Hálózatok

**14. tétel - Ethernet szegmensek összekapcsolása az OSI 2. rétegben. Bridge protokollok. (statikus, dinamikus) Feszítőfás hidak. Távoli hidak. A switching technológia, az Ethernet switch-ek típusai.**

OSI Modell:

1. Fizikai réteg
2. Adatkapcsolati r.
3. Hálózati r.
4. Szállítási r.
5. Viszonylati r.
6. Megjelenési r.
7. Alkalmazási r.

**Ethernet szegmensek összekapcsolása az OSI 2. rétegben bridge eszközzel**

Routerhez hasonlóan hálózati szegmenseket köt össze. Különbség:

* Router az OSI modell 3. rétegét használja, tehát szoftveresen hozzárendelt IP címek alapján irányítja a kereteket
* Bridge az OSI modell 2. rétegét használja – MAC cím alapján irányítja a kereteket

Nem kell egyformának lennie a két fizikai csatornának (egyik pl. koax, másik pl üvegszál)

**Transzparens híd feladata és működése.**

A transzparens híd válogatás nélküli üzemmódban működik, azaz minden keretet elfogad, amely hozzá a csatlakoztatott hálózaton megjelenik.

* Amikor a hidakat először bekapcsolják a tábláik üresek, így az elárasztásos algoritmust használják:  
  *Minden bejövő keretet továbbadják az összes LAN-hoz kivéve, amelyiktől érkezett.*
* Idővel a hidak megtanulják, hogy a célállomások merre találhatóak. Miután a célállomás ismertté vált már nem képezik az elárasztásos tárgyát.
* Azaz az algoritmus, amit a transzparens hidak használnak, a hátrafelé tanulás (backward learning)

**Feszítőfás hidak**

* Kettő vagy több, egymással párhuzamosan bekötött hidat is használnak a megbízhatóság növelése érdekében. -> hurkok alakulhatnak ki
  + megoldás: a hidak kommunikálnak egymással, és lefedik a hálózat aktuális topológiáját egy fesztiőfával, amely eléri az összes LAN-t, így egy hurokmentes topológia jön létre.

**Távoli hidak**

A hidakat arra használják, hogy kettő vagy több, egymástól távoli LAN-t kössenek össze. (pl: városok között) Ezt úgy érthetjük el, ha mindegyik LAN-ra csatlakoztatunk egy hidat és ezeket összekötjük.

**A swtiching techonológia**

* A switch az Ethernet címek alapján képes eldönteni, hogy egy adatcsomagot mely portjára irányítsa, így az A-B és C-D jellegű párbeszédek nem ütköznek össze.
* Ehhez, olyan nagy sebességű belső csatorna szükséges, mely meghaladja az egyidőben folytatott párbeszédek összes sávszélességét.  
  Ma már akár 200 port is elhelyezhető, így a sávszélesség igény 100 Mbit/s is lehet.
* Előnye: a hálózat terhelhetősége igen magas lehet.

**Ethernet switch-ek típusai**

Az Ethernet switch hasonló a bridge-hez, csak több szegmens között képes kapcsolatot teremteni.

Kap egy keretet, feldolgozza a címinfókat és ez alapján dönt.

Fajtái:

* Store and forward swtich: Megvárja a teljes keret beérkezését és csak ezután továbbít. Relatív lassú, mert elleőriz
* Cut trough switch: Megvárja a célcímet, ezután küldi a keretet. Gyors, de nem ellenőrzi a hibát

Több switch is összekapcsolható hatékonyabb szegmentálás megvalósításához. (Koax kábellel)

**15. tétel - A hálózati réteg helye és legfontosabb feladatai. Datagram és virtuális áramkör alapú szolgálat. Alapvető forgalomirányítási algoritmusok: az elárasztás, a legrövidebb út algoritmus, a távolságvektor alapú forgalomirányítás.**

**A hálózati réteg helye és feladata**

OSI modell 3. rétege (adatkapcsolati és szállítási réteg között helyezkedik el)

Feladata: csomagok eljuttatása a forrástól a célig.

Ha a forrás és a cél eltérő típusú hálózatokban vannak, a réteg feladata a hálózatok közti különbségből adódó problémák megoldása.

**Datagram és virtuális áramkör alapú szolgálat**

Két eltérő hálózatszervezési módszer létezik:

1. Összeköttetés alapú – másnéven virutális áramkörnek (VÁ)
2. Összeköttetés-mentes – másnéven datagram

Virtuális áramkör

A virtuális áramkörök kialakításához minden csomópontnak fenn kell tartani egy olyan táblázatot, amely bejegyzései a rajta keresztül haladó éppen használt virtuális áramkörök jellemzőit (honnan jött—hova megy) tartalmazzák, és az azonosításukra egy sorszámot használnak.

Datagram

Minden egyes csomag, különböző útvonalakat követhet, mivel a csomagok útválasztása egymástól független. Ilyenkor a csomagoknak tartalmazniuk kell mind a forrás, mind a cél teljes címét. *IMP program*

Hátrány:

* Ahol tranzakciót dolgoznak fel, a kapcsolat felépítése és bontása sok idő.
* Egy IMP gép meghibásodásánál az összes VÁ-t újra kell építeni.

**Forgalomirányítási algoritmusok**

A forgalomirányítás (routing) feladata a csomagok hatékony (gyors) eljuttatása az egyik csomópontból a másikba.

* *Elárasztás*: A csomópontok, mikor egy csomagot továbbítanak, a bejövő csomagot **minden vonalra kiküldik**, kivéve ahonnan érkezett. A lépések száma korlátozva van
  + Előny: Egy példányban mindenképp a legrövidebb úton ér célba, megbízható.
  + Hátrány: Terheli a rendszert (redundancia)
* *Legrövidebb út algoritmus*: Két pont között **meg kell találni a legoptimálisabb útvonalat**. Az optimális útvonal nem feltétlenül jelenti a fizikailag legrövidebb útvonalat, mivel számos egyéb tényező is befolyásolhatja az optimális választást: lehet például mértéknek a **csomópontátlépések** számát tekinteni, lehet azt az **időt**, hogy mennyi idő alatt jut el a csomag, vagy a **vonalhasználat költségeit**. A feladat a gráf két csomópontja közötti olyan élekből álló útvonal meghatározása (shortest path), amelyre az érintett élek mértékeinek összege minimális. Az ismertetett módszer Dijsktrá-tól (1959) származik
* *Távolságvektor alapú algoritmus*: A távolság alapú algoritmus a hálózatban minden összeköttetéshez **egy irányt** (vektort) és egy **távolságot** határoz meg. Minden router tartalmaz egy **bejegyzést**. Ez a bejegyzés két részből áll: az adott célhoz előnyben részesített kimeneti vonalból és a becsült időből vagy távolságból.

**16. tétel - Az IP protokoll helye és feladatai. Az IPv4 és IPv6 csomag fontosabb fejrész információi. Az IPv4 címzési rendszere, az IPv4 cím szerkezete. A hálózat címe és az üzenetszórási (broadcast) cím. Az IP címek osztályozása. Az alhálózati maszk szerepe: a hálózat felosztása alhálózatokra. Az alapértelmezett átjáró. Példa több alhálózatot (és routert) tartalmazó IP hálózatra.**

**IP protokoll helye és feladatai**

* Az internetprotokoll az internet hálózat egyik alapvető szabványa (avagy protokollja). Ezen protokoll segítségével kommunikálnak egymással az internetre kötött csomópontok (számítógépek, hálózati eszközök, web kamerák stb.).
* Feladata: A protokoll meghatározza az egymásnak küldhető üzenetek felépítését, sorrendjét stb.
* Helye: Az IP a klasszikus OSI besorolás alapján (3.) a hálózati rétegben helyezkedik el. *Csomagkapcsolt hálózatot valósít meg, azaz nem építi fel a kapcsolatot a forrás és a cél között, hanem minden egyes csomagot külön irányít (routol).*

**Az IPv4 csomag fontosabb fejrész információ**

A csomag 4 bájtos duplaszavakból áll.

A képen szöveg, képernyőkép, Betűtípus, sor látható

Automatikusan generált leírás

* A **verzió** mező a protokoll verzióját azonosítja. Jelenlegi értéke: 4. Az új IPV6-os protokoll esetén ez az érték: 6
* Az **IHL** (=Ip Header Length) adja a fejrész hosszát 32 bites egységekben (20 bájt+opció rész). Minimális értéke: 5
* A **szolgálat típus** mező teszi lehetővé a hoszt számára, hogy kijelölje az alhálózattól kívánt szolgálat típusát.
* **A teljes hosszúság** mező a teljes datagram hosszát tartalmazza (fejrész+adat). A maximális hosszúság: 65536 bájt
* Az **azonosítás** mező alapján állapítja meg a célhoszt, hogy egy újonnan érkezett csomag melyik datagrammhoz tartozik.
* Az **MF** bit neve More Fragments (több darab) rövidítése. A széttördelt datagram darabokat MF=1 értékkel jelzi, kivéve az utolsót, ahol MF=0. Ehhez kapcsolódik a datagram darabeltolás mező, ami azt jelöli ki, hogy az adott darab hol található a datagramban. Minden datagramdarab hosszúságának (kivéve az utolsót), 8 bájt egész számú többszörösének kell lennie
* Az **élettartam**, más néven TTL (Time To Live) mező lényegében egy 8 bites számláló, amely a csomagok élettartamát tartalmazza másodpercben. Amikor az értéke 0-ra változik, akkor az adott csomag megsemmisül. Így a maximális élettartam 255 másodperc lehet.
* A **protokoll** mező kijelöli, hogy a datagram a különféle szállítási folyamatok közül melyikhez tartozik. A TCP a leggyakoribb választás, de léteznek egyebek is (UDP, ICMP,…).
* A **fejrész ellenőrző összege** csak a fejrész ellenőrzésére szolgál. Egy ilyen ellenőrzőösszeg azért hasznos, mert a fejrész a darabolások miatt változhat az átjárókban.
* A **forráscím** és **célcím** mezők 32 biten a hoszt címet tartalmazzák.
* Az **opciók** mező rugalmasan alkalmazható biztonsági, forrás általi forgalomirányítási, hibajelentési, hibakeresési, időpont megjelölési és egyéb információs célokra.

**Az IPv4 címzési rendszere, az IPv4 cím szerkezete**

Mivel az internet lényegében **hálózatok összekapcsolása**, a címzési rendszer kialakításánál ezt figyelembe vették: **a címzés hierarchikus**, azaz vannak hálózatok és ezen belül gépek. Így célszerű a címet **két részre** bontani: egy **hálózatot azonosító** (netid), és egy, az adott hálózaton belül **gépet azonosító** (hostid) címre. A hálózatok közötti kapcsolatot az útválasztók (router) biztosítják.

A 32 bit-es IP címeket pontokkal elválasztott **decimális egész**ként adjuk meg: pl. 192.190.173.37

Magánhálózati címtartományok:

* A – 10.x.x.x
* B – 172.12.x.x – 172.31.x.x
* C – 192.168.x.x

**A hálózat címe és az üzenetszórási (broadcast) cím**

* Ezzel a címmel az összes helyi gépet megcímezhetjük.
* A broadcast címnek foglalt az adott **networkon megcímezhető legnagyobb hostcím**. Tehát a címben a host részen csupa 1-es szerepel. Így például a 192.168.2.0/255.255.255.0 tartományban a broadcast számára foglalt a 192.168.2.255 cím.

**Az IP címek osztályozása**

****

**Az alhálózati maszk szerepe:** a hálózat felosztása alhálózatokra

* Az alhálózati maszk segítségével állapítható meg, hogy az IP cím mely része **azonosítja** **a** **hálózatot** és mely része **az** **interfészt** (gazdagépet)
* Az IP-címen belül a **hálózati azonosítót** és az **állomásazonosítót** az alhálózati maszk **választja szét**
* Az alhálózati maszkok **32 bites számok**, amelyekben az IPcímen belül egymás utáni **egyes (1) bitek** azonosítják a hálózatazonosító, és **egymás utáni nulla (0) bitek** az állomásazonosító részt.

**Az alapértelmezett átjáró**

Biztosítják az alapértelmezett utat a TCP/IP-állomások számára, amikor azok távoli hálózatokban levő más állomásokkal kívánnak kommunikálni.

**17. tétel - Autonóm hálózatok, a belső és külső átjáró protokoll (IGP/EGP) fogalma. Forgalomirányítás az IP hálózaton: a RIP és az OSPF protokoll. A DHCP protokoll. AZ ARP és az RARP címfeloldási protokoll.**

**Autonóm hálózatok**

Azonos routing politikát folytató hálózatok csoportja.

* + Azonos dinamikus routing protokollt használnak
  + Routing információt a routerek csak csoporton belüli routertől fogadnak el.

**Autonóm rendszerek jelölése**: ASxx xx = szám

**Belső és külső átjáró protokoll (IGP/EGP)**

*A routing protokollnak két fő típusa van:*

* *Interior Gateway Protocol*(IGP): Autonóm rendszeren belül működik. Tartalmazza a Routing Information Protocolt-t (RIP) és a Interior Gateway Routing Protocol-t (IGRP).
* *Exterior Gateway Protocol*(EGP):Autonóm rendszerek között működik. Tartalmazza a Border Gateway Protocollt (BGP)
  + a BGP nem igényel periodikus frissítést, incremental update

**A RIP és az OSPF protokoll**

**RIP (Routing Information Protokoll):** minden router broadcast **üzeneteket** küld ki a hozzá kapcsolódó hálózatnak, hogy rajta keresztül **milyen hálózatok érhetőek** el és **milyen költséggel**

* Mindig a kisebb költségű hirdetést építik be a routerek a routing táblába
* A RIP 30 másodpercenként küldi a broadcast útvonal-információit

**OSPF (Open Shortest Path First):** információk alapján építik fel a teljes hálózat térképeit, s ez alapján generálják a routing táblát. Elvei:

* *Publikus protokoll* (O – Open Shortest…)
* *Mindenféle távmértéket támogat* (fizikai távolság, késleltetés, stb)
* *Terheléskiegyenlítés*: Nem csak a legjobb útvonalon küldjön, hanem a második, harmadikon is.
* *Hierarchikus rendszerek támogatása*. Az egyes routereknek nem kell az egész hálózat topológiáját ismernie.

**A DHCP protokoll**

A DHCP-vel **dinamikusan oszthatóak ki IP-címek**, tehát a hálózatról lecsatlakozó számítógépek IP-címeit megkapják a hálózatra felcsatlakozó számítógépek, ezért hatékonyabban használhatóak ki a szűkebb címtartományok

* TCP/IP hálózatra csatlakozó számítógépek automatikusan megkapják a hálózat használatához szükséges beállításoka

*3 féle IP-kiosztás lehetséges DHCP-vel*

* Kézi (MAC cím alapján)
* Automatikus (DHCP-vel kiadható IP- tartomány megadásával)
* Dinamikus (IP tartomány megadásával, IP címek „újrahasznosításával”)

**Az ARP és az RARP címfeloldási protokoll**

Az ARP a TCP/IP alapú szoftverek által használt **IP címekhez MAC-címeket rendel**

Az ARP az azonos fizikai hálózaton elhelyezkedő állomások számára a következő **protokollszolgáltatásokat** biztosítja:

* Az eszközhozzáférés-vezérlő cím meghatározásához **kérdést tesz fel**: "Mi az eszközhozzáférés-vezérlő címe annak az eszköznek, amely a mellékelt IP-címmel van beállítva?"
* a válasz küldője feljegyzi a másik IP és MAC címét egy helyi táblázatba, melynek neve **ARP gyorsítótár**

**Reverse Address Resolution Protocol (RARP):** feladata a saját IP cím lekérdezése (pl. boot) a saját MAC cím alapján. Az ARP-vel **ellentétes folyamatot végez**, vagyis a kapcsolati címeket, mint pl. egy Ethernet címet IP-címmé alakít át

**18. tétel - A szállítási réteg helye és feladatai. A TCP protokoll működése: a port fogalma, a TCP fejléc, összeköttetés létesítése és bontása, átviteli politika, torlódáskezelés. Az UDP protokoll.**

**A szállítási réteg helye és feladatai**

*Helye*: Az OSI modell alulról 4. rétege, az alsó három réteg logikai folytatásának tekinthető.

*Feladata*: A hálózat két tetszőleges számítógépe közötti **kommunikációs kapcsolat** biztosítása. A hálózatba kapcsolt számítógépek **egyedi azonosítójának** a biztosítása, valamint a **hálózati csomagok útvonalának a kijelölése** két tetszőleges számítógép között.

**TCP (Transmission Controll Protokoll) protokoll működése**

* összeköttetés alapú megbízható
* változtatható ablakméret és timer futási idő, terheléstől függően
* küldendő csomagokat sorszámozza
* kezeli a portokat

1. A TCP fogadja a tetszőleges hosszúságú üzeneteket a felhasználói folyamattól és azokat maximum 64 kbájtos darabokra vágja szét.
2. Ezeket datagramokként küldi el.
3. Időzítéseket kezel
4. A darabokat helyes sorrendbe rakja össze őket eredeti üzenetté

**Port fogalma:** A port hálózatra kötött számítógépek egymással való kommunikációjának csatlakozási pontja. Különböző szolgáltatásait a gépen definiált különböző portokra (kapuk) csatlakozva érhetjük el

**A képen szöveg, képernyőkép, Betűtípus, sor látható

Automatikusan generált leírás**

A **TCP fejléc** 24 bájt hosszú (6 db 4 bájt hosszú szó). A legfontosabb információk a **feladó** és a **címzett** **port száma**, és a **datagram sorszáma**. Az előbbi dönti el, hogy melyik program küldte az üzenetet és melyik programnak, az utóbbi, pedig a datagram sorrendiségét határozza meg összerakáskor.

**TCP összeköttetés létesítése**

Az összeköttetések létesítésére **a három utas kézfogás** technikát alkalmazzák a TCP-ben.

1. A kliens kezdeményezi a **kapcsolat kiépítését**.
2. A szerver a **TCP fejrészből** (jelzőbitekből) látja, hogy új kapcsolat kiépítése indult. A szerv**er jóváhagyó** **válaszüzenetet küld**.
3. Miután a **kliens** megkapja a választ, **egy jóváhagyást küld** a szerver felé.
4. Miután a szerver megkapja a kliens válaszát, **a kapcsolat kiépült**.

*Ezután megindul az applikációs rétegben használt protokollnak megfelelő adatátviteli kommunikáció.*

**TCP összeköttetés bontása**

Bár a TCP-összeköttetések duplexek, hogy megérthessük az összeköttetések bontásának módját, legjobb **két szimplex összeköttetésnek** tekinteni azokat. Amikor **mindkét irányt lezárták**, az összeköttetés befejeződött.

**Átviteli politika**

Az áramlásvezérlés célja, hogy megakadályozza az egyik oldal túltöltését, ha az nem képes lépést tartani az adatok fogadásával. Ezt a mechanizmust a **vevőablak (receiver window)** szabályozza, amely a vevő által küldött visszajelzésen alapul.

**Torlódásvezérlés**

A torlódáskezelés lényege, hogy ne legyenek a hálózat egyes részei túlterheltek. A TCP az adatok biztonságos továbbítása érdekében és az elárasztás vezérlésére az ablakozás technikáját alkalmazza. Több ablakméret is egyszerre definiálva van.

*receive window:* Megmondja, hogy a **vevőnek mekkora szabad buffer-területe van** az adatok fogadására. Ezt minden TCP fejlécben elküldi a Window mezőben.

*congestion window:* elárasztás lekezelése, ez egy számított ablakméret.

**UDP protokoll (Used Datagram Protokoll)**

Az internet egyik alapprotokollja. Feladata **datagram alapú szolgáltatás biztosítása**, azaz rövid, gyors üzenetek küldése. Jellemzően akkor használják, amikor a **gyorsaság fontosabb a megbízhatóságnál**. pl. DNS, hálózati játékok

* összeköttetés mentes protokoll
* nincs bonyolult adminisztráció
* kezeli a porotokat
* tartalmaz CRC-t

**19. tétel - A DNS (körzeti névkezelő rendszer) leírása. A doménnév szerverek működése, kapcsolat a doménnév szerverek között. Doménneves azonosítóhoz tartozó IP cím megállapításának menete. Hálózati védelem lehetséges esetei tűzfal, proxy használatával.**

**DNS**

A Domain név rendszer (Domain Name System vagy DNS) egy hierarchikus kiosztott név rendszer számítógépeknek, *szolgáltatásoknak vagy bármilyen erőforrásnak, ami az internethez vagy magánhálózathoz csatlakozik.*

Feladata: A domain nevek lefordítása a hozzájuk tartozó IP címre.

**A domain név szerverek működése**

**A protokoll kérdés-válasz alapú:** a kliensek kérdeznek, a szerverek válaszolnak. A nevek feloldását egy elosztott számítógépes rendszer biztosítja, amely független, együttműködő név szerverekből áll.

* *autoritatív névszerver:* **Egy adott zóna felelőse**. Az adott zónával kapcsolatban tárolt adatai emiatt tehát „**biztonságosnak**” tekinthetők.
* *nem autoritatív névszerver:* a zónákra vonatkozó adatait másod- vagy harmadkézből a (forrásból) kapja; így az ebben tárolt információt „**nem** **biztonságosnak**” tekintjük.

**Domain neves azonosítóhoz tartozó IP cím megállapításának menete**

A host resolver-e először megnézi a saját cache-ét, és csak akkor fordul a névszerverhez, ha nem találja a keresett nevet a cacheben.

**Hálózati védelem**

A **tűzfal** (angolul firewall) célja, hogy a hálózaton keresztül egy adott számítógépbe ne történhessen illetéktelen behatolás. A tűzfalak általában folyamatosan jegyzik a forgalom bizonyos adatait, továbbá riasztásokat is adhatnak.

* olyan hálózati biztonsági rendszer, amely felügyeli és szabályozza a bejövő és kimenő hálózati forgalmat
* akadályt képez egy megbízható belső hálózat és egy bizonytalan külső hálózat között

A tűzfal **proxy-t** használ. Ez egy közvetítő eszköz, amely a kliens és az internet közötti kapcsolatot kezeli. Szerepe, hogy az kliens (például egy webböngésző) kéréseit továbbítsa a megfelelő szerver felé, majd a válaszokat visszaküldje az kliensnek.

**20. tétel - Vezeték nélküli átviteli szabványok. Vezeték nélküli hálózatok osztályozása. Wlan hálózatok szabványai. Ad-Hoc és infrastruktúrált hálózatok. Vezeték nélküli hálózatok adatvédelmi lehetőségei.**

**WLAN**

A vezeték nélküli LAN-okat WLAN-nak nevezzük.

* Sebességük 1-540 Mbit/s.
* A WLAN-ok rádió frekvenciát használnak
* megfelel az IEEE 802.11-es szabványoknak

**Előnyei**

* Hordozhatóság
* Skálázhatóság
* Rugalmasság
* Költség hatékony
* Rövid telepítési idő

**Hátrányok**

* Interferencia: a érzékeny a más elektromágneses erőteret keltő eszközöktől
* Hálózati és adatvédelem
* Technológia: nem biztosítja a vezetékes hálózatok által nyújtott sebességet és megbízhatóságot

**2 fajta WLAN forma ad-hoc és infrastrukturális mód**

* **ad-hoc:** 2 vagy több vezeték nélküli hálózatot kapcsolunk össze
* **infra:** önálló eszköz alkalmazása szükséges a vezeték nélküli kommunikáció irányításához

**A képen szöveg, Betűtípus, képernyőkép, szám látható

Automatikusan generált leírás**

**WLAN-ok támadási lehetőségei**

* Egyik egyszerű módszer a vezeték nélküli hálózatba való bejutáshoz, ha tudjuk a hálózat nevét és az SSID-t.
* Alapértelmezett SSID és jelszó elősegíti a támadót.
* Vannak olyan eszközök, amelyek képesek elfogni a vezeték nélküli jeleket és a titkosítatlanul küldött adatokat.

**Védelmek**: Egyedi SSID, egyedi rejtett SSID, MAC cím szűrési táblák használata.

**21. tétel - A számítógép-hálózat fogalma, hálózatok csoportosítása, jellemző alkalmazási területek. A kommunikációs hálózat fogalma és típusai: üzenetszórásos, pontpont közötti és csatornákból felépülő hálózat. Az OSI modell rétegei és az egyes rétegek feladatai. A rétegközi interfész és a protokoll fogalma.**

**Számítógép-hálózat fogalma**

A számítógép hálózatok alatt az egymással kapcsolatban lévő önálló, autonóm számítógépek rendszerét értjük.

**Hálózatok csoportosítása**

*A hálózatok kiterjedés szerinti csoportosítása*

***Lokális hálózatok*** *(LAN):* kis távolságon belül eszközök egymás közötti kommunikációja

***Nagyvárosi*** *(MAN):* nagyvárosi hálózat intézmények közötti kommunikáció. kb. 50 km

***Távolsági*** *(WAN):* földrajzilag távoli felhasználókat köti össze. pl. Internet

*Topológia alapján történő csoportosítás*

***BUS****:* a gépek közös átviteli közegre csatlakoznak

***RING****:* gyűrűre fel vannak fűzve

***TREE****:* Két gép között csak egy útvonal van

***STAR****:* minden gép csak központi géppel van összekötve

*Átviteli sebesség alapján történő csoportosítás*

***Lassú (30 kbit/s):*** Általában telefonvonalakat használnak az adatátvitelre

***Közepes (1-20 Mbit/s):*** A LAN-ok többsége ebbe a kategóriába sorolható

***Nagy sebességű (50 Mbit/s fölött):*** Manapság a 100 Mbit/s-os lokális hálózatok terjednek el

*Kommunikáció iránya szerinti csoportosítás*

***Simplex:*** Az egyik állomás csak az adó a másik csak a vevő

***Fél duplex:*** Mindkét irányban megengedett az adatátvitel, de egy időben csak az egyik irányban élhet

***Duplex:*** Mindkét állomás egyszerre lehet adó és vevő is

**Kommunikációs hálózat fogalma és típusai**

Fogalma: Azokat a számítógépeket, amelyeket egy számítógépes rendszerben összekötünk host-oknak nevezzük. Ezeket a gépeket kommunikációs alhálózatok kötik össze, amelyek feladata a host-ok közötti kommunikáció megvalósítása.

Típusai:

**Üzenetszórásos hálózat**: **Egy kommunikációs csatorna** van, és ezen az egy csatornán osztozik az összes hálózatba kapcsolt számítógép

**Pont-pont közötti csatornákból felépülő hálózat**: **Két kommunikációs végpontot kötnek össze** és a csomagok ezen a kábelen keresztül haladnak. Amikor egy vevő megkapja a csomagot és az nem neki szól, akkor azt továbbadja egy következő pont-pont összeköttetésen keresztül.

**Az OSI modell rétegei és az egyes rétegek feladatai**

Nemzetközi Szabványügyi Szervezet (International Standard Organization) kidolgozott egy olyan modell-ajánlást, amelyet ma már minden hálózati rendszer tervezésekor követnek. 7 réteg közül

1. **Fizikai** réteg (physical layer): Valójában ezen a rétegen zajlik a tényleges **fizikai kommunikáció.**
2. **Adatkapcsolati** réteg (data link layer): feladata **adatok** megbízható **továbbítása** az adó és fogadó között. Az adatokat adatkeretekké tördeli, ellátja kiegészítő cím, egyéb és ellenőrző információval, ezeket sorrendhelyesen továbbítja, majd a vevő által visszaküldött nyugtakereteket véve ezeket feldolgozza.
3. **Hálózati** réteg (network layer): lényegében a kommunikációs alhálózatok működését vezérli. Nagyobb hálózatok esetén a keretek vevőtől a célba juttatása elvileg **több útvonal**on is lehetséges, feladata bizonyos szempontból az **optimális útvonalnak a kiválasztása**. Ez a tevékenység az útvonalválasztás (routing), és több megoldása lehetséges
4. **Szállítási** réteg (transport layer): Feladata a host-ok közötti átvitel megvalósítása. A kapott adatokat szükség esetén kisebb darabokra vágja, átadja a hálózati rétegnek.
5. **Együttműködési** réteg (session layer): Más néven: viszony réteg. A különböző gépek felhasználói viszonyt létesítenek egymással, például bejelentkezés egy távoli operációs rendszerbe, állománytovábbítás két gép között.
6. **Megjelenítési** réteg (presentation layer): a feladata az **adatok egységes kezelése**. A legtöbb alkalmazói program nem csupán egy bitfolyamot, hanem neveket, dátumokat, szövegeket küld. Ezeket általában adatstruktúrákban ábrázolják. A **kódolás sem minden esetben egységes**, pl. a karakterek kódolására az ASCII mellett az EBCDIC kód is használt. Ezért egységes, absztrakt adatstruktúrákat kell kialakítani, amelyek kezelését a megjelenítési réteg végzi. További, e réteg által kezelt vonatkozások: az **adattömörítés**, illetve az **átvitt adatok titkosítása**.
7. **Alkalmazási** réteg (application layer): Mivel ez kapcsolódik legszorosabban a felhasználóhoz, itt kell a hálózati felhasználói kapcsolatok megoldásait megvalósítani. Megvalósítandó feladat a fájlok átvitelekor az **eltérő névkonvenciók kezelése**, az **elektronikus levelezés**, és **mindazon feladat, amit internet szolgáltatásként ismerünk**.

**A rétegközi interfész és a protokoll fogalma**

**A rétegközi interfész:** Különböző hálózati rétegek közötti kapcsolat és kommunikáció szabályozása, amely biztosítja a rétegek közötti szolgáltatások átvitelét.

A **protokollok** a hálózati kommunikáció szabályait és eljárásait határozzák meg. Ezek lehetővé teszik, hogy különböző eszközök és alkalmazások kommunikáljanak egymással