    - Multimédia session-ök leírására
    - Az SDP-t az üzenetek mint message body viszik át
    - Jelzi
        - A vételo képességeket
        - A médiastream-ek cél-portcímeit
- A SIP előnyei
    - Programozhatóság
    - Integráció más Internet-szolgáltatásokkal
        - Címek hasonlóak a sima URL-hez, ezért weblapba, e-mailbe ágyazhatók
        - A hívások weblapokhoz, e-mailre, IRC-re, chat-re továbbíthatók
        - Bináris és szöveges adatátvitel

Összefoglalás
- H.323
    - ITU
    - Távközlési hívásvezérlő protokollon alapul
    - Rosszul skálázható (Megaco/H.248-cal kombinálás segít)
    - Állapot-alapú, bináris protokoll
    - Webalapú szolgátatásokkal nehezen kombinálható
- SIP
    - IETF
    - IP-központú
    - Állapotmentes, szöveges protokoll
    - Kombinálható mindenféle webalapú szolgáltatással

Megaco / H.248 – IETF és ITU
- Az IETF és az ITU közti együttműködés eredménye
- Előzményei:
    - SGCP (Simple GW Control Prot.)
    - MGCP (Media GW Control Prot.)
- XGCP alapelve

    - GW-re koncentrál
    - Válasszuk el a GW-től annak vezérlését
        - MG – media GW
        - MGC – media GW controller
    - Kapunk egy belső szétosztott rendszert, mely kívülről egynek látszik
- Előny:
    - MG-k és MGC-k szabad elhelyezhetősége a hálózatban
    - Bővíthető rendszer
- Referenciamodell
    - MG
        - „Részei”:
            - Endpoint-ok: a médiafolyamok be- és kilépési pontja, HW/SW az MG-ben
            - Connection-ök: különböző MG-k endpoint-jai együttesen, p-p v. p-mp kapcsolatok
            - Call: a connection-ök logikai társítása, p-p és p-mp kapcsolatok
        - Doboz, általában a felhasználónál
    - MGC
        - Itt futnak az MG-ket vezérlő protokollok
        - Nyilvános távközlési szolgáltató esetén ez a központban van (neve: softswitch)

Megaco/H.248 összefoglalása
- Vezérlő protokoll a szétbontott GW két komponense, az MG és MGC-k között
    - nem hívásvezérlő protokoll
    - a media GW vezérlési és hívásvezérlési funkciók ortogonálisak
    - a GW-funkcionalitás MG-re és MGC-re történő szétbontásának előnyei:
        - kiterjeszthetőség
        - MG-k szabad elhelyezése
- Fontos bővítés az M.323-hoz
- SIP-pel kombinálható

QoS: a best effort-on túl – IntServ, DiffServ

QoS-t igénylő alkalmazások:
- valós idejű, átvitel- és késleltetés-érzékeny
- nem valósidejű, elasztikus, átvitel- és késleltetés-tűrő

QoS összeköttetés-alapú hálózatokban
- Elv: minden ATM összeköttetéshez társul QoS kategória, a hálózat ezt garantáltan betartja
- Megvalósítás:
    - Forgalomjellemzés, forgalomleírók
    - QoS paraméterkészlete
    - ATM szolgáltatási kategóriák
    - Torlódásvezérlés
        - Preventív: CAC (Call Admission Control) – beengedés-szabályozás
        - Reaktív: ABR

ATM QoS-szolgáltatások
- CBR
    - Forgalomleírók: PCR, CDVT
    - QoS jellemzők: maxCDV, maxCTD, CLR
- rt-VBR
    - Forgalomleírók: PCR, CDVT, SCR, MBS
    - QoS jellemzők: maxCDV, maxCTD, CLR

- nrt-VBR
    - Forgalomleírók: PCR, CDVT, SCR, MBS
    - QoS jellemzők: CLR
- UBR
    - Forgalomleírók: PCR specifikált, de a CAC és a policing nem használja
    - QoS jellemzők: nincs

QoS összeköttetés-mentes hálózatokban
- IP-alapú megoldások
    - IntServ (Integrated Services) – egyedi csomagfolyamokra, finom felbontású módszer
    - DiffServ (Differentiated Services) –folyamosztályokra, durvafelbontású módszer
- ATM
    - Önmagában finom felbontású, de a QoS nem a hálózati rétegben valósul meg
    - Lehet durva felbontású, lehet összefogott csomagfolyam egyetlen VC-n

QoS módszerek viszonya:
- Best-effor: megkülönböztetés nélküli csomagtovábbítás
- DiffServ: különböző kiszolgálás folyamosztályokra
- IntServ: igényeket figyelembe véve egyedileg szolgál ki csomagfolyamokat

IntServ (Integrated Services)
- Szolgáltatásosztályok
    - Best effort
    - Guaranteed quality: garantált korlátok bármely csomag késleltetésére
    - Controlled-load: függetlenít a többi forgalomtól, törekszik a legjobbra
- Alkalmazások igényei és az IntServ-szolgáltatások
    - Elastic applications
        - Nincs késleltetési vagy egyéb korlát
        - Tipikus TCP/IP adat-alkalmazások

      → Best effort service – 3 alosztály:
        - Interactive burst (pl. web)
        - Interactive bulk (pl. FTP)
        - Async (pl. e-mail)

      ATM-analógia: UBR
    - RTT (RealTime Tolerant) app's
        - Enyhe késleltetési korlátok, alkalmankénti csomagvesztés megengedett

      → Controlled load service
        - Átlagos késleltetést garantál, mennyiségi biztosítékok nélkül

      ATM-analógia: nrt-VBR
    - RTI (RealTime Intolerant) app's
        - Min. késleltetés és –ingadozás
        - Pl. beszéd, videókonferencia

      → Guaranteed Service

      ATM-analógia: rt-VBR, CBR
- IntServ mechanizmusok
    - Forgalomleírók – traffic descriptors: a felhasználó specifikálja igényeit (flowspec)
        - Elemei:
            - TSpec (traffic specification): szükséges sávszélesség megadása a forgalmi jellemzők leírásával
            - RSpec (request spec.): szolgáltatási igény megadása (controlled load, késleltetési korlát)
    - Beengedés-szabályozás – admission control: a felhasználó meghatározott szolgáltatást kér, a hálózat ez alapján dönti el, beengedi-e
        - A TSpec és az RSpec-et alapján dönt
        - Controlled load esetén jó lehet a heurisztika is

        - Guaranteed esetén szigorúbb vizsgálat kell
    - Erőforrásfoglalás jelzésátvitellel: a felhasználó és a hálózat megbeszéli az erőforrásfoglalást (áramkörkapcsolt vagy összeköttetés-alapú hálózatoknál ez mehet a hívásvezérlő protokollokkal)
    - A forrás forgalmának ellenőrzése és szűrése– policing: a hálózat ügyel arra, hogy a forrás forgalma ne térjen el a megadottól
        - Eszköze: tokenvödör, mely szűri a forgalmat: küldhetünk *b* byte-nyi burst-öt (ha a vödörbe nem fér be, eldobunk belőle), de az átlagsebesség csak *r* byte/sec lehet (ezeket a paramétereket (is) használjuk a TSpec-ben)
    - Ütemezés – scheduling: a hálózat összeállítja a kiszolgálási csomagsorrendet a csomópontokon
- Jelzésátvitel: az RSVP (Resource reSerVation Prot.) – nem csak az IntServ-nél (H.323-nál is)
    - Jellemzők:
        - Vevőoldali erőforrás-foglalás (a vevő foglal az adótól képességeket saját igényei szerint) tehát egyirányú (szimplex) csatorna, illetve a vevőnek ismernie kell:
            - az adó TSpec-ét
            - a csomagok útját, hogy erőforrást foglalhasson a csomópontoknál

          Menete:

          21) az adó PATH üzenetet küld (benne: TSpec), ezt az úton minden úton levő router feljegyzi
          22) a vevő RESV üzenettel foglal, benne: RSpec

        - Soft State: az igények elhalnak, ha
            - Nem igényli a session explicit lezárását – kedvez a multicast-nak
            - Időnként (félpercenként) nem frissíti a foglalást – CPE-k hibáitól védi a hálózatot
- Az IntServ csomagkezelése
    - Csomagminősítés
        - A source addr, dest addr, protocol number, src port, dest port értékek alapján minden csomagot hozzá kell rendelni az arra vonatkozó foglaláshoz
    - Csomagkezelés
        - Guaranteed service esetén WFQ biztosítja a végpontok közti késleltetést
        - Controlled-load esetén elég ennél egyszerűbb módszer is
- IntServ skálázhatóság (növekedési képesség)
    - Nem képes növekedni
        - Best effort kiszolgálásnál nincs folyamhoz kötött állapot-nyilvántartás a routernél
        - Ezért a hálózat növekedésével elég, ha a routerek a linkek sebességnövekedésével lépést tudnak tartani
    - Lényegében összeköttetés-alapú szolgáltatást nyújtunk (annak minden nehézségével), de anélkül, hogy annak előnyét, a lokális címzést kihasználnánk.
    - Olyan módszer kell, mely nem egyedi folyamokat kezel.

DiffServ (Differentiated Services)
- Kisszámú forgalomosztályhoz rendel erőforrásokat
    - Osztály lehet pl. Premium, Regular
- Nem használ külön jelzéseket (pl. RSVP), pl. egy folyam Premium-igényét a csomagfejben jelzi egy bittel
- Architektúra
    - Edge router
        - Folyamonkénti forgalommenedzselést végez
        - A széleken megjelöli a csomagokat, a folyamonkénti profil szerint, ez lehet:
            - In-profile
            - Out-profile
        - Megjelölés
            - Osztály szerinti: a különböző osztályokhoz tartozó csomagokat eltérően jelöljük
            - Osztályon belüli: a folyam konform (profilnak megfelelő) és non-konform részei eltérő jelölést kapnak

        - Menete
            - Megfigyeljük a forgalmat (meter) és a nem konform csomagokat vagy formáljuk (shaping), vagy eldobjuk (dropping)
        - Profile: egyeztetett A sebesség és B vödörméret
    - Core router
        - Osztályonkénti forgalommenedzselést végez
        - Pufferelés a jelölések alapján: elsőbbség az in-profile csomagoknak
- Routerek viselkedése
    - PHB (Per-Hop Behavior) – a különböző szolgáltatásokat a DiffServ ezzel a routerenkénti viselkedéssel éri el; a PHB kiválasztásához az IP fejléc ToS mezőjében 6 bit szolgál IPv4 esetén (IPv6-nál a Traffic class mezőben), ez a 6 bit a DSCP (DiffServ Code Points).
      Két alapvető PHB:
        - EF (Expedited forwarding)
            - Ez a legegyszerűbb PHB, a csomagok továbbítása minimális késleltetéssel és kis csomagvesztéssel történik
            - Célszerű, ha az EF-forgalom érkezési ütemét csak a routerek link-sebessége korlátozza
            - Az EF előnyt élvez más forgalmakkal szemben
            - Alkalmazások: beszéd, videó
        - AF (Assured forwarding)
            - Összesen 14 kiszolgálás közül a DSCP mező 6 bitje választja a megfelelőt:
                - AF DSCP
                - EF DSCP: 101 110
                - Best effort
            - A megfelelő kiszolgálást prioritásos sorok és eldobási jellemzők valósítják meg
    - Nincs együttműködés a végpontok között, mint az IntServ-nél
- Előnyök
    - 3. rétegbeli, így bármely 2. rétegbeli – IP-re alkalmas – infrastruktúrán működhet
    - Nem kell jelezni minden routeren
    - Nincs folyamonkénti állapot-nyilvántartás a gerinchálózatban
    - A komplexitást a hálózat szélére tolja
- Hátrányok
    - Önmagában nem ad QoS-t a végpontok között
    - Problémás, ha az úton van nem DiffServ-képességű router

IntServ és DiffServ összehasonlítás:

Jellemző	IntServ	DiffServ
Szolgáltatások kezelési módja	Végpontok között	Helyi (hop-by-hop)
Szolgáltatások kezelési hatóköre	Unicast/multicast út	Bárhol a hálózatban
Skálázhatósági korlát	Csomagfolyamok száma	Szolgáltatásosztályok száma
Számlázás alapja	Forgalom és QoS jellemzők	Forgalmi osztály használat
Forgalommenedzsment	Kb. mint az áramkörkapcsolt	Kb. mint az IP-hálózat
Tartományon átívelő megvalósítás feltétele	Többoldalú megállapodás	Kétoldalú megállapodás

IntServ szolgáltatás a DiffServ hálózaton:

21) Az adó PATH üzenetet küld a vevőnek
22) A vevő RESV válasza eléri az adóoldali Edge router-t
23) Ez a router a DiffServ Bandwidth Broker-éhez fordul egy igénnyel
24) Ha a BB elfogadja, akkor értesíti az adót (RESV)
25) Az adó elkezdi a csomagküldést, az Edge router jelöli a csomagokat DSCP-vel
26) Az Edge router ellenőrzi az adó forgalmát: megfelel-e a szolgáltatási szerződésnek, a kilógó csomagokat eldobja vagy lepriorizálja
27) A Core router-el csak a DSCP-t nézik és végzik a PHB-t

QoS-biztosítási módszerek összefoglalva:

- Összeköttetés-alapú hálózatokon: ATM
- Összeköttetés-mentes hálózatokon (módszerek a hálózati rétegben, IP-protokoll alapján)
    - IntServ: folyamonkénti QoS, rosszul skálázható
    - DiffServ: osztályonkénti QoS, gerinchálózatban alkalmazható
    - End-to-end (végpontok közti) QoS-het a kettő együtt kell

MPLS – Multi-Protocol Label Switching

Összeköttetés-alapú hálózatok

- A routerek packet forwarding feladat feladata egyszerű, ezáltal gyorsak
- A packet forwarding tevékenysége független az útvonalirányítási tevékenységétől
- A kapcsolatot csak egyszer kell felépíteni, ez megtehető okosan
- Működés:
    - Felhasználó jelzési információt küld, benne a cél globális címével
    - A router a routing tábla alapján továbbküldi a csomagot
    - Feljegyzi a kiépülő csatornabeli címkéjét (lokális azonosítóját)
    - Elküldi a következő routernek a saját címkéjét
    - A kommunikáció végén a csatornát le kell bontani

Összeköttetés-mentes hálózatok

- Nem kell várni a kapcsolat felépülésére
- Hibatűrő (útvonalválasztás)
- Nagyon jó „túlélési esélyek”
- Működés: jön a csomag, továbbítjuk, adminisztráció nincs; nem is akarunk a routerekben állapot-nyilvántartást

A két módszer kombinálása

- Ha kell QoS, kell állapot-nyilvántartás is
- Tulajdonképpen készíthetnének az összeköttetés-mentes hálózatok is feljegyzéseket, akár az összes lehetséges VC-ről, mielőtt még bárki igényelte volna – ez nem lenne olyan állapot-nyilvántartás, mint az összeköttetés-alapú hálózatnál
- A routing táblák bejegyzéseiben a globális címek mellett/helyett tárolunk lokális azonosítókat is, így lehetséges a csomagok routolása helyett a kapcsolásuk

MPLS – MultiProtocol Label Switching: kapcsolás a továbbításhoz, címke az adatkapcsolati rétegbeli adategységben. Az MPLS + IP egyesíti az IP és az összeköttetés-alapú csomagkapcsolás legjobb tulajdonságait.

Az IP és az MPLS csomagtovábbítása – összehasonlítás

- IP
    - Csomagtovábbítása nem elég hatékony
    - Az összeköttetés-mentesség miatt minden router dönteni kényszerül, az IP-fejléc a döntéshez szükséges információn kívül sok felesleget tartalmaz
- MPLS
    - Felosztja a címteret FEC-ekre (Forward Equivalence Class) – ezek a továbbítást tekintve azonosan kezelendő csomagosztályok – és ezeknek megfelelő rövid, lokális érvényű címeket = címkéket használ a továbbításho

Az MPLS

- Működése: útvonalirányítás a határon, kapcsolás a gerincben
    - A címkekapcsoló router (LSR – Label Switching Router) a csomagokat a rájuk ragasztott fix hosszúságú címkék alapján továbbítja, ez mutat a kimenő interfészre

    - Az LSR átírja a címkét a csomag elküldése előtt
    - Az ATM kapcsolók ugyanígy továbbítják a cellákat
- Elemei
    - A csomagtovábbítás LSP-ken (Label Switched Path – címkekapcsolt utakon) történik
    - Az LSP-t az LSR-ek és LER-ek alkotják:
        - LSR: gyors router az MPLS-gerincben
        - LER (Label Edge Router) egy router az MPLS és a hozzáférési hálózat határán
    - A címkék kiosztását vagy az LDP (Label Distributing Prot.), vagy az RSVP, vagy valamelyik routing protokoll végzi
    - Az adatcsomagok végigviszik címkéiket az útjukon
- A csomagtovábbítás előnyei
    - Csak a belépésnél történik FEC-be besorolás
        - A besoroláshoz sok szempont figyelembe vehető az IP-fejen túl
        - Buta, de gyors gépek a csomópontokon
        - Ugyanaz a csomag máshogy sorolható be a belépő (ingress) routertől függően
        - A csomagnak nem kell magával vinnie a preferált útvonal adatait
- A FEC és a címkék
    - FEC: a csomagok egy csoportja, besorolás csak a belépéskor
    - Címkék:
        - A csomag a címkét magával viszi egy 2. réteg jelölésként
        - Minden közbenső router a címke alapján továbbítja a csomagot
        - A címkék értéke lokális jelentésű
- Címkék elhelyezése
    - Közbeiktatott (shim/ferinc) header: [adatkapcs. Fej | MPLS fej | hálózati fej | egyéb fej + adat]
      MPLS-fej: [címke (20 bit) | Exp (3 bit) | S (1 bit) | TTL (8 bit)]
    - Ha az adatkapcs.rétegbeli protokoll összeköttetés-alapú, használhatjuk annak a címkéjét
        - ATM celláknál: VPI/VCI
        - Frame Relay keretkben: DLCI
- Címkék kiosztása – honnan tudja a küldő, milyen címkét használjon
    - MPLS-ben több protokoll is használható ehhez
        - BGP kibővítve – saját adatok mellett címkeinformációt is vihet
        - RSVP – ugyanígy
        - LDP (Label Distribution Protocol)
    - Szabályok
        - Fogadó kijelöli, küldőnek továbbítja
        - Kéretlenül vagy kérésre
- Címkekapcsolt utak létrehozása – a címkekiosztás szabályai
    - Az MPLS-képességű eszközök MPLS-tartományt képeznek, ezeken belül képzünk a FEC-ekhez utakat, ezek az LSP-k. Az LSP létrehozása megelőzi az adatátvitelt.
    - Az MPLS két módja LSP-képzésre:
        - Lépésenkénti: minden LSR önállóan választ lépést egy FEC-hez, bármilyen routing protokollt használva
        - Explicit: forgalommenedzsment vagy QoS szempontok szerint létrehozott LSP-k
- Összefoglaló
    - Az IP hálózat routerei a routing révén minden lehetséges útra vonatkozó információval rendelkeznek
    - A lehetséges utak rögzíthetők, még mielőtt bárki igényelné őket
    - Különböző minőségű utak igény szerint is kialakíthatók
    - A hálózati rétegben kialakított utakon (LSP) a csomagtovábbítás az adatkapcsolati rétegben történik (címkekapcsolással)

A GMPLS (általánosított MPLS)

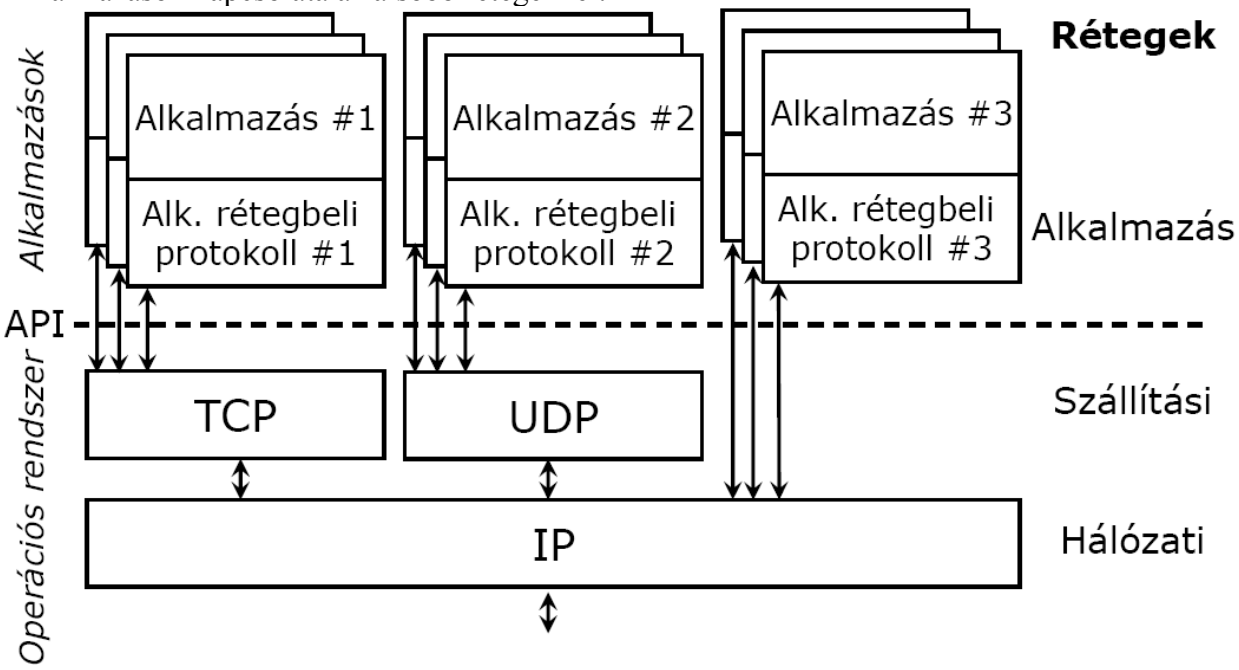
- Címkekapcsolt utak létrehozása nem csak csomagkapcsolt hálózatokban
    - PSC (Packet Switch Capable interfaces)

    - L2SC (Layer-2 Switch Capable interfaces)
    - TDM (TDM Capable interfaces)
    - LSC (Lambda Switch Capable interfaces) – hullámhossz
    - FSC (Fiber-Switch Capable interfaces)
- Az utak a csomaghálózat csomópontjait összekötő linkeken jönnek létre
- Ezek kialakítása idő-, hullámhossz- és térosztású fizikai hálózatokon történik
- A fizikai átviteli utak vezérlése (jelzése) történhet meg a GMPLS révén a hálózati szintről

Hálózati alkalmazások

Alkalmazásrétegbeli protokollok, hálózatbiztonság

Alkalmazások kapcsolata az alsóbb rétegekkel:



Alkalmazás-rétegbeli protokollok
- Általában az alkalmazás implementálja
    - Logikájához igazodik
    - Kevés másik alkalmazás használja
- Mégis szabványosítani kell, hogy a programok együttműködhessenek

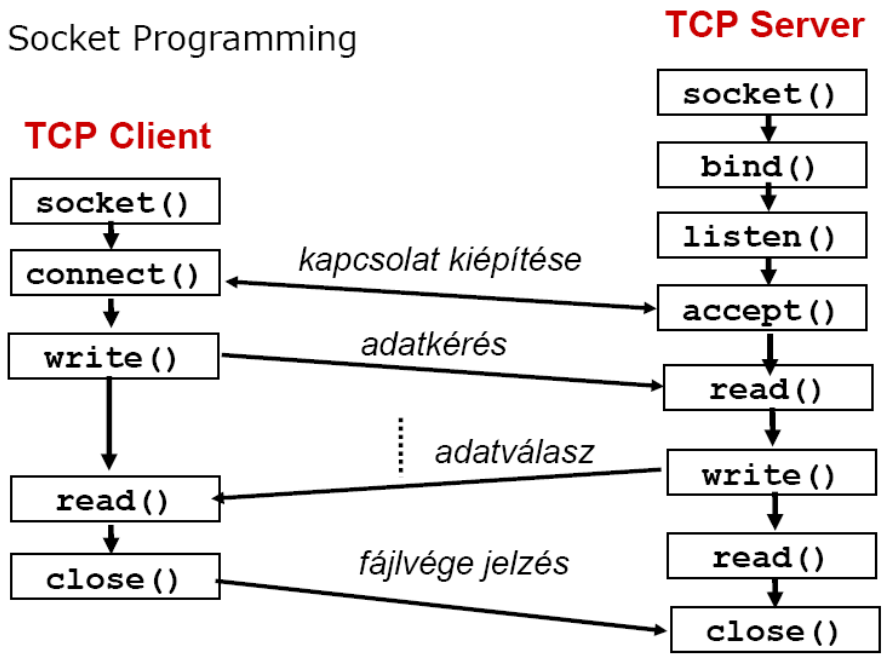
Alkalmazások környezete
- Alsóbb rétegek, mint szolgáltatások → op.renszer biztosítja, API-t szolgáltat, ez olyan, mint a SAP (Service Access Point)
- Ennek rendszerhívásait használva létrehozható a kívánt kommunikációs csatorna és annak az alkalmazás által használható végződése, a socket

Kliens-szerver architektúra
- Kliens: kapcsolatot kezdeményező ügyfél, a szolgáltatást meg kell címeznie (IP/DNS-név + portszám)
- Szerver: szolgáltatást nyújtó kiszolgáló – figyel

Porthozzárendelés
- Szerveren
    - Egy port csak egy szolgáltatáshoz tartozhat
    - Statikus

    - 1-65536 tartományból való, tipikusan 1-1023-ig
- Kliensen
    - Dinamikus kiosztás a még nem használtak közül
    - Általában 1024-65535 tartományból

TCP kommunikáció socket-hívásokkal



Telnet
- Nagyon régi
- Távoli parancssor: parancs elküldése, visszajelzés megjelenítése
- Ma is használják hálózati adminisztrációhoz
- Nem biztonságos – helyette: SSH (Secure Shell)

FTP – File Transfer Protocol
- Az egyik első fájlátviteli protokoll
- TCP 21-es port – ha a TCP 20-as portot használjuk adatcsatornaként, akkor ez csak vezérlés
- Parancsok: open, ls, put, get, delete, bye
- Adattípus figyelembevétele: ASCII, Binary

Levelezőrendszerek

Komponensek
- UA (User Agent) – levelező kliens
- MTA (Mail Transfer Agent) (SMTP Server)

Használt protokollok
- SMTP: levéltovábbítás
- POP3, IMAP4: levelek lekérdezése

Cél meghatározása: DNS segítségével (MX rekord)

Levelek lekérdezése – POP3 és IMAP4
- POP3 (Post Office Protocol v3)
    - Parancsorientált
    - TCP 110-es port

    - POP3S – POP3 TLS titkosítással, TCP 995
- IMAP4 (Internet Message Protocol v4)
    - Parancsorientált
    - TCP 143-as port
    - IMAP4S – IMAP4 TLS titkosítással, TCP 993
    - Okosabb a POP3-nál:
        - Könyvtárstruktúra támogatása
        - Keresés támogatása
        - Nem törli automatikusan a szerveren tárolt leveleket

Levelek továbbítása – SMTP (Simple Mail Transfer Protocol)

- Parancsorientált állapotkódokkal
    - Leggyakoribb parancsok
        - HELO: üdvözlés, ESMTP-nél EHLO
        - MAIL FROM:<mailcím> – feladó
        - RCPT TO:<mailcím> – címzett
        - DATA – adat jön
        - <CR><LF>.<CR><LF> – adat vége
        - QUIT – kapcsolat bontása
        - VRFY<mailcím> – létezik-e a cím
        - NOOP – kapcsolat ellenőrzése, fenntartása
- TCP 25
- STMP relay: nem közvetlen továbbítás, egy vagy több SMTP (relay) szerver közbeiktatásával
- SMTPS (SMTP Secure) – SMTP TLS csatornában, TCP 465
- Kiterjesztések: ESMTP (Extended SMTP) – kibővített parancskészlet és funkcionalitás

Webes rendszerek

HTTP – HyperText Transfer Protocol

- Parancsorientált állapotkódokkal
- Speciális fejlécek
- TCP 80
- Proxy
    - Kliens és DNS/webszerver között áll, a kliens nevében jár el
    - Főként a hatékony cache-elés érdekében
    - NAT helyett
    - Általában TCP 8080
- Gyakori HTTP parancsok
    - GET <URL> HTTP/1.1 – adott URL tartalmának lekérése
    - HEAD – mint a GET, de csak a metaadatokat kéri le
    - POST – kliens adatokat küld a szervernek
    - PUT – kb. mint a POST; fájlfeltöltéshez
    - DELETE – URL tartalmának törlése
- Gyakori HTTP állapotkódok
    - 200: OK
    - 401: Unauthorized
    - 403: Forbidden
    - 404: Not found
- Alkalmazási területek
    - Statikus és dinamikus HTML oldalak
    - Fájl le- és feltöltés; kiegészítés: WebDAV

        - HTTP parancs- és fejléc-bővítmény
        - FTP-szerű fájlkezelés
        - Hozzáféréskezelés (meg van nyitva írásra, ennek megújítása)
    - WebServices – PRC-szerű távoli eljáráshívás, SOAP (HTTP-n XML alapú kérés/válasz)
    - Protokollalagút
        - Más protokollokat HTTP-be csomagolva visznek át
        - Tűzfalak kijátszása (HTTP 80-as port mindenhol engedélyezett)
- Biztonság
    - Hitelesítés
        - Névtelen hozzáférés (Anonymous)
        - Alapvető (Basic) – Base64 kódolás
        - Digest – Challange-response alapú
        - Integrált – LANMan, NTLM, Kerberos
        - Tanúsítvány (Certificate)
    - HTTPS
        - HTTP SSL-en (PKI:RSA; DES, 3DES)
        - TCP 443

Hálózatbiztonság

A hálózatbiztonság építőelemei

- AAA (Authentication, Authorization, Accounting) – hitelesítés, jogosultság-hozzárendelés, számlázás
- Algoritmusok
    - Titkosítás
        - Szimmetrikus kulcsú: DES, 3DES, AES
        - Nyilvános kulcsú: RSA, elliptikus görbék
    - Hitelesítés
        - Kerberos
            - Adott tartományon belül működik
            - Időbélyeget használt
        - PKI (Public Key Infrasturcture)
            - Nyilvános kulcsú titkosírás felhasználásával
            - Digitálisan aláírt tanúsítványokat kiállító szervezetek (CA: Certificate Authority)
                - Ők adhatnak ki tanúsítványt
                - Felette levőkben megbízik
                - Legfelsőbb szintű CA-ban meg kell bízni
    - Kulcscsere
- Összetett megoldások
    - IPSec
        - Hitelesítés, kulcscsere- és titkosítás-egyeztető és –megvalósító keretrendszer
        - Típusai
            - AH (Authentication Header): digitálisan aláírt IP-csomag (fejlécestül)
            - ESP (Encapsulated Security Payload): titkosított tartalmú csomag
    - SSL – SSH, FTPS, HTTPS, SMTPS, POP3S, IMAP4S, …
    - TLS

A hálózatbiztonság eszközei

- Hálózati eszközök
    - FireWall (FW)
    - Behatolás-észlelő rendszer (IDS – Intrusion Detection System)
    - Behatolás-megelőző rendszer (IPS – Intrusion Prevention System)

- Biztonságosan tervezett, implementált, terjesztett,… alkalmazás
- Biztonságosan üzemeltetett alkalmazás (Social Engineering)

NAT – Network Address Translation

NAT
- Belső (magán) hálózat és az Internet összekötése
- Csak hálózati rétegbeli átalakítás – címcserével → transzparens

NAT router több IP-címmel (m = n)
- A router rendelkezik megfelelő számú nyilvános címmel, hogy minden belső cím kaphasson egyet
- Külső-belső címösszerendelés
    - Statikus
    - Dinamikus – biztonsági szempontból előnyös

NAT router kevés IP-címmel (m > n)
- A routernél nincs elég nyilvános cím minden belső címhez
- Külső-belső csomagösszerendelési stratégia kell
    - Statikus
        - Több, mint egy belső cím jut egy külsőre
        - Ilyenkor hogyan talál vissza a belső állomáshoz egy vissza-irányú csomag?
    - Dinamikus
        - Használhatjuk a következő szabad IP-címet
        - Na de nincs mindenkinek elég cím

NAT működése
- Nem csak az IP-címeket, hanem a portokat is módosítjuk: NAPT (Network Address Port Translation)
- Biztonsági rés
    - A bejegyzések dinamikusan adódnak hozzá és törlődnek
    - Ha létecik C_{Xy} porthoz bejegyzés, és erre a portra bárki csomagot küld, akkor ez az X állomás y portjára továbbítódik (port scan, DoS)
    - Ez a probléma NAT nélkül is fennáll
- Megoldás – a maszkolás (masquerade)
    - A NAT táblát bővíteni kell a külső fél IP és portcímével
    - A NAT router eldob minden más állomástól jövő csomagot
    - Egy egyszerű tűzfalmegoldás
- Virtual server
    - Belső szerver közzététele statikus NAT tábla bejegyzéssel
    - Úgy tűnik, mintha a szolgáltatás a NAT routeren lenne
    - Két típus
        - Minden IP-forgalom továbbításra kerül
        - Csak az adott portra érkező forgalom megy tovább
    - A belső kiszolgálókat védi más forgalomtól
- Erőforrások megosztása
    - Több mint 1 belső kiszolgáló
        - Terheléselosztás: a belső szerverek között
        - Magas rendelkezésreállás: egy szerver hibájakor a többi még működik
    - Több mint 1 külső interface
        - Terheléselosztás: a több kapcsolaton
        - Magas rendelkezésreállás: egy kapcsolat hibájakor a többi még működik
- Problémák a NAT-tal
    - Másodlagos kapcsolatok hibája, pl. FTP (TCP 20/21: vezérlő-/adatcsatorna)
    - IP-cím az alkalmazásrétegben – Routing protokollok, DNS, FTP, H.323, SIP, HTTP (abszolút URL)
    - Megoldás:
        - Az alkalmazás-rétegbeli IP-cím cseréje → ISO rétegmodell koncepció elromlik

        - Proxy a NAT routerben
    - Megoldás biztonságos csatornákkal
        - Nincs lehetőség a csatornák tartalmának, de általában még az IP-címek megváltoztatására sem ☹
            - IPSec (AH, ESP)
            - SSL/TLS (HTTPS, …)
        - Megoldás
            - NAT-T (Traversal)
                - Becsomagolás (fejrész-hozzáadás) és továbbítás az UDP 4500 porton
                - A másik félnek is támogatnia kell a NAT-T-t a kicsomagoláshoz és a becsomagolt válaszhoz
- Összefoglalás
    - Aggregálás egy multiplexelési szint elvesztésével (IP ↔ port)
    - Beavatkozás a végpont-végpont kapcsolatba
    - Használata körültekintést igényel
        - Nem NATolható protokollok
        - Másodlagos kapcsolatok
        - Korlátozott tűzfalfunkció

Tűzfalak

Szolgáltatások
- Szabály-alapú forgalomszűrés és továbbítás
- Működési típusok
    - Állapotalapú (stateful) vagy állapotmentes (stateless)
    - NAT vagy routing
    - Közzététel (publishing) támogatása
    - Protokoll- és alkalmazásszintű szűrés támogatása
- Egyéb funkciók
    - Proxy
        - Gyorsítótárral
        - HTTP és FTP forgalomra
    - VPN kiszolgáló
    - Monitorozás, naplózás, riasztás, jelentések