Z1 *Számítógép hálózatok I. (IN-401)*

Z1/1 A számítógép hálózatok kialakulásának okai, hálózatok csoportosítása (LAN-MAN-WAN). A számítógép hálózatokkal kapcsolatos alapfogalmak (vonalkapcsolás, üzenetkapcsolás, csomagkapcsolás), topológiák. Hálózati szoftver alapfogalmak (réteg, protokoll, interfész, hálózati architektúra).

A számítógép hálózatok kialakulásának okai:

- **Erőforrás-megosztás:**

  Célja az, hogy a hálózatban levő programok, adatok és eszközök- az erőforrások és a felhasználók fizikai helyétől függetlenül - bárki számára elérhetők legyenek.

- **Nagyobb megbízhatóság:**

  Minden adat két vagy több gépen is megtalálható, így ha valamelyik adathoz nem férünk hozzá az egyik gépen (pl. hardverhiba következtében), akkor ugyanannak egy másolatát elérhetjük egy másik gépen. Több CPU használata miatt nő a megbízhatóság, mert ha az egyik leáll, akkor a teljesítmény csökken, de a rendszer üzemképes marad.

- **Takarékosság:**

  A kis számítógépek sokkal jobb ár/teljesítmény aránnyal rendelkeznek, mint nagyobbak. Az erőforrásgépek kb. tízszer gyorsabbak, mint az egyetlen chipből álló mikroprocesszorok, ugyanakkor kb. ezerszeres az áruk. Ez az aránytalanság arra késztette a rendszertervezőket, hogy olyan rendszereket építsenek ki, amelyekben minden felhasználónak saját személyi számítógépe van, és az adatokat egy vagy több, közösen használt szerveren tárolják.

- **Skálázhatóság:**

  Annak a biztosítása, hogy a rendszer teljesítményét a terhelés növekedésével oly módon lehessen fokozatosan növelni, hogy újabb processzorokat adunk hozzá.

- **Hatékony kommunikációs eszköz:**

  Pl.: az alkalmazottak könnyen megírhassanak egy közös cikket (on-line módosításokkal).

- **Programozási ok:**

  Szükséges a közös adatokkal való dolgozás.

Lokális hálózat (Local Area Network, LAN):

Olyan magánhálózat, amely egyetlen épületen belül vagy egy legfeljebb néhányszor tíz kilométer kiterjedésű területen található. A hagyományos LAN-ok 10 Mb/s és 100 Mb/s közötti sebességgel működnek, kicsi a késleltetésük és nagyon keveset hibáznak. Az újabb LAN-ok még nagyobb, akár több száz Mb/s-os sebességgel működnek.

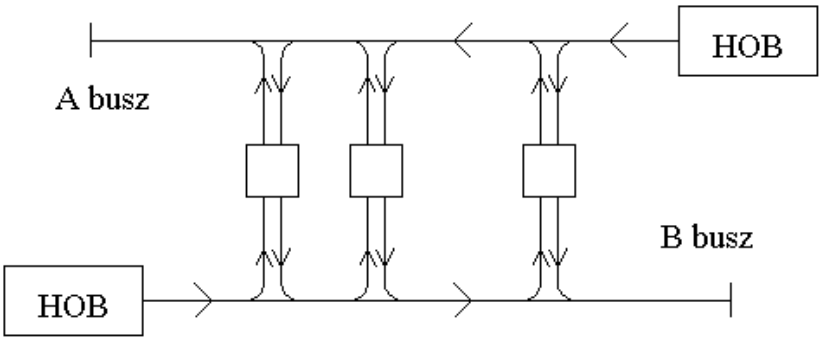
- **Előnyök:**
  - Erőforrások megosztása: nyomtatók, háttértárak
  - Teljesítmény egyenletesebb megosztása: párhuzamosíthatóság
  - Nagyobb megbízhatóság: pl. DNS
  - Költségmegtakarítás
  - Központosított adatbázisok
  - Gyorsuló kommunikáció
- **Hátrány:**
  - Új biztonsági kérdések (adatbiztonság)

Nagyvárosi hálózat (Metropolitan Area Network, MAN)

Lényegében a Lokális hálózat nagyobb változata, és általában hasonló technológiára épül. Összeköthet egymáshoz közel fekvő vállalati irodákat vagy akár egy egész várost. Lehet magánhálózat vagy nyilvános hálózat.

A MAN-okat azért soroljuk mégis külön kategóriába, mert kidolgoztak számukra egy szabványt. Ez a hálózat a DQDB (Distributed Queue Dual Bus), IEEE 802.6. A DQDB két egyirányú sínből (kábelből) áll, ezekhez csatlakozik valamennyi számítógép, ahogy mindez az ábrán is látható. Mindkét sín rendelkezik egy főállomással (head-of-

bus), amely az átviteli tevékenységeket kezdeményezi. A küldőtől jobbra eső gépeknek szánt üzenetek a felső sínt, az attól balra levő gépeknek szánt üzenetek pedig az alsó sínt használják.

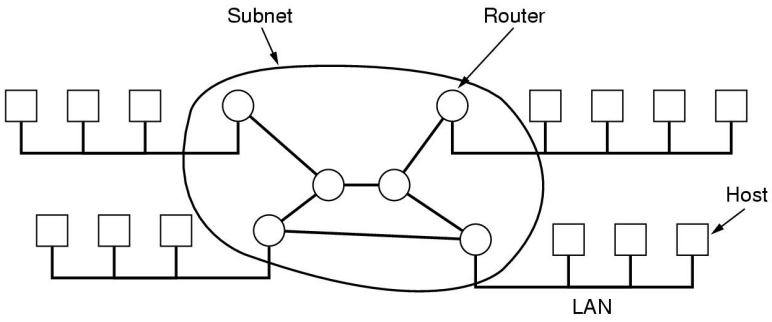


A DQDB nagyvárosi hálózat architektúrája

A MAN-ok esetében kulcsfontosságú az, hogy legyen egy olyan adatszóró közeg (a 802.6 esetén ez két kábelt jelent), amelyhez az összes gép csatlakozni tud. Ez ugyanis nagymértékben leegyszerűsíti a tervezést a többi hálózathoz képest.

Nagy kiterjedésű hálózat (Wide Area Network, WAN)

Nagy földrajzi kiterjedésű területeket, általában egy országot vagy egy földrészt fed le. Olyan gépeket foglal magába, amelyeket felhasználói programok futtatására terveztek. Ezeket a gépeket a hagyományoknak megfelelően hosztoknak, végrendszereknek nevezzük. A hosztokat egy alhálózat kapcsolja össze. Az alhálózat feladata az, hogy továbbítsa az üzeneteket a hosztok között.



A hosztok és az alhálózat közötti kapcsolat

A legtöbb nagy kiterjedésű hálózatban az alhálózat két különböző komponensből áll: az átviteli vonalakból és a kapcsolóelemekből. Az átviteli vonalak (más néven áramkörök, csatornák) a biteket szállítják a számítógépek között.

A kapcsolóelemek olyan speciális számítógépek, amelyeket két vagy több átviteli vonal összekapcsolására használunk. Amikor adatok érkeznek az egyik bejövő vonalon, a kapcsolóelemnek ki kell választania egy kimenő vonalat, hogy azokat továbbítsa.

Számítógép hálózatokkal kapcsolatos alapfogalmak (vonalkapcsolás, üzenetkapcsolás, csomagkapcsolás)

Vonalkapcsolt:

Elindítok egy jelet, eldönti, hogy merre menjen - idő telik el -, elmegy az A pontba, mire elér szintén idő telik el. Ha elérünk a célhoz, már nincs múló idő, mert megvan az útvonal, nyugtázó jelet küld vissza - ehhez is idő kell -. Telefonhálózat analógiája. Nem jó, mert a teljes útvonalat leköti tartósan. Változatos feladatokra nem alkalmas.

Az adó és a vevő közti összeköttetés megteremtésére ki kell alakítani azt az útvonalat, amelyeknek részei a kapcsolóközpontokon keresztül vannak összekötve. Első lépésben fizikai kapcsolat létesül adó és vevő között, ami az összeköttetés idejére áll fenn. Az összeköttetésen keresztül megvalósul az adatátvitel, majd annak befejezésével a kapcsolat leomlik. Az információátvitelt meg kell, hogy előzze a híváskérés hatására létrejövő összeköttetés. Előnye a tényleges fizikai összeköttetés létrehozása, ezután a két állomás úgy képes kommunikálni, mintha pont-pont összeköttetés valósult volna meg. Hátránya a kapcsolat létrehozásához szükséges sokszor jelentős időtartam, és az, hogy ilyenkor a csatorna mégis kisajátítja a vonalat. Ha a csatorna nem teljes kapacitással üzemel, akkor ez a vonal kihasználtságát rontja.

Üzenetkapcsolt:

A teljes információ megy bizonyos útvonalon csomóponttól csomópontig. Nem elég csak a hasznos információt elküldeni, hozzá kell írni a címinformációt is. Tartósan csak az útvonal egy része van lekötve. Szomszédos csomópontok közti átvitel. Ilyenkor nincs előre kiépített út az adó és a vevő között. Az adó az elküldendő adatblokkját elküldi az első IMP-nek (interfész üzenetfeldolgozó), az továbbküldi a következőnek egészen a vevő host-hoz kapcsolódó IMP-hez. Az ilyen hálózatok a *tárol és továbbít* (Store and Forward) hálózatok pl.: távíró (lyukszalag). Az üzenetkapcsolás esetén nincs az adatblokk méretére korlátozás, ami nagy kapacitású IMP-t igényel. A másik hátránya, hogy egy nagy üzenet, akár percekre lefoglalhatja a közreműködő IMP-ket és a köztük lévő átviteli csatornát.

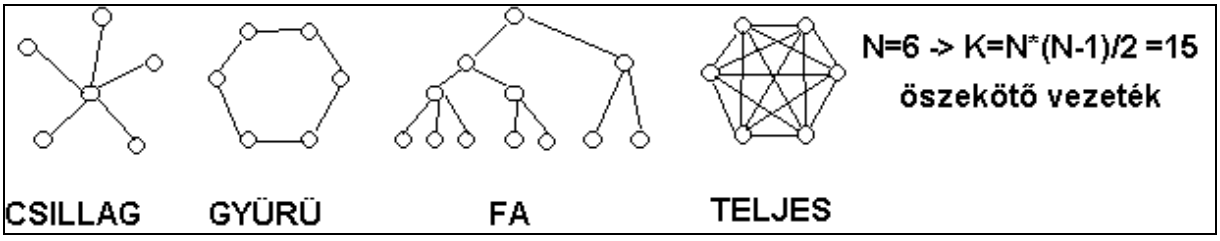
Csomagkapcsolt:

A nagy információt csomagokra vágják és így küldik el. Az első csomagot elindítják, ez valamennyi idő alatt eljut az első csomópontba. A csomópontban keletkezik némi késleltetési idő - merre menjen -, ezután feladja a következő csomóponthoz és ugyanebben az időben indul a következő csomag az első ponttól. Az üzenet csomagokra bontása, címzés csomópontonként. Csomagok időben átlapolt továbbítása. Gyorsabb, mint az üzenetkapcsolásos, nem foglalja le az útvonalat tartósan. Ha a csomagok útvonala azonos: nincs sorrendi probléma. Ha a csomagok útvonala különböző: a célnál van a sorba rendezés. Az átviendő adatblokk méretét korlátozzuk és csomagblokká bontjuk. A csomagkapcsoló hálózatok hatékonyan alkalmazhatók interaktív forgalom (ember - gép kapcsolat) kezelésére is, mivel biztosítják, hogy bármelyik felhasználó csupán néhány ezredmásodpercre sajátíthat ki egy vonalalt. A csomagkapcsolás nagyon hatékonyan képes a vonalak kihasználására, mivel adott két pont között az összeköttetést több irányból érkező és továbbítandó csomag is használja. Másrészről fennáll annak a veszélye, hogy a bemenő adatforgalom csomagjai úgy elárasztanak egy IMP-t, hogy korlátozott tárolókapacitása miatt csomagokat veszít. Míg vonalkapcsolás esetén az üzenet lényegében egyben kerül átvitelre. Csomagkapcsoláskor a csomagok sorrendje megváltozhat, és a sorrendhelyes összerakásukról is gondoskodni kell.

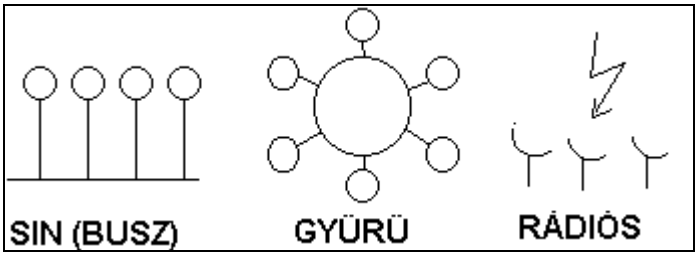
<u>Hálózati topológiák:</u>

A hálózati topológiát a kábelek lerendeződése, a csomópontok földrajzi elhelyezkedése határozza meg. Ez a „hálózat alakja”. (Az Ethernet sín, ill. csillag topológiát alkalmaz.)

- ***Sín:*** a hálózatnak van egy gerince (bachbone) (közös adatátviteli vonal), amihez az összes csomópont csatlakozik. A gerinc minkét vége ellenállással van lezárva, a rendszer elemei sorba vannak fűzve egy kábelre. Minden csomópontnak egyedi címe van. Olcsó, kevés kábel kell hozzá. Hiba esetén az egész hálózat működésképtelen lesz. Üzenetszórásos. Szabályozómechanizmusa: ütközés-feldolgozásos (CSMA/CD, CSMA/CA) vagy időosztásos (TDMA) vagy vezérlőjeles (vezérlőgép kell).
- ***Csillag:*** a csomópontok egy közös elosztóba (hub) vannak bekötve. A csillag topológiánál pedig elosztók (hub) gyűjtik össze egy-egy gépcsoport jeleit és továbbítják a központ felé. A csillag topológia előnye az, hogy egy új elosztó beépítésével újabb és újabb gépcsoportokat lehet a rendszerhez kapcsolni. Nem üzenetszórásos (ponttól-pontig). Szakadás esetén megbízhatóbb, sok kábel kell hozzá → drága.
- ***Gyűrűs:*** a csomópontokat közvetlenül egymáshoz csatlakoztatják soros elrendezésben, így azok egy zárt hurkot alkotnak. Az üzenetek fogadása egy alkalmas csatoló eszköz segítségével történik. Olcsóbb, mint a sínes, lassú, információtárolás nem tudjuk, hogy hol van, bolyong. Logikai biztonság szempontjából megjósolhatatlan, nem tudjuk, ki hallgatja le. Ha egy ponton megszakad, átmegy sínbe, ekkor is még mindenki mindenkivel kapcsolatba tud lépni. Előre történő huzalozása nehézkes, új csomópont hozzáadása, vagy elvétele megbonthatja a hálózatot. A biztonság kedvéért két kábellel is összeköthetik a gépeket. Az adatáramlásnak iránya van. Amíg az adatot nem szedik le, addig tárolódik a gyűrűben. Ez nem túl jó, ezért küldőnek kell leszedni és nyugtázni, hogy ne keringjen a végtelenségig.
- ***Fa:*** a sín topológia fa topológiává egészíthető ki, amelyben a többszörös sínágak különböző pontokon kapcsolódnak össze, így alkotva egy fastruktúrát. Meghibásodás esetén csak a csomópont és a hozzátartozó gyökerek esnek ki. Hierarchikus szerkezetű. Az egy szinten lévő gépek kommunikálnak a legtöbbet. Olcsóbb a teljes hálózatnál, leszakadhatnak az ágak. Ha egy géphez való vonal szakad meg, akkor olyan, mint egy csillag, de a hierarchián fent, attól még a kisebb telepek működnek.
- ***Teljes:*** biztonságos logikailag, legdrágább, technikai szempontból is jó.
- ***Szabálytalan:*** sok gép között sokféle kapcsolat van, de nem az összes.



Pont-pont topológiák



Üzenetszórásos topológiák

<u>Hálózati szoftver alapfogalmak</u>

<u>Réteg</u>: A számítógép hálózatok tervezését strukturális módszerekkel végzik, tehát az egyes részeket rétegekbe, vagy más néven szintekbe szervezik, melyek mindegyike az előzőre épül. Két gép között a rétegek mindig azonos szintű rétegekkel kommunikálnak, úgy hogy az egyes réteg az alatta elhelyezkedőnek vezérlőinformációkat és adatokat ad át egészen a legalsó rétegig, ami a kapcsolatot megvalósító fizikai réteghez tartozik.
<u>Protokoll</u>: Egy adott kapcsolatnál használt szabályok és megállapodások összessége.
<u>Interfész</u>: réteginterfész, amely az alsóbb réteg által a felsőnek nyújtott elemi műveleteket és szolgálatokat határozza meg.
<u>Hálózati architektúra</u>: A rétegek és rétegprotokollok halmaza.

Z1/2 A számítógép hálózatok réteges referenciamodelljei, ISO-OSI és a TCP/IP hivatkozási modellek összehasonlítása és kritikája, a szabványosítás problémája. Általános rétegfeladatok

Az ISO-OSI hivatkozási modellek:

OSI (Open System Interconnection – Nyílt Rendszerek Összekapcsolása) 7 rétegű modell nem egy hálózati architektúra, nem határoz meg konkrét protokollokat és szolgálatokat az egyes rétegekben. Csakis azt mondja meg, hogy az egyes rétegeknek mit kellene csinálniuk. Az ISO (International Standards Organization – Nemzetközi Szabványügyi Szervezet) szabványokat is készít az egyes rétegek számára, igaz ezek szorosan véve nem részei a modellnek. Mindegyiket különálló szabványként publikálták.

Rétegek: ADÓ		Rétegek: VEVŐ
Alkalmazási réteg		Alkalmazási réteg
Megjelenítési réteg		Megjelenítési réteg
Viszony réteg	Társ protokoll	Viszony réteg
Szállítási réteg	(logikai kapcsolat)	Szállítási réteg
Hálózati réteg		Hálózati réteg
Adatkapcsolati réteg		Adatkapcsolati réteg
Fizikai réteg	ÁTVIVŐ KÖZEG	Fizikai réteg

Fizikai réteg (physical layer): a bitek kommunikációs csatornára való bocsátásáért felelős. Biztosítania kell az elküldött bitek hibátlan megérkezését. Ezen a rétegen zajlik a tényleges fizikai kommunikáció. Ez már technikai megoldás, a bitsorozat átvitele helyesen. Átviteli közegek (sodrott érpár, koaxiális kábel, twinaxiális kábel, optikai kábel, rádiós átvitel), kódolási formák (természetes kódolás, RTZ, NRZ, Manchester 2, differenciális Manchester). Azokat a mechanikai és villamos eszközöket, illetve eljárásokat öleli fel, amelyek az adatok átviteléhez, az adatkapcsolati entitások közötti fizikai összeköttetés létrehozásához, fenntartásához és bontásához szükséges.

Adatkapcsolati réteg (data-link layer): alapvető feladata az, hogy tetszőleges kezdetleges adatátviteli eszközt olyan adatátviteli vonallá transzformáljon, amely a hálózati réteg számára átviteli hibától mentesnek tűnik. A küldő a bemenő adatokat adatkeretekre tördeli, ellátja kiegészítő cím és ellenőrző információval, majd a vevő által visszaküldött nyugtakeretet feldolgozza. (kerethatárok, transzparencia probléma -transzparens, ha a küldendő bitsorozat ugyanaz, mint a vezérlőjel - , vezérlőjelek, nyugtázások, hibafelmérés és kiküszöbölés). BSC és HDLC protokollok. (kódolások, sűrítések).

Hálózati réteg (network layer): a kommunikációs alhálózatok működését vezérli (útvonalkeresés, címzési módok, torlódáskezelés). A két végpont közti kapcsolat lebonyolítása és a torlódás elkerülése a feladata, tehát a keretek vevőtől célba való juttatásának optimális útvonalának kiválasztása. Eltérő lehet a hálózatok címzési módszere, különbözhetnek a maximális csomagméreteik és protokolljaik is. E problémák megoldásáért, azaz a heterogén hálózatok összekapcsolásáért a hálózati réteg a felelős. Üzenetszórásos hálózatokban az útvonal-kiválasztási mechanizmus igen egyszerű, így a hálózati réteg általában vékony, sokszor nem is létezik.

Szállítási réteg (transport layer): alapvető feladata a hostok közötti átvitel megvalósítása, vagyis az, hogy adatokat fogadjon a viszonyrétegtől, kisebb darabra vágja szét azokat (ha szükséges), majd adja tovább a hálózati rétegnek és biztosítsa, hogy minden darab hibátlanul megérkezzék a másik oldalra. Továbbá, mind ezeket hatékonyan kell végrehajtania, ráadásul oly módon, hogy a viszonyréteg elől el kell fednie a hardvertechnikában elkerülhetetlenül bekövetkező változásokat (hibamentes szállítás a dolga).

Viszony réteg (session layer): lehetővé teszi, hogy különböző gépek felhasználói viszonyt (session) létesítsenek egymással. A viszonyréteg, akárcsak a szállítási réteg közönséges adatátvitelt tesz lehetővé, de néhány olyan szolgáltatással kiegészítve, amelyek egyes alkalmazásokhoz hasznosak lehetnek. Egy viszony pl. arra alkalmas, hogy egy felhasználó bejelentkezzen egy távoli időosztásos rendszerbe vagy, hogy állományokat továbbítson két gép között. A két végpontban lévő programok tudnak kommunikálni. A viszonyréteg egyik szolgáltatása a párbeszéd szervezése. A viszonyok egy időben egy- és kétirányú adatáramlást is lehetővé tehetnek. A viszonyréteg egy másik szolgáltatása a szinkronizáció (két nem közvetlenül összekötött pont között kapcsolat). Szinkronizációs ellenőrzési pontokat iktat be, ezt úgy biztosítva, hogy hosszú időn keresztüli adatfolyam átvitele alatt bekövetkező hiba esetén elegendő az utolsó ellenőrzési ponttól ismételni az elveszett adatok átvitelét.

Megjelenítési réteg (presentation layer): olyan feladatok végrehajtásáért felelős, amelyek elég gyakoriak ahhoz, hogy általános megoldásúak legyenek ahelyett, hogy a felhasználók esetenként külön-külön oldják meg azokat. Az alsó rétegektől eltérően, amelyek csak a bitek megbízható ide-oda mozgatásával foglalkoznak, a megjelenítési

réteg az átviendő információ szintaktikájával és szemantikájával, egységes kezelésével foglalkozik. A megjelenítési réteg az információábrázolás más vonatkozásait is magába foglalja. Ilyen pl. az adatátvitel hatékonyabbá tételét elősegítő adattömörítés továbbá a hitelesítést és titkosítást lehetővé tevő kriptográfia. (két pont között hibátlan átvitel). Tehát tömören a feladata az adatok egységes kezelése, az adattömörítés és az átvitt adatok titkosítása.

Alkalmazási réteg (application layer): széles körben igényelt protokollokat tartalmaz. Feladata a fájlok átvitelekor az eltérő névkonvenziók kezelése. Az állománytovábbításokon kívül ehhez a réteghez tartozik még az elektronikus levelezés, a távoli munkabevitel, a katalóguskikeresés, és még egy sor egyéb, általános-, ill. speciális célú alkalmazási feladat is. Ez kapcsolódik szorosan a felhasználóhoz, itt kell a hálózati felhasználói kapcsolatok megoldásait megvalósítani.

A TCP/IP hivatkozási modellek:

A TCP/IP (Transmission Control Protocol / Internet Protocol) egy 4 rétegű modell. Nem csak az interneten alkalmazható, de elsősorban internet alkalmazások használják.

TCP/IP rétegek

Alkalmazási réteg
Szállítási réteg
Hálózati réteg (Internet)
Hálózat elérési réteg

Hálózat elérési réteg (Network Interface)*:* Részleteket határoz meg arra vonatkozóan, hogy a rendszer hogyan küldi el ténylegesen az adatokat a hálózaton keresztül, például, hogy a hálózati adathordozókkal közvetlen kapcsolatban álló hardvereszközök (koaxiális kábel, optikai szál vagy sodrott érpárú rézvezeték) hogyan látják el elektronikus jelzésekkel az egyes biteket.

Hálózati réteg (Internet)*:* Az adatokból IP-datagramokat állít össze, amelyek tartalmazzák a forrás és a cél címét, amelyet a rendszer a datagramok állomások közötti, hálózatokon keresztüli továbbításakor használ. Ez a réteg az IP-datagramok útválasztását végzi.

Szállítási réteg*:* A szállítási réteg feladata az, hogy lehetővé tegye a forrás- és célállomások közötti kommunikációt, szinkronizációt. A rétegben két szállítási protokollt definiálhatunk: TCP (Transmission Control Protocol, átvitelvezérlő protokoll): a beérkező bájtos adatfolyamot szeletekre osztja, majd ezeket továbbítja. A továbbítás során hibamentes bájtos adatfolyamatot biztosít. UDP (User Datagram Protocol, felhasználói adatforgalom protokoll): Nem megbízható adatfolyam továbbítást biztosít. Elsősorban olyan továbbításnál használatos, ahol nem a megérkezett üzenet tartalma a fontos, hanem a csomag beérkezése vagy elmaradása. (pl.: ping csomagok)

Alkalmazási szint*:* Felhasználói és hálózati kapcsolatot biztosító protokollok: ftp, telnet, smtp, dns, stb..

ISO-OSI és a TCP/IP hivatkozási modellek összehasonlítása és kritikája

Hasonlóságok:

- Mindkettő rétegekből tevődik össze
- Mindkettőben található egy alkalmazási réteg, bár funkciójuk igencsak különböző
- Mindkettő hasonló funkciójú szállítási és hálózati réteggel rendelkezik
- Csomagkapcsolt technológiát vesznek alapul
- A hálózati szakembereknek mindkettőt ismerniük kell

Különbségek:

- A TCP/IP az alkalmazási rétegre hárítja a megjelenítési és a viszonyréteg funkcióit
- A TCP/IP az OSI modell adatkapcsolati rétegét és a fizikai réteget egy réteggé vonja össze
- A TCP/IP kevesebb rétege miatt egyszerűbbnek tűnik
- A TCP/IP protokolljaira épült az Internet, tehát a TCP/IP modell csak a protokolljai miatt nyert létjogosultságot. Ezzel szemben az OSI modellre épülő protokollokat egyetlen hálózat sem használja, bár mindenki az OSI modell alapján gondolkodik.

Kritikájuk:

Az OSI modell kritikája:

Rossz időzítés, rossz technológia (különböző rétegfeladatok ismétlődnek, kommunikáció orientált), rossz implementálás.

- **Rossz időzítés:**

Egy szabvány megjelentetésének időpontja rendkívül erősen befolyásolhatja annak sikerét. A szabványosításnak a kutatások befejezése után és a beruházások megkezdése előtt kell megtörténnie. Ez azért fontos, hogy a kellő tapasztalat birtokában egységes szabványt hozhassunk létre.

Mire az OSI protokollok megjelentek, addigra a versenytárs TCP/IP protokollok már széles körben elterjedtek a kutatóegyetemeken.

- **Rossz technológia:**

A protokollok nem voltak tökéletesek. A viszony réteget alig használja a legtöbb alkalmazás, a megjelenítési réteg pedig szinte teljesen üres. Eredetileg csak öt réteg volt, de mivel a nagy befolyású IBM-nek már volt egy 7 rétegű modellje ezért 7 rétegűre módosították.

- **Rosszul implementálható:**

  A modell és a protokollok rendkívüli bonyolultsága miatt az implementációk kezdetben terjedelmesek, kezelhetetlenek és lassúak voltak. Mindenki megbukott, aki próbálkozott vele. Nem telt bele sok idő, és az „OSI"-ról mindenkinek a „gyenge minőség" jutott az eszébe. Bár az idők során egyre jobbak lettek a termékek, a kialakult kép nem változott.

  Ugyanakkora TCP/IP egyik első implementációja a Berkeley-féle UNIX része volt, és nem csak nagyon jó, de még ingyenes is volt. Az emberek gyorsan rászoktak, így komoly felhasználói tábora alakult ki. Ennek köszönhetően egyre jobb lett a termék, ami tovább növelte a felhasználók körét.

TCP/IP modell kritikája:

Nem tisztázott a specifikáció és az implementáció, a hálózat elérés réteg a fizikai és az adatkapcsolati réteget nem választja el.

- A modell nem tesz világos különbséget a szolgálat, az interfész és a protokoll fogalma között
- A TCP/IP modell egyáltalán nem általános érvényű, és önmagán kívül más protokollkészletek leírására nem igazán alkalmas.
- A TCP/IP modell nem különbözteti meg a fizikai és az adatkapcsolati réteget, pedig ez két teljesen különböző dolog.
- Az IP és a TCP protokollt alaposan átgondolták, és jól implementálták, a többi protokoll nagy része inkább eseti jellegű

Elméletben az OSI az ideális, de gyakorlatban a TCP/IP.

A szabványosítás problémája:

Alapvetően a szabványoknak két családja van: a de-facto és a de-jure. A második esetben bizottságok deklarálnak, hivatalosan dokumentálnak szabványokat. Az első pedig egy széles körben használt konkrét megoldásból alakul ki, amelyet aztán célszerű de-jure szabványokká alakítani. A hálózatok esetében is több vezető cég a saját termékeit akarta ráerőltetni másokra, hogy az ő eszköze, megoldása legyen a hivatalos szabvány.

A sok kompromisszumos megoldás mellett megszületett a hétrétegű ISO-OSI modell. Nagyszerűségét bizonyítja, hogy bár nem szabvány, csak egy modellajánlás, ma már a hálózatok kialakításánál alapul veszik.

Z1/3 A fizikai réteg jellemzői és adatátvitellel kapcsolatos alapfogalmak (szinkron-aszinkron, szimplex-félduplex-duplex), az átviteli csatorna jellemzése, átviteli közegek, átviteli módok, kódolások.

Fizikai réteg (physical layer):

a bitek kommunikációs csatornára való bocsátásáért felelős. Biztosítania kell az elküldött bitek hibátlan megérkezését. Ezen a rétegen zajlik a tényleges fizikai kommunikáció. Ez már technikai megoldás, a bitsorozat átvitele helyesen. Átviteli közegek (sodrott érpár, koaxiális kábel, twinaxiális kábel, optikai kábel, rádiós átvitel), kódolási formák (természetes kódolás, RTZ, NRZ, Manchester 2, differenciális Manchester). Azokat a mechanikai és villamos eszközöket, illetve eljárásokat öleli fel, amelyek az adatok átviteléhez, az adatkapcsolati entitások közötti fizikai összeköttetés létrehozásához, fenntartásához és bontásához szükséges.

A bitek kommunikációs csatornára való bocsátásáért felelős. Ezen a rétegen zajlik a tényleges fizikai kommunikáció. Ez már technikai megoldás, a bitsorozat átvitele helyesen. Az adatátvitelt a használt sávszélesség, valamint az adatátviteli sebesség jellemzi, azon kívül persze, milyen a fizikai kialakítása.

Sávszélesség:

Analóg rendszerek esetén használt fogalom: egy adott analóg jel maximális és minimális frekvenciájának a különbségét értjük alatta.

Adatátviteli sebesség:

Digitális hálózatok jellemzője, mértékegysége

bit/s: egy időegység alatt átvitt bitek száma

baud: a felhasznált jel értékében 1 másodperc alatt bekövetkezett változások száma

Adatátviteli modell:

Forrás ---> Adó ---------- Csatorna (+Zaj) ---------- Vevő ---> Cél

Átviteli módok:

- **Aszinkron:** melynek lényege, hogy az adó és a vevő nem hangolják össze a tempót. Start-stop byte-onként történik az adatátvitel. A kibocsátás és a mintavételezés ritmusa eltérő. A karakterszervezésű üzenetek átviteli módja. Hosszú adatátvitel nem valósítható meg vele.
- **Szinkron:** melynek lényege, hogy az adó először elküld egy jelet a vevőnek, az ráhangolódik, így szinkronba kerül az adóval. Így az üzenet bitjei szigorú rendben követik egymást. Nagytömegű adat esetén gyorsabb, hibavédettebb. Bitszervezésű üzenetek átviteli módja.

Adatátviteli szabályok:

- **Szimplex:** egy csatorna, az adat csak egy irányba folyhat. Az egyik az adó, a másik a vevő. Az adótól a vevőig folyhat az átvitel. Pl.: rádió
- **Félduplex:** egy csatorna, az adat két irányba folyhat, de nem egyidőben. Egyszer az egyik fél az adó és a másik a vevő utána pedig fordítva az adatáramlás irányától függően. Ez az átvitel a számítógépek közötti kommunikációra alkalmas. Pl.: CB rádió.
- **Duplex:** két csatornán kétirányú adatátvitelt enged meg egyidőben tehát mindkét állomásnak egyidejűleg teszi lehetővé az adást és a vételt. Egyik csatorna sérülése esetén átmehet félduplexbe. Pl.: telefon.

A csatorna néhány fontos jellemzője:

- Átviteli mód (szinkron, aszinkron)
- Alkalmazott adatátviteli szabály (szipmlex, fél-duplex, duplex)
- Csatornakapacitás
- Hibatűrés, megbízhatóság
- Zajszint
- Lehallgathatóság

Átviteli közegek:

Vezetékes:

UTP, STP (Csavart érpár):

UTP (Unshielded Twisted Pair – árnyékolatlan csavart érpár)

Külső zavarok ellen védtelen adatátviteli közeg, leggyakrabban alkalmazott kábeltípus az Ethernet hálózatoknál. Az UTP kábel számos hálózatokban használt, 4 érpárból álló átviteli közeg. Az UTP kábeleknek mind a 8 rézvezetéke szigetelőanyaggal van körbevéve. Emellett a vezetékek párosával össze vannak sodorva, így csökkentve az elektromágneses es rádiófrekvenciás interferencia jeltorzító hatását. Az árnyékolatlan érpárok közötti áthallást úgy csökkentik, hogy az egyes párokat eltérő mértekben sodorjak. A kábel végén RJ-45-os csatlakozó van, amely a hálózati kártyába csatlakozik. A kábeleket kategóriákba soroljak és *CAT + szám* típusú jelzéssel látják el. A nagyobb szám nagyobb adatátviteli sebességet jelöl.

TIA/EIA T568A T568B-elterjetebb

Lehetséges színsorrendek:

B. TÍPUS: 1. Narancs-feher 2. Narancs 3. Zold-feher 4. Kek 5. Kek-feher 6. Zold 7: Barna-feher 8. Barna.

A. TÍPUS: 1. Zold-feher 2. Zold 3. Narancs-feher 4. Kek 5. Kekfeher 6. Narancs 7. Barna-feher 8. Barna.

Egyenes kábel: az UTP kabel mindket vege azonos szinsorrend szerint van osszeallitva.

Keresztkötésű kábel: az UTP kabel ket vege kulonboző szinsorrend szerint kerul kialakitasra.

STP (Shielded Twisted Pair – árnyékolt csavart érpár)

Szerkezetet tekintve hasonlo az UTP kabelhez, de a műanyag kulső burkolaton kivul tartalmaz meg egy arnyekolo (femszovet burok) reteget is. A retegnek koszonhetően kulonosen jol vedett a zajhatasoktol. Kialakitasabol kovetkezően igen draga megoldas, csakis celfeladatok megvalositasara alkalmazzak, ahol a komoly zajerzeketlenseg elvaras.

FTP (Foiled Twisted Pair –fóliázott csavart érpát)

Ezeket a kábeleket gyakran tévesztik össze az STP kábelekkel. Pedig a különbség alapvető. Az STP kábelek esetében az árnyékolást egy, a koaxiális kábeléhez hasonló rézháló biztosítja, míg az FTP esetében ez egy vékony fémfólia köpenyt jelent a sodrott érpárak körül. Az STP kábelek sokkal vastagabbak, nehezebben telepíthetők, mint az FTP kábelek, árnyékolási paramétereik pedig rosszabbak, főként a nagyobb frekvenciák tartományában.

Koaxális kábelek:

Egyszerű, árnyékolt ér. A TV-jelek átvitelére használták kezdetben. Két fajtája terjedt el: az **alapsávú** és a **szélessávú** koaxális kábel.

A koax kábelek legfontosabb jellemzői:

- hullámellenállás
- késleltetési idő
- csillapítás

ALAPSÁVÚ koax:

Lokális hálózatokhoz, digitális jelátvitelre használatos. Az adatátviteli sebesség távolságfüggő (1 Km-en akár 100 Mbit/s).

- **Alapsávú vékony koax**: 10Base2 200 m-es távolságig. Arcnet és Ethernet. BNC csatlakozókat alkalmaz.
- **Alapsávú vastag koax:** 10Base5 500 m-ig. Ethernet. Lényegesen kisebb csillapítású. Vámpírcsatlakozó.

SZÉLESSÁVÚ koax:

Nagy távolságra szállít analóg jelet (300-450 Mhz). Analóg erősítőkre van szükség, ezért átvitel csak szimplex. A duplex átvitel megoldásai: egykábeles (két különböző frekvenciatartomány) és kétkábeles.

Üvegszálas kábel:

A jelenlegi legkorszerűbb vezetekes adatatviteli modszer, az uvegszal technologia alkalmazasa. Az informacio fenyimpulzusok formajaban terjed egy fenyvezető kozegben, praktikusan egy uvegszalon. Az atvitel harom elem segitsegevel valosul meg: fenyforras - atviteli kozeg - fenyerzekelő. A fenyforras egy LED dioda, vagy lezerdioda.

A fényforrás (LED vagy lézerdióda) fényét adott átviteli közegen keresztül (egy vagy többmódusú üvegszál) juttatjuk egy fényérzékelőre. Az átvitelt akadályozó tényezők:

- **Visszaverődés:** a két közeg határán lép fel, amit gondos illesztéssel minimalizálhatunk.
- **Csillapítás:** döntően az üvegben lévő szennyeződések okozzák
- **Határfelületen kilépő fénysugarak:** a teljes visszaverődés jelensége szünteti meg.

TÖBBMÓDUSÚ üvegszál(multimode fiber): esetén a fény az üvegszálban a kis beesési szögek miatt visszaverődik.

EGYMÓDUSÚ üvegszálnál (single/mono mode fiber): A szál átmérője közel azonos az alkalmazott fény hullámhosszával. Ilyen esetben lézerdiódát kell alkalmaznunk.

A jelek be és kicsatolására kétféle illesztés használatos:

- PASSZÍV ILLESZTŐ: Egy fotodióda és egy LED. Csillapítása van, ezért csak korlátozottan használható.
- AKTÍV ILLESZTŐ: Jelismétlő. Elektromos jelekké alakítja a fényjelet, ezért közvetlen elektromos illesztésre is használható. Ethernet hálózatokon az üvegszálas kábelt **10BaseF** néven definiálták.

Vezeték nélküli átviteli közegek:

- **Infravörös/lézer:**

  Jól irányítható, nagy távolságra hatásos, védett. Légköri szennyeződések zavarként jelentkeznek.

- **Rádióhullám:**

  Mikrohullámú átvitelnél (2-40 GHz) a láthatóság feltétel. Légköri zavarok hatnak rá. A frekvencia-kiosztás hatósági feladat.

- **Szórt spektrumú sugárzás:**

  Kisebb távolságokra lokális hálózatoknál. Széles frekvenciasávot használ. Antennája akár egy darab vezeték is lehet.

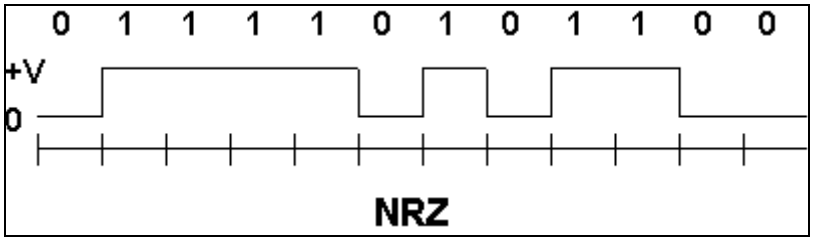
- **Műholdas átvitel:**

  A műholdon elhelyezett transzponderek a felküldött jelet (5,925..6,425 GHz) egy másik frekvencián (3,7..4,4 GHz) felerősítve visszasugározzák. A visszatérő jelzés néhány száztól néhány kilométeres átmérőjű területet fedhet le.

Kódolások:

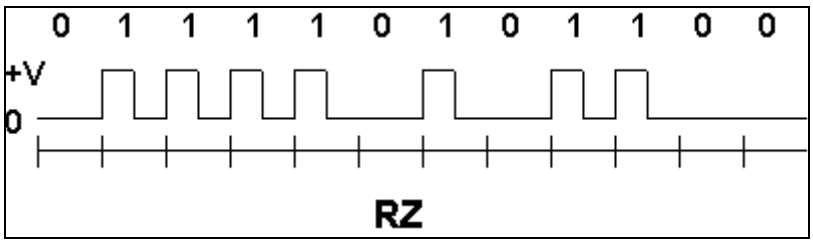
A fizikai vonalon való átvitelnél a bitek ábrázolására több lehetőség is van. Gyakorlatban használt lehetőségek:

- **NRZ (Non Return to Zero):** Nullára vissza nem térő
  Azaz mindig az a feszültség van a vonalon, amit az ábrázolt bit határoz meg. Ez a leginkább gyakori, "természetes" jelforma. Legegyszerűbb, természetes kódolás. A bitérték: **1**: ha magas a jelszint, **0**: ha alacsony.



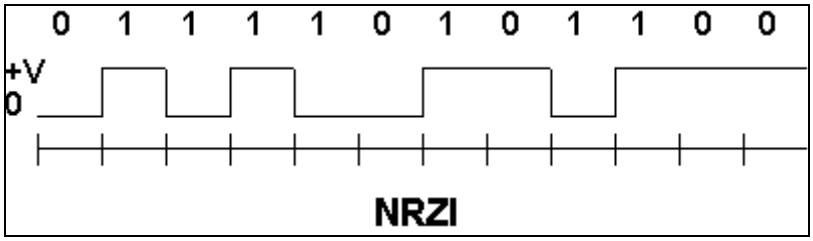
- **RZ (Return to Zero):** Nullára visszatérő

  A jelszint mindig alacsony, de egyes jel esetében a bitidő első felében magas a jelszint. A nulla a "nyugalmi állapot", 1 bitnél a bitidő első felében a +V, a második felében a jel visszatér a 0-ra:



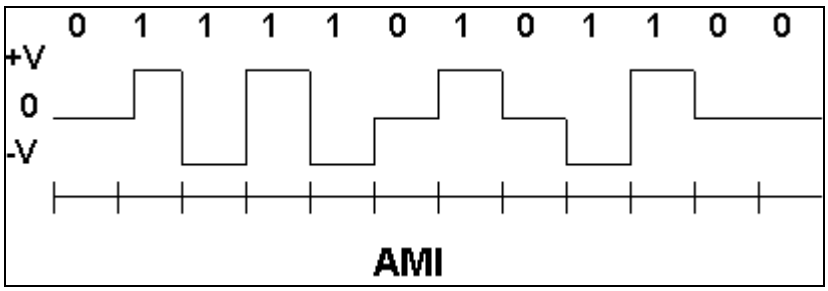
- **NRZI (Non Return to Zero Invertive):** Nullára nem visszatérő, „megszakadásos”

  Ua. mint az NRZ, azonban ha 1-esek követik egymást akkor a jelszint az előző ellentettjére változik.



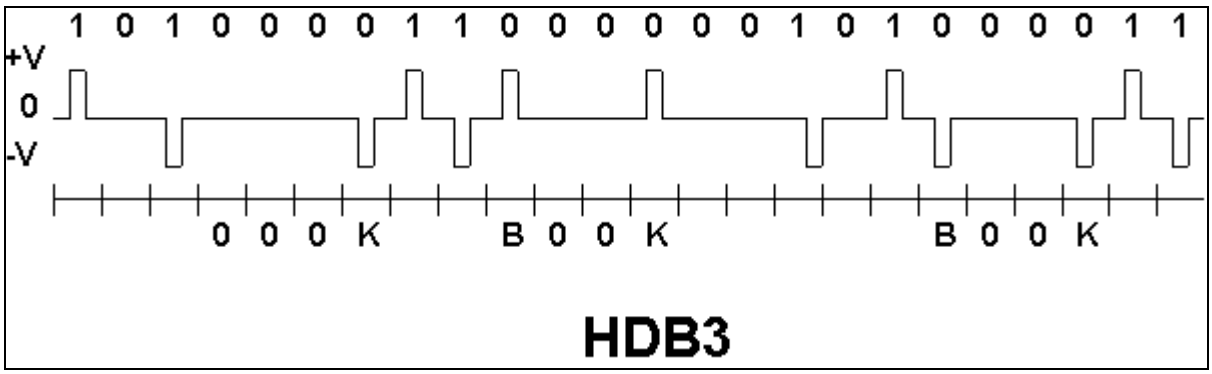
- **AMI (Alternate Mark Inversion):** Váltakozó 1 invertálás

  Itt negatív feszültség érték is használt. A 0 jelszintje 0, az 1-es V+ vagy V-, éppen az előző 1-es (nem kell közvetlenül előtte lennie) érték ellentettje.



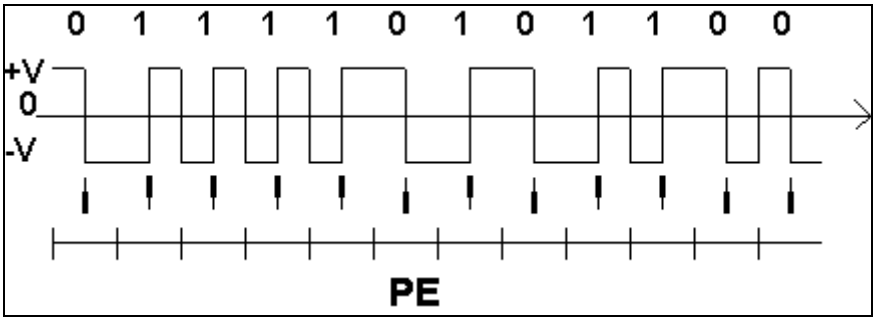
- **HDB3(High Density Bipolar 3):** Nagy sűrűségű bipoláris 3

  Mikor 4 egymás utáni 0 bit következik, akkor megváltoztatjuk az utolsót K-ra, így 000K-t kapunk K polaritása megegyezik az előző 1-es polaritásával. Hosszú 0 sorozatok esetén az első 0-nál a vevő B-t vesz majd 4 db 0 után K-t így tudja, hogy 0 és nem 1-es.



- **PE(Phase Encode (Manchester):** Manchester kódolás

  A jelátmenet iránya mutatja a bitet. A lefelé irányuló polaritás váltás 0-t a felfelé irányuló 1-t jelöl. Több azonos bit esetén két bit között félidőben vissza kell térnie az eredeti szintre, azért, hogy ugyanolyan irányú legyen az átmenet.



Z1/4 Az adatkapcsolati réteg feladata, keretezés, keretezési eljárások. Hibavédelem, Hamming-távolság, hibajelzési, hibajavítási képesség.

Adatkapcsolati réteg (data link layer):

Alapvető feladata az, hogy tetszőleges kezdetleges adatátviteli eszközt olyan adatátviteli vonallá transzformáljon, amely a hálózati réteg számára átviteli hibától mentesnek tűnik. A küldő a bemenő adatokat adatkeretekre tördeli, ellátja kiegészítő cím és ellenőrző információval, majd a vevő által visszaküldött nyugtakeretet feldolgozza. (kerethatárok, transzparencia probléma -transzparens, ha a küldendő bitsorozat ugyanaz, mint a vezérlőjel - , vezérlőjelek, nyugtázások, hibafelmérés és kiküszöbölés). BSC és HDLC protokollok. (kódolások, sűrítések).

Feladata az adatok megbízható továbbítása az adó és vevő között. Ez általában úgy történik, hogy az átviendő adatokat adatkeretekké (data frame) tördeli, ellátja kiegészítő cím, egyéb és ellenőrző információval, ezeket sorrendhelyesen továbbítja, majd a vevő által visszaküldött nyugtakereteket véve ezeket feldolgozza.

Keretezés

A hálózati rétegtől kapott csomagot egy fejléccel (cím, keretinformáció) valamint CRC bejegyzéssel (hibaellenőrzés) látja el, ahonnan, így mint **keret** kerül át a fizikai réteghez.

Keretek képzése:

- **Karaktersorozatnál:**
  - **Karakterszámláló módszer:** a fejlécben megadjuk a leadott karakterek számát, amiből a vevő a karaktersorozat végét azonosíthatja.
  - **Kezdő- és végkarakterek alkalmazása:** egy speciális karaktersorozattal jelöljük a keret kezdetét és végét. A kezdetet DLE STX, és a végét DLE ETX karakterkettőssel jelezzük. Ezek az ASCII kódtáblában megtalálható karakterek.
- **Bitsorozatnál:**
  - **Kezdő- és végjelző bitek beszúrása:** Kezdő és végjelző bitsorozatot kap a csomag (01111110), valamint az adó az adatmezőben található 5 egymást követő 1-es után beszúr egy 0-át is. A vevőnél ez a bit valamint a kezdő és a végjel leválasztódik.

Hibakezelés

Az adatátvitel és a kommunikáció fontos kérdése az átvitel során fellépő hibák kezelése. Az adatkapcsolati réteg a keretezésen kívül a hibakezelésért is felelős. Egyedi bithibák kezelésére a **hibajavító(ECC)** és **hibajelző kódok(EDC)** alkalmazása ad lehetőséget. Mindkét esetben az adatblokkokat redundanciával küldik, hogy a vevő az esetleges hiba tényét felfedezhesse (hibajelzés) illetve megállapíthassa, hogy minek kellett volna jönnie (hibajavítás). A hibajavító eljárás fontos jellemzője a Hamming távolság, mely a javítható hibák számát adja meg. Ez egyenlő a kezdeti és kódolt szó közötti XOR kapcsolat által adott 1-esek számával.

A hibajelzés fajtái

Paritásbites hibajelzés

A hibajelzés legegyszerűbb az egyik leggyakrabban használt fajtája. Két alapvető típusát különböztethetjük meg, a páros- és a páratlan paritást. Páros-paritás használatakor az adatot olyan bittel egészítjük ki, hogy az adatcsomagban, amelyben már a paritásbit is benne van, az egyesek száma páros legyen. A páratlan-paritás megoldás is hasonló, csak itt az adatcsomag 1-eseinek száma páratlannak kell lennie. Ha átvitel során bármelyik bit megváltozik, akkor azt képes a vevő érzékelni. Természetesen a módszer csak akkor működik, ha az átvitel előtt a résztvevők megállapodnak a paritás típusában.

Tömbparitás vizsgálat:

A paritásbites hibajelzés továbbfejlesztése. Az átvitelre kerülő információblokkot egy mátrixnak tekintjük. A mátrix oszlopainak száma a paritásbittel kiegészített kódszó hossza, a sorok száma pedig a blokkban lévő kódszavak száma. Minden sor tartalmaz egy paritásbitet, ezen túlmenően minden képzeletbeli oszlophoz is kiszámítunk egy paritásbitet. Ezt a paritásszót az utolsó kódszó után továbbítjuk.

CRC – Cyclic Redundancy Check:

Csoportos hibák elleni védelemre. Egy keretnyi adatot egy előre meghatározott bitsorozattal elosztunk, és a maradékot a keret részeként továbbítjuk. A vevőnél is elosztjuk, majd a kapott maradékokat összehasonlítjuk.

Hibajavítási eljárások

Előre vezető ágban történő hibajavítás (FEC - Forward Error Correction) során az átküldendő adathoz hozzácsatoljuk az adat segítségével képzett Redundanciát, együtt a kettőt küldjük el és a vevőre bízzuk, hogy a redundancia segítségével helyreállísa az esetleg meghibásodott adatot (hibajavító kódolás). A vevő teljes kiszolgáltatottsága a redundanciától annak méretét fogja növelni.

Ha a vevő és a küldő közt lehetőség van kommunikációra élhetünk az automatikus ismétléskérés (ARQ - Automatic Repeat ReQuest) adta lehetőségekkel a redundancia csökkentésére, ezért azonban biztosítanunk kell a nyugtázás lehetőségét. Ilyenkor csak hibajelző kódolásra van szükség, ami ugyanakkora redundancia mellett nagyobb biztonságot nyújt.

Z1/5 Elemi adatkapcsolati protokollok, csúszó-ablakos protokollok, visszalépés N-nel, szelektív ismétléses protokollok.

Elemi adatkapcsolati protokollok

Adatkapcsolati rétegek közötti protokollok.

Egyirányú protokollok:

- **Korlátozás nélküli, egyirányú (szimplex) protokoll:** Az adó feltétel nélkül küldi a kereteket, a vevő vizsgálja a kapcsolatot érkezett-e keret, ha igen a protokoll elvégzi az átalakítást keretből csomaggá, s azt a hálózati réteghez küldi. Ha nem érkezett, újra vizsgálja az adatfolyamot. Megfelelő gyors vevő és lassú adó esetében.
- **Egyirányú „megáll és vár" protokoll:** Egy adó egy vevő működik, az adó viszont csak akkor küld új keretet, ha az előző célba érkezéséről nyugta érkezett. Ez viszont fél-duplex fizikai megvalósítást kíván. Lassabb vevő esetén azonban szükséges.
- **Szimplex protokoll zajos csatornához:**

  Ha egy keret megsérül az átvitel során, a vevő hardvere ezt felismeri, amikor kiszámítja az ellenőrző összeget. Ha a keret úgy sérül meg, hogy az ellenőrző összeg ennek ellenére helyes - ami rendkívül ritkán fordul elő -, ez a protokoll (és az összes többi is) hibázhat - azaz egy hibás keretet kézbesíthetnek a hálózati rétegnek.
- **Egyirányú összetett protokoll:** Az előző esetben előfordulhat, hogy a nyugta elmaradása miatt idővel az előző keret újra elindul, s a vevő többször kaphatja meg ugyanazt. Itt egy kiegészítő bittel (keret fejléce) megjelöli a vevő, hogy új vagy régi keretet küldött. A vevő ugyanígy nyugtát küld a kapott keretről, viszont a jelző bit olvasásakor megvizsgálja megkapta-e már azt a keretet.

Kétirányú protokollok(duplex):

- **Egyszerű megoldás két duplex átviteli csatorna alkalmazása.** Külön egy az adatkereteknek, s egy a nyugtáknak.
- **Megoldható két szimplex csatornával is**, ha az adatkeretekhez hozzácsatoljuk az előző vételről informáló nyugtát. Így megnő a küldött bitfolyam hossza, viszont az átviteli közeg kialakítása leegyszerűsödik.
- **Csúszó ablakos protokoll:** Megengedhető, hogy egyszerre több keret is tartózkodjon a csatornán. S amint nyugta érkezik az egyik célbaéréséről, újabb keret kerülhet a csatornára. Az ablak itt a csatornán lévő kereteket jelenti. Az adónak sending window, küldő ablaka van, míg a vevőnek receiving window, vételi ablaka. A küldő ablakban az elküldött, de még nem nyugtázott keretek vannak. A vételi ablak az elfogadható keretek sorszámait tartalmazza. A csúszóablak (sliding window) a csatornán lévő kereteket tartalmazza.

  3 altípus:

  - Egybites csúszóablakos protokoll: A vevő és az adó is rendelkezik egy 1 elemű csúszóablakkal (egy keret van a vonalon), vagyis az adó csak akkor küld adatot, ha az előző megérkezéséről megerősítést kap.
  - Visszalépés n-nel technikájú protokoll: Ha a keretek átviteli ideje hosszú akkor az előző megoldás nem jó. Ilyenkor a megoldás az, ha a csatornán több keret van egymás után. Ezt csővonalnak (pipelining) hívják. Ha egy keret sérülve érkezik, a hibás keret utáni kereteket nyugtázatlanul eldobja, kényszerítve az adót az ismétlésre. Zajos vonal esetén ez csökkenti az átviteli sebességet.
  - Szelektív ismétlő protokoll: Itt nem szakad meg a vétel a rossz keretnél, a jókat továbbra is fogadja. Amikor az adó felfedezi, hogy volt hibás keret (nem kap nyugtát róla), akkor azt újraküldi. Esetleges kiegészítés??

Z1/6 A közegelérési alréteg feladatai, a csatornakiosztás lehetőségei, többszörös hozzáférésű protokollok. Ütközéses, ütközésmentes, korlátozott versenyes protokollok.

A közegelérési alréteg feladatai

Az osztott csatornához való hozzáférést az adatkapcsolati réteg alsó alrétege vezérli(közegelérési alréteg, Medium Acces Conntrol)

Csatornakiosztás lehetőségei

1. **Statikus:** Az időt diszkrét időintervallumokra osztjuk fel, és a ciklikus multiplexeléses ütemezést alkalmazzuk. Így minden gép csak akkor férhet a csatornához és adhat, amikor a saját időintervalluma következik. A statikus kiosztás kihasználatlanul hagyja a csatornakapacitást akkor, amikor egy gépnek nincs adnivalója a számára kiosztott időintervallumban. Néhány rendszer ezért dinamikus csatornakiosztást alkalmaz.
2. **Dinamikus:** Szabad kezdeményezésen alapuló.
   - **Centralizált:** Van egy egység, amely eldönti, hogy ki lesz a következő.
   - **Decentralizált:** Nincs ilyen egység, minden állomásnak magának kell eldöntenie, vajon akar-e és tud-e adni vagy sem.

Többszörös hozzáférésű protokollok

1. **Ütközést jelző vivőérzékeléses többszörös hozzáférés (CSMA/CD):** Ennél a módszernél, mielőtt egy állomás adatokat küldene, először 'belehallgat' a csatornába, hogy megtudja, hogy van-e éppen olyan állomás, amelyik használja a csatornát. Ha a csatorna 'csendes', akkor a 'hallgatódzó' állomás elküldi az üzenetét. A vivőérzékelés (carrier sense) jelenti az adás előtti belehallgatást. Az állomás által küldött üzenet a csatornán keresztül minden állomáshoz eljut, és véve az üzenetet a bennfoglalt cím alapján eldöntheti, hogy az neki szólt (és ilyenkor feldolgozza), vagy pedig nem (és akkor eldobja). Ütközés esetén minden adó megszakítja az adattovábbítást, majd véletlenszerű ideig várakozik. A várakozás után újra megkísérel adni az előző ismeretek szerint (hallgat,…).
   Gyér forgalom esetén gyors, de a terheléssel hatványozottan arányosan lassul. Az Ethernet hálózat használja ezt a módszert.
2. ***Ütközést elkerülõ, vivõérzékeléses többszörös hozzáférés* (CSMA/CA):** A CSMA/CD - től abban különbözik, hogy adás után minden állomás adott ideig vár (pl.: prioritás szerint). Ha ez idő alatt nem kezdeményez senki, akkor az állomás adhat.
3. **Időosztásos többszörös hozzáférésű eljárás (TDMA):** Elsősorban busz felépítésű hálózatoknál használják. A buszhoz kapcsolódó minden mellékállomás egy adott időszeletben adhat. Ha nincs üzenet, a csatorna kihasználatlan marad. Problémát jelenthet a szinkronizálás.

Ütközésmentes protokollok

- **Egy bittérkép (helyfoglalásos) protokoll**
  Az alapvető bittérkép-eljárásban (basic bit-map method) az ütköztetési periódus pontosan *N (a csatornát használó állomások száma)* időrésből áll. Ha a 0-s állomás adni szeretne, akkor 1-es bitet küld a 0-s (első) versengési időrésben. Ha egy állomás nem szeretne adatot küldeni, akkor nem küld jelet. Az ütköztetési periódus végére kialakul a küldési sorrend, mely sorrendben a csomagok küldése történik, amiután újabb ütköztetési periódus következik.

- **Bináris visszaszámlálás**
  Az alapvető bit-térképes protokoll legnagyobb hátránya az, hogy a versengési periódus hossza állomásonként 1 bittel nő. Bináris állomáscímeket használva azonban jobb eredményeket érhetünk el. Ez esetben a forgalmazni kívánó állomás elkezdi a bináris címét, a legnagyobb helyi értékű bittel kezdve, mindenkinek szétküldeni. Az összes állomás címének azonos hosszúságúnak kell lennie. Az elküldött címek azonos helyi értékű bitjei logikai VAGY kapcsolatba lépnek egymással. Ezt a protokollt **bináris visszaszámlálásnak (binary countdown)** nevezzük.

A konfliktusok elkerülése érdekében szükség van egy kiegészítő szabályra is: amint egy állomás észleli, hogy 1-gyel lett felülírva egy olyan, magasabb helyi értékű címbit pozíció, ahol a saját címében 0 van, fel kell adnia a próbálkozást. Például, ha a 0010, 0100, 1001 és 1010 címekkel rendelkező állomások szeretnék használni a csatornát, akkor mindannyian elkezdik szétküldeni a legmagasabb címbitjüket, jelen esetben 0-t, 0-t, 1-et, illetve 1-et. Ezek logikai VAGY kapcsolata 1-et eredményez. A 0010 és a 0100 című állomások, látván az 1-et, feladják a versenyt, mivel látják, hogy a versenyben magasabb című állomás is részt vesz. Az 1001 és 1010 állomások tovább folytatják a versengést.
A következő bit 0, így mindkét állomás versenyben marad. Az ezt követő bit azonban 1, így az 1001 című állomás feladja a versengést. A győztes tehát az 1010 állomás lesz, mivel övé a legnagyobb cím. Miután megnyerte a „licitálást", továbbíthat egy keretet, amely után újabb verseny kezdődik a forgalmazás jogáért.

Ütközéses protokollok

Ethernet/Fast ethernet

Az ütközéses helyi hálózati protokollok legelterjedtebb típusa. Az ütközéses protokoll annyit jelent, hogy a hálózatra felfűzött számítógépek minden adatot észlelnek, de csak a nekik szólókra válaszolnak. Amikor egy állomás adatot akar küldeni, figyelni kezdi a hálózatot, folyik-e éppen forgalom. Ha igen, akkor vár, ellenkezőesetben elkezdi az adást. Ez egybeeshet egy másik állomás adáskezdésével, ekkor az üzenetek ütköznek, acélállomások nem tudják venni őket. Az ütközést mindkét (illetve az összes) adóállomás érzékeli, és leállítja a küldést. Ezután véletlenszerű ideig várnak, majd újra figyelni kezdik a csatornát. Ha ismét ütközést észlel, már nagyobb tartományból választ véletlenszerűen várakozási időt. Ezáltal teszi lehetővé a hálózati torlódások gyorslevonulását. Az eljárás kis és közepes forgalom esetén hatékony. A szabvány többféle keretformátumot is engedélyez.

Korlátozott versenyes protokollok

A versenyhelyzetes protokollok jól teljesítenek kis terhelésnél, de nagy terhelésnél nagyon romlik a hatásfok. Az ütközésmentes protokollok kis terhelésnél is jelentős késleltetéseket produkálnak, de a terhelés növekedésével javul a hatásfokuk. Pl.: a bit-térkép protokoll akkor a legnagyobb hatásfokú, ha minden állomás adni akar, hiszen akkor minden keret csak egyetlen időréssel bővül. Kívánatos lenne a kedvező tulajdonságok ötvözése. Az erre irányuló algoritmusok a **korlátozott versenyes protokollok**.
A korlátozott versenyes protokollok alacsony terhelés mellett ütközéses protokollként, nagy terhelés esetén pedig ütözésmentes protokollként viselkedik.

Az alapötlet az, hogy az állomásokat csoportokba rendezzük, és hozzárendeljük egy-egy időréshez. Egy időrésben csak az abba a csoportba tartozó állomások versengenek az időszeletért.

Z1/7 A vezetékes és vezeték nélküli IEEE 802 LAN ok, helyi hálózatok összekapcsolása, ismétlők, elosztók, hidak.

A „vezetékes" IEEE 802 LAN protokollok

Három szabványt fogadtak el, amelyekre együttesen az IEEE 802-es szabvány részeként hivatkoznak.

1. Ethernet (IEEE 802.3-as szabvány)

Sínszervezésű, véletlen hozzáférésű, alapsávú, rádió üzemmódú hálózat. CSMA/CD rendszer. Adatátviteli sebessége 10Mbit/s, 1024 állomás csatolható. A 802.3 által engedélyezett legnagyobb kábelhossz 500 méter. Az egyes kábeleket repeaterek (jelismétlők) segítségével lehet összekötni. A kábelhálózat építésének egyik lehetséges módja, amikor különálló szegmenshalmazokat bridge-ek (hidak) segítségével kötik össze.

Előnyei

- Sok van belőle - hozzáférhető alkatrészek,
- Viszonylag egyszerű kiépíteni,
- Egyszerű algoritmust használ,
- Új állomás menet közben is csatlakoztatható,
- Kábelezés funkciója passzív funkció,
- Kis terhelésnél szinte nulla válaszidejű.

Hátrányai

- analóg komponenseket tartalmaz,
- min 64 byte-os keret,
- nem determinisztikus (nem meghatározható a vezérléshez jutás ideje),
- nincs prioritáskezelés,
- 25 km-nél nagyobb távolság nem lehet 2 munkaállomás között.

Típusai a használt koax alapján

- **Vastag (THICK vagy Ethernet version 1)**
  Nagyobb távolság és nagyobb megbízhatóság jellemzi. Max hossz 2500 méter, max 5 szegmens max 500m szegmenshosszal, 1 szegmensre 2,5 méterenként transceiver. Összesen max 100 munkaállomás. A munkaállomás és a transceiver max távolsága 50 méter. Minden szegmens egyik végét földelni kell, kábelszegmensek végein 50W-os lezáró.
- **Vékony (THIN vagy Ethernet version 2)**
  Olcsó, egyszerűen telepíthető, azonos átviteli sebesség a vastaghoz képest. Max szegmenshossz 185 méter, hálózatonként max 5 szegmens, max kiterjedés 925 méter. 30 munkahely/szegmens, minimális kábelhossz 0,5 méter. Minden szegmens egyik végét földelni kell, kábelszegmensek végein 50W-os lezáró.
- **Kevert Ethernet hálózat**
  Az épületek között üvegszálas, az épületekben a gerincvezeték vastag Ethernet, amire multiport repeaterekkel csatlakoznak a vékony Ethernet szegmenseken található munkaállomások.

Hardware elemek

Kártya, kábel, transceiver (adó-vevõ), transceiver kábel, repeater (jelismétlő), optikai kábel, lezárók, csatlakozók, bridge.

802.3 keretformátum:

7	1	6	6	2	0-1500	0-46	4 byte
Előtag (Adó-vevő összeszinkro-nizálására)	Kerethatároló eleje (Start of Frame)	Célcím	Forráscím	Adatmező hossza	Adat	Töltelék	Ellenőrző összeg

Ethernet típusok

- 10Base2: Thin Coax,
- 10Base5: Thick Coax,
- 10Base-T: Twisted Pair,
- 10Base-F: Optical Fiber,
- 100Base-T: Twisted Pair.

2. Vezérjeles sín (Token bus): 802.4-es szabvány.

Azért alakult ki, mert a 802.3-as verziónál nem volt biztos, hogy belátható időn belül mindenki adáshoz jut. Fizikailag sín, gyakorlatilag gyűrű. A vezérjel csökkenő sorrendben megy körbe. Van prioritáskezelés. Minden állomás 4 féle csoport alállomásnak felel meg. Az állomásoknak sorszáma van, először a legmagasabb sorszámú adhat, adásjogát a vezérjel továbbküldésével adja át a következő állomásnak. Csak az adhat, aki a vezérjelet birtokolja, ütközés nem léphet fel. Időkorlátozást is használhat.

Előnyei

- Szélessávú kábelezést használ,
- Prioritásokat kezel,
- Determinisztikusabb,
- Nagy terhelésnél nem csökken az effektív átviteli képesség,
- Mehet rajta kép és hang is.

Hátrányai

- Sok analóg komponenst használ,
- Bonyolult protokoll,
- Kis terhelés jelentős késleltetést jelent,
- Optikai kábelen problémás a megvalósíthatósága.

802.4 keretformátum:

1	1	1	6	6	0-8182	4	1 byte
Előtag (Adó-vevő összeszinkronizálása)	Kezdet-jelző (analóg kódolású szimbólumok)	Keretvezérlés (adat vagy token?, prioritás)	Cél-cím	Forrás-cím	Adat	Ellenőrző összeg (CRC kód)	Végjelző (analóg kódolású szimbólumok)

3. Vezérjeles gyűrű (Token Ring): IEEE 802.5-ös szabvány.

Vételi üzemmód: 1 bitet vár. Adási üzemmód: megszakít.

Gyűrű interface: pont-pont kapcsolat van az interface-ek között. A forgalom egyirányú. A közben használt átviteli csatorna elérése azonos eséllyel történik.

1 vezérjel halad körben a gyűrű mentén, mai lényegében 1 rövid üzenet, ami utal a gyűrű foglaltságára. Csak akkor adhat valamelyik állomás, ha birtokolja a vezérjelet, azaz üresen kapta, foglaltra állítja, megtölti adatokkal, majd visszaadja a hálóba vagy kivonja a tokent a hálóból. Az üzenet a gyűrűben állomásról állomásra halad. Ha az üzenet az állomásnak szól, feldolgozza. Ha nem, továbbadja. Ha visszaért az üzenet a feladóhoz, az kivonja a gyűrűből, és szabad tokent ad körbe. Ha nem kerül az üzenet kivonásra, akkor (valamelyik) felügyelő állomás kivonja a forgalomból, és szabad vezérjelet indít körbe. Az aktív felügyelő hibája esetén valamelyik passzív felügyelő veszi át az irányítást. Prioritás is kiépíthető.

Előnyei

- bármilyen átviteli közeg lehet,
- tudja javítani saját magát,
- prioritást kezel,
- nagy teljesítménynél nagy átbocsátó képesség
- rugalmas, rövid keret.

Hátrányai

- kis terhelésnél jelentős késleltetés,
- felügyelő állomás funkció.

802.5 keretformátum:

1	1	1	6	6	korlát-lan	4	1	1 byte
SD (Start delimiter) Start-	AC Hozzáférés-vezérlés	FC Keretvezérlés (adat vagy keret?,prioritás)	Cél-cím	Forrás-cím	Adat	Ellenőrző összeg	ED (Ending delimiter) Végjelző	FS (frame status) Keret-státusz

jelző								

A vezeték nélküli IEEE 802 LAN-ok

Ismert még WiFi (wireless-fidelity) néven is, amely nem más, mint az 802.11 specifikáció brand elnevezése. A Wlan a lokális hálózat funkcióját nyújtja, de szemben azzal, nincs szükség fizikai (kábel) összeköttetésre a gépek között. Az adatátvitel a gépek (berendezések) között modulált rádiohullám segítségével történik. A Wlan sebessége tipikusan 11Mbps vagy 54Mbps. Ez elméleti adatátviteli sebesség. A gyakorlatban nagyon sok mindentől függ a maximális sebesség:

- helyszíni viszonyok
- zavarok
- a titkosítás ki/be kapcsolása a kommunikáció alatt

802.11 LAN: a rendszer cellákra van osztva. Az egyes cellákat bázisállomások irányítják, melyeket hozzáférési pontnak (AP) hívunk.
Bár egyetlen cellából is állhat a vezeték nélküli LAN, leggyakrabban néhány cellából álló rendszereket valósítanak meg, ahol a hozzáférési pontok valamilyen gerinchálózaton, elosztó rendszeren keresztül kapcsolódnak egymáshoz.

A szabvány két különböző rádiófrekvencia modulációs sémát tartalmaz: a **közvetlen sorrendes szórt spektrumú rádiós összeköttetést (DSSS – Direct Sequence Spread Spectrum)** és a **frekvenciaugrásos szórt spektrumú rádiós összeköttetést (FHSS – Frequency Hopping Spread Spectrum)**. Mindkét változatot a hadsereg tervezte megbízhatóságuk, csorbíthatatlanságuk és biztonságosságuk miatt. Mindkét típusnak saját adattovábbítási módszere van.

Az ***FHSS*** a frekvenciatartományt 7 csatornára osztja. Keskeny sávú hordozóhullámot alkalmaz, amely folyamatosan változik egy 2-4 szintes Gauss-féle frekvenciaváltó kódsorozat alapján. Más szóval, az adatátvitel frekvenciája folyamatosan pszeudovéletlen módon változik, amit mind az adó, mind a vevőállomás ismer. Ez egy elég biztonságos módszer. Illetéktelenek valószínűleg nem tudhatják, hogy mikor melyik frekvenciára váltsanak ahhoz, hogy a teljes adatfolyamot megkaphassák. Az FHSS másik előnye, hogy ugyanazon fizikai térben egyszerre több hálózat működhet párhuzamosan.

A ***DSSS*** más módszert használ. A DSSS az adatfolyamot egy nagyobb sebességű digitális kóddal kombinálja. Minden egyes adatbitet olyan mintába ágyaz, ami csak az adó- és a kívánt vevőállomás által ismert. Ezt a bitmintázatot „forgácskódnak" (chipping code) nevezik. Ez a kód magas és alacsony jelek véletlen sorozata, amelyek az éppen aktuális bitet jelentik. Ezt a „forgácskódot" invertálják, hogy az adatfolyam ellenkező bitjét jelölje. Ez a frekvenciamodulálás, amennyiben az átvitelt jól szinkronizálták, magában foglalja saját hibajavítását is, így ez a módszer jobban elviseli az interferenciákat.

802.11a : Az első nagysebességű vezeték nélküli LAN, a **802.11a** az **OFDM (Orthogonal Frequency Division Multiplexing – Ortogonális Frekvenciaosztásos Nyalábolás)** eljárás segítségével akár 54 Mb/s-os átvitelre is képes a szélesebb, 5 GHz-es ISM sávban. Ahogy az FDM rövidítés is jelzi, itt különböző frekvenciákat használnak, mégpedig 52-t, ebből 48-at az adatok számára, 4-et pedig a szinkronizációhoz – ez az ADSL-re emlékeztet. Mivel egyidejűleg több frekvencián is történik átvitel, az eljárás eltér a CDMA-tól és az FHSS-től, bár szintén a szórt spektrum egy változatának tekinthető. A bonyolult kódolási rendszer 18 Mb/s-ig fázisbillentyűzésen, onnantól kezdve pedig a QAM-en alapszik.

802.11b : Következő eljárásunk a **HR-DSSS (High Rate Direct Sequence Spread Spectrum – Nagysebességű közvetlen sorozatú szórt spektrum)**. Ez egy újabb szórt spektrum eljárás, mely 11 millió chip/s segítségével éri el a 11 Mb/s-ot a 2,4 GHz-es sávban. **802.11b**-nek is nevezik, de ez nem jelenti azt, hogy a 802.11a utódja lenne – valójában ezt a szabványt fogadták el elsőként, és piacra is előbb került. 4 átviteli sebességet támogat: 1, 2, 5,5, és 11 Mb/s-ot. A két kisebb sebesség 1 Mbaud-on működik, baudonként 1, ill. 2 bittel, és fázisbillentyűzést használ (a DSSS-sel való kompatibilitás miatt). A két nagyobb sebesség 1,375 Mbaud-on működik, 4, ill. 8 bittel baud-onként. A 802.11b működési sebessége a gyakorlatban szinte mindig 11 Mbit/s. A 802.11b lassabb ugyan a 802.11a-nál, de 7-szer nagyobb működési tartománnyal rendelkezik, ami sok esetben fontos lehet.

802.11g: egy kiegészítése a 802.11b-nek. A 802.11g megnöveli a 802.11b adatátviteli sebességét 54 Mbps-ra, miközben a frekvencia marad 2.4 GHz. A moduláció OFDM technológián alapul. A 802.11b-s kártyák képesek együttműködni a 802.11g-s hozzáférési pontokkal (access point) és viszont. Tipikus hatótávolság: 54 Mbps sebesség mellett 15 m, 11 Mbps sebesség mellett 45 m.

802.11n

	Megjelenés éve	Frekvencia tartomány	Adatsebesség (tipikus)	Adatsebesség (maximum)	Hatótávolság (épületben)
802.11	1997	2,4GHz	1 Mbit/s	2 Mbit/s	<30 m
802.11a	1999	5 GHz	25 Mbit/s	54 Mbit/s	30 m
802.11b	1999	2,4GHz	6,5 Mbit/s	11 Mbit/s	50 m
802.11g	2003 jan.	2,4GHz	25 Mbit/s	54 Mbit/s	30 m
802.11n	**2007/08 ?**	**2,4 vagy 5 GHz**	**200 Mbit/s**	**540 Mbit/s**	**50 m**

A Wireless N szabvány természetesen kompatibilis Wireless A, Wireless B, és a Wireless G szabványokkal, de ha két Wireless N berendezést kapcsolunk össze, akkor akár 12-szer gyorsabb eredményt kaphatunk a Wireless G szabványhoz képest. Alkalmas médiaalkalmazásokhoz, használhatjuk játékra, online videózásra, VOIP célokra. A szabvány OFDM-et használ.

Sajnos van egy-két megoldatlan probléma a 802.11-es szabványnál. A szabvány célja a standardizálás és a kereszt-működőképesség, mégis hiányzik belőle néhány olyan dolog, amely kulcsfontosságú a több-forgalmazós (multiple-vendor) kereszt-működőképesség eléréséhez. Például a mozgás (roaming) közbeni hozzáférési pont koordináció – a szabvány nem tartalmaz automatikus mechanizmust arra az esetre, ha valaki az egyik AP hatósugarából átsétál a másikéba. Ezen kívül nincs előírás az olyan tesztekre, melyekkel, meg lehetne állapítani, hogy egy adott eszköz megfelel-e a szabványnak, vagy sem.

A 802.11 keretszerkezete:

Keretvezérlés	Időtartam	1. cím	2. cím	3. cím	Sorszám	4. cím	Adat	Ellenőrző összeg

A 802.11 szabvány 3 különböző keretosztályt definiál: adat-, vezérlő- és menedzsment kereteket. Mindegyiknek saját fejrésze van, különböző mezőkkel, melyeket a MAC-alrétegben használnak.

IEEE 802.15.1, az IEEE-féle Bluetooth

A Bluetoothról röviden annyit érdemes tudni, hogy egy olyan adatátviteli technológia, mely a különféle elektronikus eszközök közötti adatfolyam biztosítására hivatott, mégpedig oly módon, hogy működéséhez minden fajta vezetéket nélkülöz. A Bluetooth technológiát lényegében azért fejlesztették ki pár éve, hogy segítségével minden korábbinál könnyebben és zökkenő mentesebben lehessen összekapcsolni pl. egy mobiltelefont és egy hordozható számítógépet, vagy egy kézi számítógépet és egy nyomtatót, de az ilyen és ehhez hasonló felhasználási köröket még sokáig lehetne sorolni.

A rendszer alapegysége a **pikohálózat (piconet)**, mely egy mester (master) csomópontból és legfeljebb hét darab, 10 méteres távolságon belül levő aktív szolga (slave) csomópontból áll. Ugyanabban a (nagyméretű) helységben több pikohálózat is lehet egyszerre, sőt egy híd-csomópont révén össze is lehet kötni azokat. Az egymással összekötött pikohálózatok gyűjteményét **szórt hálózatnak (scatternet)** is nevezzük. A pikohálózat hét aktív szolga csomópontja mellett legfeljebb 255 várakozó (parked) csomópont lehet a hálózatban.

A bluetooth rádiós rétege

A rádiós réteg a biteket szállítja a mestertől a szolgáig vagy fordítva. Ez egy alacsony teljesítményű rendszer, 10 méteres hatósugárral, a 2,4 GHz-es ISM-sávban. A sáv 79 darab, egyenként 1 MHz-es csatornára van osztva. Modulációs eljárásként frekvenciabillentyűzést használnak. A Hz-enkénti 1 bit kiadja a bruttó 1 Mb/s-os adatsebességet, de ezen átviteli kapacitás jó részét a járulékos információk viszik el. A csatornák igazságos szétosztásához frekvenciaugrásos szórt spektrumot alkalmaznak másodpercenként 1600 ugrással és 625 microsec tartózkodási idővel. A pikohálózat összes csomópontja egyszerre végzi az utasításokat, az ugrási sorozatot pedig a mester diktálja.

A 802.15 keretszerkezete:

Hozzáférési kód	Fejrész (Cím, Típus, F, A, S, Ellenőrző összeg)	Adatmező

IEEE 802.16 és 802.16a

Elsősorban a ritkábban lakott területeken lehet népszerű az a WiMAX drótnélküli szabvány, amely közel 50 km-es hatótávolságot ígér, és elérést biztosít a DSL, illetve kábeles hozzáféréssel nem rendelkező felhasználók számára.

A WiMAX névvel illetett IEEE 802.16 és 802.16a szabványok közel 25 kilométeres hatósugárral rendelkeznek, legnagyobb elérhető adatátviteli sebességük pedig 70 Mbps, amelyen a hálózatra kapcsolódó felhasználóknak osztozniuk kell. A 802.16a változat a 802.16 módosított változata, amelyet az IEEE a közelmúltban fogadott el. A

módosított specifikáció az eredeti 10 GHz – 56 GHz-es tartománnyal szemben a 2 GHz – 11 GHz –es frekvenciasávot használja, lehetővé téve ezzel a Wi-Fi csomópontok létesítését is a WiMAX hálózaton belül.

A 802.11 és a 802.16 bizonyos mértékig hasonló környezetben működnek, főleg abban a tekintetben, hogy mindkettőt nagy sávszélességű vezeték nélküli kommunikációra tervezték. Vannak azonban köztük fontos különbségek is. Először is, a 802.16 épületek számára nyújt szolgáltatásokat, márpedig az épületek nem mozognak, legalábbis nem mondhatjuk el azt, hogy túl gyakran vándorolnának egyik cellából a másikba. A 802.11 nagy része a mozgással foglalkozik, annak pedig itt nincs jelentősége. Másodszor, az épületekben egynél több számítógép is lehet, ilyen bonyodalmak viszont nem lépnek fel ott, ahol a célállomást egyetlen hordozható számítógép jelenti. Az épületek tulajdonosai ugyanakkor sokkal több pénzt tudnak áldozni a kommunikációs eszközökre, mint a hordozható számítógépek tulajdonosai, ezért itt jobb rádiókat is lehet alkalmazni. Ez azt jelenti, hogy a 802.16-nál duplex kommunikáció használható – erről a 802.11-nek le kellett mondania, hogy alacsonyan tarthassa a rádiók költségét.

A 802.16 egész városrészeket, vagyis több km-es távolságokat ível át, ezért a bázisállomáson vett jel teljesítménye a különböző adók esetében erős szórást mutathatnak. A 802.16a szabvány a 2-től 11 GHz-ig terjedő sávban fogja támogatni az OFDM-et, a 802.16b pedig az 5 GHz-es ISM sávban fog működni. Mindkét elgondolás a 802.11-hez való közeledéshez tesz kísérletet.

A 802.16 keretszerkezete:

0	E C	Típus		C I	EK		Hossz	Összeköttetés - azonosító	Fejrész CRC	Adatmező	CRC

Hálózatok összekapcsolásának eszközei és problémái

1. Repeater (jelismétlő)

Az ismétlő egy fizikai rétegbeli eszköz, amely mindkét irányból veszi, felerősíti és továbbítja a jeleket. ***Jelismétlő*** ez egy erősítő, jelformáló és újraütemező funkcióval ellátott eszköz, melynek célja, hogy kiterjesszék a kábelezhető távolságot. Garantálni kell, hogy a jel torzulása esetén még máshol vehető legyen. Az Ethernetnél 185 m, optikainál 30 km hosszú kábelnél garantálják a hibátlan jelvételt, ha távolabbra akarok menni, akkor kell alkalmazni a jelismétlőt (R), ami veszi a jelet, nem csinál vele semmit, de a kimenetén szabályos jelalakban és erősségben újra kibocsátja. Ethernet: 1 szegmensen max. 30 számítógép lehet, repeater ezt lehet sokszorozni. Egy kommunikációs csatornában csak két repeater lehet. A legolcsóbb és legbutább hálózati elem.

- jelerősítés, újraformázás és újraidőzítés a kábelezhető távolság kiterjeszthetősége érdekében
- kapcsolat az 1. (fizikai) rétegen
- nincs módosítás a hozzáférési protokollon
- az átviteli közeg változtatásának lehetősége
- gyenge biztonsági tulajdonságok
- a repeaterek számát a felső rétegek korlátozzák.

2. Bridge (híd)

A LAN-okat lehet vele összekapcsolni. Az adatkapcsolati rétegben működő eszköz. A hidak az adatkapcsolati rétegbeli címeket vizsgálják meg, hogy elvégezhessék a forgalomirányítást.

Olyan eszköz, mely a 2. (adatkapcsolati) rétegen kínál összeköttetési lehetőséget a különböző hozzáférési protokollok és médiák között. A bemenetén megjelent jelet átalakítja a kimenetén lévő hálózat szabályainak megfelelően. A bridge sokszor célszámítógép. Szórja az üzenetet, elviszi az információt olyan hálózatra is, ahová nem kellene, zaj keletkezik. Célszerű bizonyos részterületek szükségleteit ellátó, azonos típusú hálózatokat úgy egyesíteni, hogy belső forgalmuk elkülönüljön egymástól. Ez a logikai kapcsolatvezérlés szintű címek strukturálásával, közvetítőként híd alkalmazásával oldható meg.

- kapcsolat a különböző hozzáférési protokollok között
- csomagszétbontás és összeállítás
- nincs útvonal optimalizálás
- gyenge biztonsági tulajdonságok
  - -ha szakadás van a hálózatban nem tud alternatív útvonalat találni
  - - Csomagütközések

3. HUB (Elosztó)

Az egyik portjukon vett keretet bitről bitre átmásolják a másik portjukra, mintegy meghosszabítva ezzel az elektromos jellemzők miatt rövidre korlátozott szegmenst.

Problémái: - Csomagütközések.

4. Switch (kapcsoló)

A kapcsolók csak a megfelelő, címzett állomásnak küldik ki az érkező keretet, logikai kapcsolást hajtva végre. Ezek tulajdonképpen multiport bridge-ek. Képesek nem blokkoló módon továbbítani a kereteket. Problémái:

- nincs útvonal optimalizálás
- ha szakadás van a hálózatban nem tud alternatív útvonalat találni
- gyenge biztonsági tulajdonságok.

5. Router (forgalomirányító)

Router (elosztó-irányító): olyan eszköz, mely a 3. (hálózati) rétegen kínál kapcsolatot, melyek ugyanazt a protokollt használják. Legdrágább, ellátja a bridge összes funkcióit. Ha bemenetén van információcsomag, csak azon a kimenetén engedi ki ahol a címzett van, ha kell konvertáltan. A routerek egymással is képesek hálózatot alkotni. (A router forgalomirányításra képes, fel tudja mérni, ha több útvonal lehetséges) → szakadás esetén át tudja szervezni a forgalmat. Csomagot kap, megnézi a fejlécét, irányítási döntést hoz arra vonatkozóan, hogy kell-e továbbítani vagy sem. Problémái:

- megtalálja az optimális útvonalat, viszont ehhez hálózati forgalmat generál
- Lassabb, mint a többi eszköz
- Drága
- Üvegszálas hálózatoknál meg eléggé bonyolult.

6. Gateway

Gateway: olyan eszköz, mely a teljesen különböző hálózatok és architektúrák összekapcsolását teszi lehetővé a szállítási vagy alkalmazási rétegben

- lényegében mind a 7 réteg támogatása

- jelentős fejlesztési költség

a teljesítmény problematikussá válhat

Olyan eszköz, mely a teljesen különböző hálózatok és architektúrák összekapcsolását teszi lehetővé. Problémái:

- jelentős fejlesztési költség
- a teljesítmény problematikussá válhat.

Z1/8 A hálózati réteg feladatai. Forgalomirányító algoritmusok. Legrövidebb útvonal alapú algoritmus, elárasztás, távolságvektor alapú forgalomirányítás, kapcsolatállapot alapú forgalomirányítás, hierarchikus forgalomirányítás

A hálózati réteg feladatai (Network layer)

Hálózati réteg (network layer): a kommunikációs alhálózatok működését vezérli (útvonalkeresés, címzési módok, torlódáskezelés). A két végpont közti kapcsolat lebonyolítása és a torlódás elkerülése a feladata, tehát a keretek vevőtől célba való juttatásának optimális útvonalának kiválasztása. Eltérő lehet a hálózatok címzési módszere, különbözhetnek a maximális csomagméreteik és protokolljaik is. E problémák megoldásáért, azaz a heterogén hálózatok összekapcsolásáért a hálózati réteg a felelős. Üzenetszórásos hálózatokban az útvonal-kiválasztási mechanizmus igen egyszerű, így a hálózati réteg általában vékony, sokszor nem is létezik.

Forgalomirányító algoritmusok

Routing feladata a csomagok hatékony (gyors) célba juttatása, illetve útvonal kijelölése a forrástól a célig. Mivel az IMP-k kapacitása véges, torlódás alakulhat ki valamelyik előtt.

Vonalkapcsolt hálózatoknál az útvonal kijelölése a hívás fázisában történik, csomagkapcsolt esetében minden egyes csomagra külön-külön, vagy egy adott útvonalon egy sorozat csomag megy át. Az IMP-nek tehát routing táblákat kell tartalmaznia, ahol a vele kapcsolatban álló más csomópontokra vonatkozó adatok vannak bejegyezve.

A forgalomirányító algoritmusok osztályozásának alapjául a következő négy irányítási főfunkciót tekinthetjük:

- vezérlésmód (hogyan történjen?)
- döntésfolyamat (milyen esetben kell?)
- információ-karbantartó folyamat (hálózati forgalmi ismeretek frissítése)
- továbbító eljárás (hogyan jut el a vezérlési információ a csomópontokhoz)

A forgalomirányító algoritmusoknak két osztálya van: az adaptív (alkalmazkodó), a hálózati forgalomhoz igazodik, és a determinisztikus (előre meghatározott), ahol az útvonal választási döntéseket nem befolyásolják a forgalom mért vagy becsült értékei.

Fontos mindig a legrövidebb út meghatározása.

A forgalomirányító algoritmusoknak két osztálya van:

- az **adaptív** (alkalmazkodó), a hálózati forgalomhoz igazodik,
- a **determinisztikus** (előre meghatározott), ahol az útvonal választási döntéseket nem befolyásolják a forgalom mért vagy becsült értékei.

Ezek alapján 4 lehetséges vezérlésmód különböztethető meg:

1. Determinisztikus forgalomirányítás

Olyan rögzített eljárás, amelyet a változó feltételek nem befolyásolnak. Rögzített eljárás, a hálózati forgalomhoz nem alkalmazkodik.

a. Véletlen forgalomirányító eljárás

Itt a csomagok nagy hálózat esetében előfordulhat, hogy csak bolyonganak, mert „véletlenül” kiválasztott útvonalával nem jut el a célig.

b. Elárasztásos forgalomirányító eljárás

A bejövő csomagot a csomópont minden kimenő vonalra elküldi. A csomag 1 példánya biztos, hogy a legrövidebb útvonalon ér a célba. A lépések száma korlátozva van. A sokszorosítás lassítja a hálózatot. Megbízható.

2. Elszigetelt adaptív

Minden csomópont hoz irányítási döntéseket, de csak helyi információk alapján. Helyi forgalmi információk alapján irányít

a. „Forró krumpli” algoritmus

A csomagot a legrövidebb elérésű vonalra helyezi.

b. Fordított tanulás módszere

A csomagon van egy indító állomást azonosító, s egy számláló jel. Az IMP-k növelik a számláló értékét, a célállomás így kapni fog egy útvonal hosszt az indító állomás távolságáról. Ha másik útvonalon is érkezik ugyanonnan csomag, a célállomás az optimálisabb útvonalat tartja meg.

3. Elosztott adaptív

Helyi és más csomópontoktól kapott információk alapján irányít. A csomópontokban táblázatok vannak, hogy csomópontok milyen távolságban vannak tőle, ez kezdeti értéknél a topológia alapján egy becsült érték, csomagküldés után már valós érték lesz. A csomagot tehát a táblázatban a cél felé mutató legrövidebb elérésű útvonalon küldi el.

4, Központosított adaptív

Egy közös irányító központ vezérli az irányítást . A rendszer lelke a forgalomirányító központ (RCC – Routing Control Center). A csomópontok ide küldenek helyzetjelentéseket, s így egy átfogó kép alakul ki a hálózati forgalomról. A csomópontokhoz a központ legrövidebb útvonal táblákat küld vissza.

Legrövidebb útvonal alapú forgalomirányítás

Két adott router közötti útvonal kiválasztásához az algoritmus egyszerűen a köztük levő legrövidebb utat keresi meg a gráfban. Egy út hoszszát mérhetjük a megtett ugrások számával, a földrajzi távolsággal és még sok egyébbel. Például mindegyik él súlya lehetne egy szabványos tesztcsomagra vonatkozó átlagos sorbanállási és átviteli késleltetés, amelyet óránkénti próbafuttatásokkal mérnénk. Ezzel az élsúlyozással a legrövidebb út a leggyorsabb út lesz, a legkevesebb kilométerű vagy legkevesebb élből álló helyett. Számos algoritmus ismert egy gráf két csomópontja közti legrövidebb út kiszámítására, egy példa a Dijkstra algoritmus.

Távolságvektor alapú forgalomirányítás

Dinaminkus algoritmus. A távolság alapú forgalomirányítás (distance vector routing) alapja, hogy minden kapcsolóelem egy táblázatot tart fenn, amelyben minden célponthoz eltárolják a hozzá vezető legrövidebb útvonalat, valamint azt, hogy melyik annak a vonalnak az azonosítója, amelyen keresztül elérhető a célpont. A megoldás nem használható semmire, ha a szomszédos csomópontok nem tudnak egymás táblázatairól semmit, éppen ezért egymás között megadott időközönként frissíteniük kell a táblázatokat. A táblázat alapján képesek a kapcsolóelemek megkeresni a legoptimálisabb útvonalat. Van egy nagyon érdekes tulajdonsága ennek a módszernek. Az, hogy a kedvező változások a hálózatban gyorsabban terjednek, mint a kedvezőtlenek.

Kapcsolatállapot alapú forgalomirányítás

Bővebben: http://prog.hu/cikkek/211/Forgalomiranyitas+a+halozati+retegben+2/oldal/3.html

Működési elve:

1, Kutassa fel a szomszédait, majd meg kell szereznie a hálózati címeiket.
Hello csomag küldése. Válasz pedig a kapcsolódó pontok azonosítója.

2, Minden szomszéd irányába meg kell mérnie a késleltetést, valamint ki kell számítania a költségeket.

3, Össze kell állítani egy csomagot, amely tartalmazza az eddig beszerzett információkat.

4, Ezeket a csomagokat el kell küldeni minden egyes kapcsolóelemnek.

5, Ennek alapján ki kell számítani az összes kapcsolóelemhez vezető legrövidebb út irányát, valamit késleltetését.

Hierarchikus forgalomirányítás

Ennek a lényege, hogy forgalomirányító csomópontokat tartományokra (regions) osztjuk fel. Minden forgalomirányító tudja, hogy milyen módon irányítsa a saját tartományában közlekedő csomagokat, de a többi tartomány szerkezeti felépítéséről mit sem tud. Ilyen módon működik a telefonhálózat is. Kialakulásának oka a hálózatok növekvő mérete okozta erőforrásigény növekedés.

Z1/9, A torlódás problémája. Torlódásvédelmi lehetőségek és módszerek. Lyukas vödör, vezérjeles vödör algoritmus, pufferelés, lefojtó csomagok, eltávolítási lehetőségek.

A torlódás problémája

Torlódás (congestion): Az a helyzet, amikor a fogadó állomások és csomópontok bemeneti várakozási sorai megtelnek.

Erősebb változata a **befulladás** (lock-up): mikor bizonyos információfolyam végleg leáll.

A valószínű ok, a kimenő vonalak viszonylagos lassúsága a bemenő vonalakhoz képest A torlódás a hálózat bénulásához vezethet, ezt el kell kerülni.

Stratégiák:

1. Pufferek foglalása

Virtuális áramkörök esetén használható, az IMP-k csak akkor fogadnak újabb csomagot, ha van szabad puffer-ük (tárolóterületük).

2. Csomageldobásos módszer

Datagram szolgálatnál, ha nincs szabad puffer a befogadásra, nem várakoztatjuk, hanem eldobjuk. Amennyiben nyugtázott csomagokat is használunk, akkor ezeknek célba juttatása fontos, ezek részére külön puffer tartható fenn, minden mást eldobhat.

3. Izometrikus torlódásvezérlés

Mivel a hálózaton jelenlévõ túl sok csomag okozza a torlódást, ezért célszerû a csomagok számát korlátozni. Ezt úgy lehet megtenni, hogy a hálózatban engedélycsomagok járnak körbe. Ha egy IMP adni kíván, egy ilyen engedélyt kell vennie, és annak továbbadása helyett egy adatcsomagot küldhet tovább. Mivel a hálózatban az engedélyek száma korlátozott, így az ezeket helyettesítõ csomagok száma is korlátozva lesz. Persze ez nem garantálja, hogy egy IMP-t ne árasszanak el csomagok.

4. Lefojtó csomagok használata

Csak akkor kezdik korlátozni az adást, amikor torlódási veszély van. Az IMP-k figyelik a kimeneti vonalainak átlagos kihasználtságát, és ezt mindig újraszámítja a pillanatnyi vonalkihasználtságát és egy 0 és 1 közötti felejtési tényező alapján. Ha ez az értéke átlép egy küszöböt, akkor a kimeneti vonal „figyelmeztetés” állapotba kerül. Ha egy csomagot erre kell továbbküldeni, akkor elküldi, de közben a forráshelyre egy lefojtó csomagot küld, hogy visszafogja az ilyen irányba menő forgalmat.

A vezérjeles vödör algoritmus (Token Bucket Filter)

Ez egy egyszerű sorbanállási módszer, amelyben az érkező csomagokat egy előre meghatározott mértékben engedi át, de lehetőséget ad rövid tüskékre, amikor az előre meghatározott sebességet (rate) át lehet lépni. A TBF meglehetősen pontos, emellett hálózat- és processzor barát. Ez lehet az első szóba jöhető választás, amikor le szeretnénk lassítani egy hálózati eszköz kimenő forgalmát. A TBF megvalósítása: puffer (vödör), állandóan kitöltve néhány információs darabbal (vezérjel – token), ez egy bizonyos sebességgel (rate) rendelkezik. A puffer másik legfontosabb paramétere a mérete, ennyi jelet tud eltárolni.Minden egyes vezérjel egy bejövő csomagot gyűjt be, és ezután törlődik a vödörbő

Lyukas vödör algoritmus

A lyukas vödör algoritmus a terhelés egyenletességét javítja.

A vödörből viszonylag egyenletesen kerülnek ki a csomagok még akkor is, ha lökésszerűen kerül felöltésre. Ha a hálózatra a csomagokat egyenletesen tesszük fel számottevően csökken a torlódásveszély.

Az algoritmus minden "óraütésre" egy csomagot zúdít a "vödörbe" mindaddig, míg van szabad puffer. Ha nincs szabad puffer, akkor a töltési folyamatot várakoztatjuk.

A folyamat jól működik, ha a csomagok nagyjából egyforma hosszúak. Változó csomaghossz esetén az egyszerű algoritmus nem megfelelő. Célszerű óraütésenként nem egy csomagot, hanem egy meghatározott számú bájtot helyezni a vödörbe.

Terhelés eltávolítás

A csomagok egy részét egyszerűen eldobjuk. Nem mindegy azonban , hogy mit dobunk el, mert a csomagok nem egyenértékűek. Ha egy csomag ráültetett nyugtát tartalmaz nem célszerű eldobni, mert nem csak az eldobott csomagot, hanem azt is meg kell ismételni, aminek a nyugtáját eldobtuk. A régi csomag valószínűleg

értékesebb, mert sok algoritmus az első meg nem érkezett csomagtól újraadja a mögötte lévő összes csomagot. Jó lenne, ha lennének kevésbé fontos csomagjaink.

A felhasználót érdekeltté tehetjük, hogy osztályozza a csomagjait, ha a "soha ne dobd el" csomagokhoz képest alacsonyabb tarifával szállítjuk az alacsony prioritású csomagokat. Valószínű, hogy az alacsony prioritású csomagok eldobásával a hálózat működése helyreállítható.

Az alacsony prioritású csomagok így később kerülnek továbbításra, a magasabb prioritásúak pedig valószínűleg biztonságosabban érnek célba.

Z1/10 A szállítási réteg feladatai, a szállítási szolgálat és a szállítási protokollok elemei.

A szállítási réteg (Transport layer)

Szállítási réteg (transport layer): alapvető feladata a hostok közötti átvitel megvalósítása, vagyis az, hogy adatokat fogadjon a viszonyrétegtől, kisebb darabra vágja szét azokat (ha szükséges), majd adja tovább a hálózati rétegnek és biztosítsa, hogy minden darab hibátlanul megérkezzék a másik oldalra. Továbbá, mind ezeket hatékonyan kell végrehajtania, ráadásul oly módon, hogy a viszonyréteg elől el kell fednie a hardvertechnikában elkerülhetetlenül bekövetkező változásokat (hibamentes szállítás a dolga). Fontos feladata még a címzések kezelése.

A szállítási szolgálat

A szállítási réteg legfőbb célja az, hogy hatékony, megbízható, és gazdaságos szolgálatot nyújtson a felhasználóinak, általában az alkalmazási rétegben futó folyamatoknak. E cél érdekében a szállítási réteg felhasználja a hálózati réteg által nyújtott szolgálatokat. A szállítási rétegen belül azt a hardver és/vagy szoftver elemet, amely a munkát végzi, szállítási funkcionális elemnek vagy szállítási entitásnak nevezzük.

Ez lehet az operációs rendszer magjának (kernelének) része, önálló felhasználói folyamat, egy hálózati alkalmazáshoz tartozó könyvtár vagy a hálózati illesztő kártya.

Sokan elkülönítik az 1-4. és az 5-7. rétegeket. Az alsó 4 réteget együttesen a **szállítási szolgáltatónak (transport service provider)**, míg a felső hármat a **szállítási szolgálat felhasználójának (transport service user)** tekintik.

A szállítási réteg vizsgálatának másik szempontja az, hogy elsődleges feladatának a hálózati réteg által nyújtott **QoS (Quality of Service - szolgálatminőség)** javítását tekintjük. Ha a hálózati réteg tökéletes, a szállítási rétegnek könnyű dolga van. Ha viszont a hálózati szolgálat gyenge, akkor a szállítási szolgálatnak kell áthidalni a szállítási szolgálatot igénylők elvárása és a hálózati réteg képessége közötti szándékot. Hálózatok és hálózati eszközök képessége az erőforrások meghatározott rend szerinti felosztására, és garantált sávszélesség biztosására. A QoS-t támogató hálózatokon a magas prioritású üzenetek előnyben részesíthetők alacsonyabb besorolású társaikkal szemben, és konkurrencia-helyzetben előbbiek továbbítása utóbbiak feltartóztatásával garantált sebességen biztosítható.

A QoS meghatározott paraméterekkel jellemezhető, ezek:

- *összeköttetés-létesítési késleltetés:* az-az idő, amely a szállítási összeköttetés igénylése és a beérkező megerősítés között eltelik
- *összeköttetés-létesítési hibavalószínűség:* paraméter annak az esélyét jelenti, hogy az összeköttetés nem jön létre a maximális összeköttetés-létesítési késleltetés miatt.
- *átbocsátóképesség:* paraméter a másodpercenként átvitt felhasználói adatbájtok számát mutatja valamilyen időtartam alatt mérve
- *átviteli késleltetés:* a forráshost szállítási felhasználója üzenetének elküldése, a célhost szállítási felhasználójának üzenetvételi időpontja között eltelt időt adja meg
- *maradó hibaarány:* az elveszett vagy sérült üzenetek számának aránya az összes elküldött üzenetek számához képest
- *védelem:* paraméter lehetőséget biztosít a szállítási felhasználónak, hogy a szállítási rétegtől meghatározott fokú védelmet igényeljen jogosulatlan harmadik fél (támadó) által végzett lehallgatás vagy adatmódosítás ellen
- *prioritás:* paraméter segítségével a szállítási felhasználó jelezheti a szállítási rétegnek, hogy némely összeköttetése fontosabb másoknál, és torlódás esetén a magasabb prioritású összeköttetéseket hamarabb szolgálja ki, mint az alacsony prioritásúakat
- *rugalmasság:* paraméter annak a valószínűségét mutatja, hogy maga a szállítási réteg szakítja meg az összeköttetést valamilyen belső hiba vagy torlódás miatt.

Kétféle szállítási szolgálat létezik:

- **Összeköttetés alapú szállítási szolgálat:** három fázisa van az összeköttetésnek: létesítés, adatátvitel és lebontás.
- **Összeköttetés nélküli szállítási szolgálat**

A szállítási réteg létezése lényegében azt teszi lehetővé, hogy a szállítási szolgálat megbízhatóbb lehessen annál a hálózati szolgálatnál, amelyre épül. A szállítási réteg képes felfedezni és kiegyenlíteni az elveszett csomagok és a csonkolt adatok okozta hibákat. Mindezen felül a szállítási szolgálat primitívjei könyvtári

függvényhívásokként is megvalósíthatók, és ezzel függetleníthetők a hálózati szolgálat primitívjeitől.

A szállítási protokollok elemei

A szállítási szolgálatot, egy a szállítási entitások között használt szállítási protokoll valósítja meg. Többek között a hibakezelést, sorszámozást, és forgalomszabályozást kell végeznie.
A szállítási rétegben a fizikai csatorna helyett az egész alhálózat szerepel.

- **Címzés:** A szállítási rétegben a cél explicit címzése kötelező. Amikor egy alkalmazási folyamat egy távoli alkalmazási folyamattal akar összeköttetést létrehozni, meg kell jelölnie, hogy melyik folyamattal akar kapcsolatba lépni. Az általánosságban használt módszer az, hogy külön szállítási címeket definiálunk az egyes folyamatok részére. Az Interneten ezeket a végpontokat portoknak hívják. Mi a TSAP (Szállítási Szolgálatelérési Pont) kifejezést használjuk. Az ezzel rokon végpont az NSAP (Hálózati Szolgálatelérési Pont). Kezdeti összeköttetés-protokoll (Initial Connection Protocol): Minden olyan gépnek van egy folyamatszervere (process server), amely szolgálatokat akar felkínálni a távoli felhasználóknak. Több portot figyel egyszerre összeköttetési kérésekre várva. Ha ezt már nem lehet létrehozni, akkor egy névszolgáltató folyamat működik.
- **Összeköttetés létesítés:** Háromutas kézfogás módszer: Ennél a módszernél az adó és a vevő más-más sorszámmal kezdi meg az adását, így a szinkronizálás a globális időtől eltérően is megvalósítható.
- **Összeköttetés bontása:** Aszimmetrikus és szimmetrikus módon lehet. Az aszimmetrikusnál elég csak az egyik oldalon bontani a vonalat. A szimmetrikusnál külön kell mindkét oldalon bontani a kapcsolatot.
- **Pufferelés és forgalomszabályozás:** Az alhálózat adattároló képességének következménye néha katasztrofális lehet, és speciális protokollok használatát teszi szükségessé.
- **Nyalábolás:** - Feltöltési multiplexelés: Felfelé nyalábolás,
- **Letöltési multiplexelés:** Lefelé nyalábolás.

Z1/11 Az Interneten használt protokollok, TCP/IP felépítése,IP, IP címzés, vezérlő protokollok

Az Interneten használt protokollok

Az Interneten leggyakrabban használt protokollok a TCP és az UDP. Ezek a leghasznosabbak számunkra, segítségükkel érjük el a létező összes szolgáltatást (FTP, HTTP, stb...), feladatuk kommunikációs csatornát biztosítani.

Egyéb protokollok: SMTP, POP3, IMAP, SIMAP, FTP, HTTP, NNTP, stb…

Az Internet szállítási rétege: a TCP

A TCP fogadja a tetszőleges hosszúságú üzeneteket a felhasználói folyamattól és azokat max 64kB részekre bontja, fejlécet fűz hozzá és csomagokként továbbítja a hálózati réteg felé. Nem ennek a rétegnek a feladata a datagrammok (adatcsomagok) helyesen és megfelelő sorrendben történő továbbítása, hanem az időzítéseket figyelve újra kell küldenie a csomagokat, illetve a kapott adatokat helyes sorrendben eredeti üzenetté alakítani. A TCP a pozitív nyugtázást használja, hiánya esetén újraküld. A küldés pillanatában elindul egy időzítő. 204 oldal

Az Internet hálózati rétege: az IP

A protokoll megbízhatatlan összeköttetés-mentes szolgálatot biztosít, a megbízhatósági mechanizmusokat a szállítási rétegben kell megvalósítani. Az IP definiálja a az adatátvitel legkisebb egységét, pontos formáját, az útválasztást, valamint néhány további olyan fontos szabályt, amelyek meghatározzák, hogy a hostok, IMP-k hogyan dolgozzák fel az IP csomagokat, mikor és hogyan kell hibajelzéseket generálni, mikor kell a csomagot eldobni. 207 oldal

Az IP csomagokat gyakran tördelni (fregmentálni) kell, mert a hálózatra jellemző maximális adatátviteli méret ezt szükségessé teszi. A kapott fragmenteknek 8 bájttal oszthatónak kell lennie, s csak a célhelyen egyesítődnek.

TCP/IP felépítése

A TCP/IP protokoll alapvetően az OSI modell két rétegének a funkcióját valósítja meg: ez a hálózati és a szállítási réteg.

A hálózati modell 4 rétegből áll:

1. Hálózat elérési

Az OSI modell 2 alsó szintjének felel meg, és ez biztosítja a kapcsolatot a csomópontok között (pl.: Ethernet, Token Ring, token Bus).

2. Hálózati réteg

Ez a réteg végzi a csomagok útvonal kijelölését a hálózatok között. Ennek a rétegnek a protokollja az Internet Protokoll (IP), az üzenetvezérlő protokoll cím meghatározó eljárása, a foglalt címet meghatározó eljárás. A rétegben előforduló események és hibák jelzésére szolgál az Internet Control Message Protocol (ICMP), az Internet Vezérlőüzenet Protokoll.

3. Hoszt-hoszt réteg

2 rétegprotokollból áll, az egyik a Transmission Control Protocol (TCP), azaz a továbbítást szabályozó eljárás, a másik az összeköttetés mentes szállítási protokoll, User Datagram Protocol (UDP).

4. Alkalmazási réteg

Itt vannak a felhasználói és a hálózati kapcsolatot biztosító programok.

IP címzés

Két részre bontották a címet. Az első rész a hálózatot, a másik pedig a konkrét hosztot azonosítja. A hálózatok közti kapcsolatot a routerek biztosítják.

Az IP címformátum 32 bit hosszúságú.

Minden osztálynak külön címmaszkja van, melyet a hálózat és a hosztcímek szétválasztására használnak. ÉS műveletet végeznek a teljes címmel, a kapott eredmény a hálózat azonosítója.

Az IP címek felépítése

X.X.X.X, ahol az „X” egy [0..255] decimális szám. Pl.: makacs.poliod.hu193.225.184.80. Az IP felépítése hierarchikus. Jelenleg az IP címek kiadása egyre nagyobb akadályokba ütközik, ugyanis kevés kiadatlan IP cím van. Ennek orvosolására dolgozzák ki az IPng (IP Next Generation-t).

Speciális IP címek

- A csupa 0 cím a saját gépet jelöli (0.0.0.0);
- 255.255.255.255 szórt üzenet címzettje (mindenki);
- A 127-tel kezdődő címek (127.X.X.X), a visszairányítás címek, a hálózatok belső tesztelésére használják;
- Ha a hoszt címrésze csak 1-es, akkor az adott hálózat összes gépe megkapja az üzenetet (broadcast).

A másik címzési rendszer a domain név rendszer. Név alapján történő címzés. Ez egy karakterlánc a FQDN, a teljes domain név. Ilyet a DNS (Domain Name System) a domain név rendszer szerint képeznek, hierarchikus felépítésű. A névből kell visszaazonosítani az IP címet. Ezt vagy a saját címtáblázatának, vagy egy Name Server segítségével oldja meg.

Összekötettés mentes szállítási protokoll: *UDP (User Datagram Protocol)*

Vannak esetek, mikor az adat olyan kicsi, hogy egy datagramban is elfér (vezérlés, kérés). Ekkor nincs szükség a TCP szállítási protokollra, elkerülve annak bonyolultságát, egy minimális fejléccel elküldhető az adat. Ha nincs nyugtázás, a protokoll szerint újra elindul a csomag.

Az Internet vezérlése: *ICMP protokoll*

A működést az IMP és az átjárok felügyelik, ha gyanús esemény következik be azt az ICMP (Internet Control Message Protocol – Internet vezérlőüzenet protokoll) alapján jelentik. Hiba- és vezérlőüzeneteket küldenek más routereknek és hostoknak. Ezek IP-csomag formában mennek, s csak az eredeti, eseményt kiváltó csomag feladója kapja meg. A protokoll az Internet tesztelésére is használható.

ARP (Adress Resolution Protocol) – ***címleképzési protokoll***

A gyakorlatban legtöbbször Ethernet kártyákat használnak fizikai és adatkapcsolati szinten. Ezek viszont 48 bites címzéssel rendelkeznek. Minden hoszt egy saját ARP táblázattal rendelkezik, ahol az IP címekhez tartozó Ethernet portok vannak megfeleltetve. Amennyiben ebben a táblázatban a címzet megvan, a kapcsolat felépül, a csomag az Ethernetes fejléccel együtt a célhoz indul. Ha nincs meg, az ARP protokoll egy kérést ad le, amiben az adott IP számú gép Ethernetes portját kéri. Amikor az adott gép észreveszi az IP címe szerint megegyező kérést, elküldi a saját Ethernet port értékét, s az bekerül a másik host ARP táblájába. Így az már el is küldheti a csomagot.

Vezérlő protokollok

1. ICMP protokoll (Internet vezérlőüzenet protokoll)

Az Internet működését a routerek szorosan figyelemmel kísérik, ha váratlan esemény következik be azt az ICMP segítségével jelentik. Hiba- és vezérlőüzeneteket küldenek más routereknek és hosztoknak. Ezek IP-csomag formában mennek, s csak az eredeti, eseményt kiváltó csomag feladója kapja meg. A protokoll az Internet tesztelésére is használható.

2. ARP protokoll (Címfeloldási protokoll)

Manapság a legtöbb hoszt egy olyan interface-kártyával kapcsolódik a LAN-hoz, amely csak a LAN-címeket érti meg. Például minden eddig gyártott Ethernet kártya 48 bites Ethernet-címmel felszerelve érkezik.

Az ARP megoldja azt a problémát, hogy megtudjuk melyik Ethernet-cím felel meg egy adott IP címnek.

3. RARP (Fordított címfeloldási protokoll)

A RARP szerver kikeresi az Ethernet-címet a konfigurációs állományaiban és visszaküldi a megfelelő IP-címet.

4. BOOTP

UDP-üzeneteket használ, melyeket a routerek továbbítanak. Ezenkivül további információkkal is ellátja a lemez nélküli munkaállomásokat.

5. DHCP (Dinamikus hoszt-konfigurációs protokoll)

Mind manuális, mind az automatikus IP-címkiosztást lehetővé teszi.

Z1/12 Az Interneten használt protokollok, TCP/IP felépítése, a TCP és az UDP protokollok.

Az Interneten használt protokollok

Az Interneten leggyakrabban használt protokollok a TCP és az UDP. Ezek a leghasznosabbak számunkra, segítségükkel érjük el a létező összes szolgáltatást (FTP, HTTP, stb...), feladatuk kommunikációs csatornát biztosítani.

Egyéb protokollok: SMTP, POP3, IMAP, SIMAP, FTP, HTTP, NNTP, stb…

Az Internet szállítási rétege: a TCP

A TCP fogadja a tetszőleges hosszúságú üzeneteket a felhasználói folyamattól és azokat max 64kB részekre bontja, fejlécet fűz hozzá és csomagokként továbbítja a hálózati réteg felé. Nem ennek a rétegnek a feladata a datagrammok (adatcsomagok) helyesen és megfelelő sorrendben történő továbbítása, hanem az időzítéseket figyelve újra kell küldenie a csomagokat, illetve a kapott adatokat helyes sorrendben eredeti üzenetté alakítani. A TCP a pozitív nyugtázást használja, hiánya esetén újraküld. A küldés pillanatában elindul egy időzítő. 204 oldal

Az Internet hálózati rétege: az IP

A protokoll megbízhatatlan összeköttetés-mentes szolgálatot biztosít, a megbízhatósági mechanizmusokat a szállítási rétegben kell megvalósítani. Az IP definiálja a az adatátvitel legkisebb egységét, pontos formáját, az útválasztást, valamint néhány további olyan fontos szabályt, amelyek meghatározzák, hogy a hostok, IMP-k hogyan dolgozzák fel az IP csomagokat, mikor és hogyan kell hibajelzéseket generálni, mikor kell a csomagot eldobni. 207 oldal

Az IP csomagokat gyakran tördelni (fregmentálni) kell, mert a hálózatra jellemző maximális adatátviteli méret ezt szükségessé teszi. A kapott fragmenteknek 8 bájttal oszthatónak kell lennie, s csak a célhelyen egyesítődnek.

TCP/IP felépítése

A TCP/IP protokoll alapvetően az OSI modell két rétegének a funkcióját valósítja meg: ez a hálózati és a szállítási réteg.

A hálózati modell 4 rétegből áll:

1. Hálózat elérési

Az OSI modell 2 alsó szintjének felel meg, és ez biztosítja a kapcsolatot a csomópontok között (pl.: Ethernet, Token Ring, token Bus).

2. Hálózati réteg

Ez a réteg végzi a csomagok útvonal kijelölését a hálózatok között. Ennek a rétegnek a protokollja az Internet Protokoll (IP), az üzenetvezérlő protokoll cím meghatározó eljárása, a foglalt címet meghatározó eljárás. A rétegben előforduló események és hibák jelzésére szolgál az Internet Control Message Protocol (ICMP), az Internet Vezérlőüzenet Protokoll.

3. Hoszt-hoszt réteg

2 rétegprotokollból áll, az egyik a Transmission Control Protocol (TCP), azaz a továbbítást szabályozó eljárás, a másik az összeköttetés mentes szállítási protokoll, User Datagram Protocol (UDP).

4. Alkalmazási réteg

Itt vannak a felhasználói és a hálózati kapcsolatot biztosító programok.

Az Internet szállítási protokolljai

UDP (User Datagram Protocol – Felhasználói Datagram Protokoll)

Összeköttetés nélküli protokoll. Egy egyszerű protokoll és van néhány sajátos alkalmazása, mint pl.: kliens-szerver-interakciók és a multimédia. Az UDP olyan alkalmazásoknak kínálja a szolgálatát, amelyek összeköttetés kiépítése nélkül akarnak beágyazott IP-datagramokat küldeni.

Olyan szegmenseket használ az átvitelhez, amelyek egy 8 byte-os fejrészből (a fejrészben megtalálható a feladó és a címzett portszáma), valamint a felhasználói adatokból állnak. A két port a végpontok forrás- és célgépen belüli azonosításra szolgál. Amikor az UDP-szegmens megérkezik, akkor az adatmezejét a szállítási entitás kézbesíti a címzett portra kapcsolódó folyamatnak.

Az UDP biztosít egy interface-t az IP-protokoll használatához, azzal a többletszolgáltatással, hogy a portok használatával egyszerre több folyamatot képes demultiplexelni.

Az Internet protokollcsomag tartalmaz összeköttetés nélküli szállítási protokollt is. Ez az **UDP (User Datagram Protocol)**. Az UDP beágyazott nyert IP datagramok küldését teszi lehetővé a felhasználók számára összeköttetés létesítése nélkül. Sok kliens-szerver alkalmazás, amely egyetlen kérdésre egyetlen választ küld, UDP-t használ ahelyett, hogy összeköttetés létesítésével és bontásával bajlódna.

Az UDP szegmens 8 bájtos fejrészből és az azt követő adat mezőből áll. A két port ugyanazt a célt szolgálja mint a TCP-ben: a forrás -és a célgépen belül azonosítja a végpontokat. Az UDP szegmens hossza tartalmazza a fejrész és az adat együttes hosszát. Az UDP ellenőrző összeg magába fogalalja az ugynevezett pszeudofejrészt, az UDP fejrészt és az UDP adatot, szükség esetén páros hosszúságura kiegészítve.

TCP (Transmission Control Protocol – Átvitel-vezérlési Protokoll)

Összeköttetés alapú protokoll. Megbízható bytefolyamot biztosít a végpontok között egy egyébként megbízhatatlan összekapcsolt hálózaton. A TCP-nek kell megteremtenie azt a megbízhatóságot, amelyet a legtöbb felhasználó megkíván, és amelyet az IP nem ad meg.

Minden TCP-t támogató gép rendelkezik egy TCP szállítási entitással, amely lehet egy könyvtári eljárás, egy felhasználói folyamat vagy a kernel része. A TCP-folyamokat és az IP-réteg felé használható interface-eket minden esetben a TCP-entitás kezeli. A felhasználói adatfolyamokat a TCP-entitás 64 KB-ot meg nem haladó méretű darabokra szedi szét. Az egyes darabokat önálló IP-datagramokban küldi el. Amikor egy géphez TCP-adatokat tartalmazó datagram érkezik, az a TCP-entitáshoz kerül, amely visszaállítja az eredeti bytefolyamokat.

Minden TCP összeköttetésen továbbított bájt rendlekezik egy 32 bites sorszámmal. Egy 10 Mb/s sebességű LAN-on teljes sebességgel adó host sorszámai elméletileg nagyjából egy óra alatt körbeérhetnének, de a gyakorlatban ez jóval tovább tart. A sorszámokat egyaránt használják nyugtázásra és a csúszóablakos mechanizmushoz, amely külön 32 bites mezőket használ a fejrészben.

A küldő és fogadó TCP entitások között szegmensek formájában folyik az adatcsere. A **szegmens** egy fix 20 bájtos fejrészből (amit további opcionális rész követhet) és nulla vagy több adatbájtból áll. A TCP szoftver dönti el, hogy mekkorák legyenek a szegmensek. Különböző írások adatait egy szegmensbe gyüjtheti, vagy egyetlen írás tartalmát több szegmensre oszthatja. A szegmens méretére mindössze két korlátozás van. Egyrészt minden szegmensnek – beleértve a TCP fejrészt is – el kell férnie a 65535 bájtos IP adatmezőben. Másrészt minden hálózatban van egy **leghosszabb átvihető adategység (maximum transfer unit, MTU)** korlát. A szegmens mérete nem haladhatja meg az MTU méretét. Gyakorlatban az MTU általában néhány ezer bájt, így ez jelent a szegmens méretére felső korlátot. Ha egy szegmens áthalad egy sor hálózaton anélkül, hogy a hosszát változtatni kellene, majd egy olyanba kerül, amelynek MTU értéke kisebb a szegmens hosszánál, akkor a hálózatok határán levő router a szegmenst két vagy több kisebb szegmensre darabolja.

TCP szegmens fejrésze:

Minden szegmens egy fix kiosztású 20 bájtos fejrésszel kezdődik, amit fejrész opciók követhetnek. A *forrásport (source port)* és *célport (destination port)* mezők azonosítják az összeköttetés helyi végpontjait. Minden host maga döntheti el, hogyan foglaljon portokat 1024-től kezdődően. Egy portszám és a host IP címe együtt alkotja a 48 bites egyedi TSAP-ot. A forrás és cél csatlakozószámok (socket numbers) együttese azonosítja az összeköttetést. A s*orszám (sequence number)* és *nyugtaszám (acknowledgement number)* mezők szerepe szokásos. A TCP *fejrészhossz (*TCP *header length)* mondja meg, hány 32 bites szóból áll a TCP fejrész. Ez az információ azért szükséges, mert a fejrész mérete az *opciók (options)* mező változó hossza miatt szintén változó. Tulajdonképpen ez a mező jelzi az adat kezdetét (32 bites szavakban mérve) a szegmensen belül, de mivel ez egyben a fejrész szavakban mért hossza is, a végeredmény ugyanaz. Ezután egy használaton kivüli 6 bites mező következik, ezek: URG, ACK, PSH, RST, SYN, FIN. A megbízhatóság érdekében van még egy ellenőrző összeg és sürgősségi mutató is a fejrészben.