

1. A számítógép hálózatok alapjai

A mai információs rendszerek alapvetően a számítógépes hálózatokra épülnek. A hálózat olyan egymáshoz kapcsolt számítógépből áll, amelyek között így lehetőség van a különböző adatok és erőforrások megosztására ill. információk cseréjére. A hálózatba kapcsolt gépeket host-oknak nevezik. Minden hostnak van (legalább egy) egyedi azonosítója (cím, szám).

A mai számítógéphálózatok alapjainak elméleti (és részben gyakorlati) vizsgálatait jórészt a 1960-as és 70-es években végezték el. Ennek eredményeképpen különböző modellek valósultak meg. Például csomagkapcsolt hálózatok, ütköztetési és token alapú hálózatok, stb.

Ma szinte minden, különböző típusú hálózat között lehetséges kapcsolatot kiépíteni, így lehetőség van a specifikus igények pontos kielégítésére (teljesítmény, ár, biztonság). Ez természetesen nem mindig egyszerű, ui. a fizikai kapcsolat mellett a megfelelő applikációknak is tudniuk kell kommunikálni egymással (pl. e-levelezés).

Napjainkban a TCP/IP alapú technológia tör előre általános felhasználás esetén, ill. az TCP/IP alapú Internet hálózat felhasználási és felhasználói köre bővül a leggyorsabban.

Hálózati csoportok méret szerint

A számítógépek (ill. processzorok) közötti kapcsolat szerint a tipikusan következő csoportokat különböztetjük meg:

név	távolság (m)	méret	szám (db)	kapcsolati sebesség (bit/s)
adatfolyam	0.1	NYÁK panel	max. néhány	nagy (>1G ?)
multiprocessoros rendszer	1	doboz	néhány	nagy (>1G ?)
LAN (Local Area Network)	10-1000	szoba, épület, intézmény	1000	100 M
WAN/MAN (Wide/Metropolitan Area Network)	10k-100k	város, ország	10k-100k	10M
globális (pl. Internet)	1000-10000k	földrész, bolygó	50M	0.1-100k(?)

Az Internet több, egymással összekapcsolt LAN-ból illetve WAN-ból áll.

Átviteli fizikai közegek

Csavart érpár (UTP)

- Szimmetrikus, a telefontechnikában is használják. Alkalmas struktúrális kábelezésre (a telefon- és adatvezetékek megegyeznek).
- Zavarvédeltsége megfelelő (sodrás miatt!).
- Jó minőségű („drága”) kábellel gyors Ethernet is lehetséges (100 Mbit/s).

Koaxiális kábel

- Kiszoruló eszköz, új fejlesztésnél nem biztos, hogy célszerű használni.
- Asszimmetrikus, 50 ohmos hullámimpedancia.
- Gyors, 10-100 Mbit/s sebességű.
- Zavarvédeltsége megfelelő (árnyékolás miatt!).
- Fontos a pontos lezárás, a helyes földelés.

Optikai kábel

- Nagysebességű (~ Gbit/sec), egyirányú átvitel (duplán szerelik). Szerelése csak célszerszámmal történhet. Mechanikusan érzékenyebb (bár léteznek megerősített kábelek).
- Egymódusú kábel: lézeres meghajtás, hullámvezető belső mag.
- Többmódusú kábel: LED-es meghajtás (olcsóbb), folyamatos törés ill. visszaverődés. Vastagabb mag.
- Zavarvédeltsége kiváló.

Infravörös / lézeres átvitel

- Kis távolságon (pl. utca két oldala, Duna felett) alkalmazható.
- Relatív olcsó üzem.
- Rádiófrekvenciás koaxiális kábel
- Egy vagy két frekvencia a TV sávban (közösségi antennarendszerek).
- Két frekvencia esetén fordító szükséges.
- Előnye a viszonylag nagy távolság (~100 km!) és a meglévő kábelek kapacitásának kihasználhatósága.

Telefonvonal

- Modemes összeköttetés részére. Az (automatikus) tárcsázással csökkenthető az üzemeltetési költség.
- Hátrány a korlátolt sávszélesség, a folyamatos számlázás és az egyoldalú kapcsolatkiépítési lehetőség.

ISDN

- Közvetlen összeköttetés pl. Internet szolgáltatók felé.
- Előny az integráltság a telefonrendszerrel (egy kapcsolaton keresztül adat és jel).
- Hátrány az átvitt adatmennyiség számlázása és a korlátolt sávszélesség.

Bérelt vonal

- Közvetlen összeköttetés modem részére.
- Előny a viszonylag alacsony ár (nagy forgalom és helyi kapcsolat esetén), valamint a garantált sávszélesség.
- A sávszélesség felső határa korlátozott.

ADSL

Kábel modem

2.4 G szórtspektrumú modemek

Elérési módszerek

A hálózati kapcsolatok elérési modelljei a következő csoportokra oszthatóak:

	vezérelt	igény szerinti
összeköttetés alapú	polling (lekérdezéses)	vonalkapcsolt
összeköttetés nélküli	tokenes	ütköztetéses

Az összeköttetés alapú kapcsolat esetén egy olyan virtuális csatorna keletkezik a kommunikáló felek között, amely véd az ismétléstől illetve adatvesztéstől.

Az összeköttetés nélküli kapcsolat esetén a kommunikáció ún. datagramok közvetítésével zajlik. Nincs garancia arra, hogy az elküldött datagram egyáltalán megérkezik a célba, sem arra, hogy csak egy példányban vagy csak az elküldés sorrendjében érkezik meg.

A vezérlés történhet központilag: ekkor pl. a központi számítógép egy lista alapján sorban lekérdezi a hálózatba kötött eszközöket. Ilyen lehet pl. egy adatgyűjtő rendszer.

A központi vezérlés másik formája a tokenes vezérlés: ekkor a hálózatra adatot csak az küldhet, akinél a vezérjel (token) van. Ilyen a Token Bus és a Token Ring struktúra.

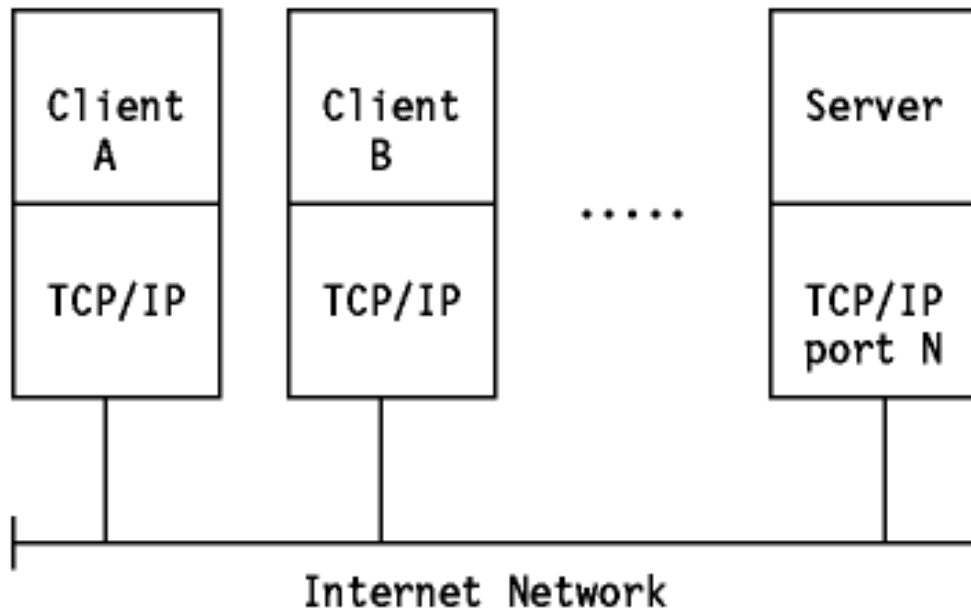
Az összeköttetés alapú igény szerinti kapcsolatra példa az X.25 vagy a telefonhálózat.

Az összeköttetés nélküli igény szerinti kapcsolatra példa az Ethernet hálózat ütköztetéses CSMA/CD (Carrier Sense Multiple Access / Collision Detect) protokollja. Véletlenszerű eléréssel, adás előtt és alatt behallgatunk a csatornába (ütközés!).

A számítógépek közötti kommunikáció szigorú szabályok (protokollok) alapján történik. A protokollok összetettek, ezért ún. logikai rétegekre osztották fel őket. Így az egyes szintek a szintek közötti kapcsolaton kívül nem függenek a többi szinttől, ezért könnyebben lehet implementálni, ellenőrizni őket, esetleges protokoll módosítás esetén a nem közvetlenül kapcsolódó szintek változatlanok maradhatnak.

A kliens-szerver modell

A hálózati kapcsolat applikációi leggyakrabban az ún. kliens-szerver modellre épülnek. Ekkor az egyik, a kezdeményező fél (a kliens) a másik féltől (szervertől) valamilyen szolgáltatást kér. A felhasználók általában a kliens oldallal kerülnek kapcsolatba.



A szerver szolgáltatások jelentős része az AIX operációs rendszerben IP socket interfészen keresztül érhető el. Ilyenkor pl. a szerver program (vagy az inetd superdaemon) figyeli az applikációhoz kapcsolódó ún. well-known portot, és bejövő kapcsolat esetén elindítja a szervert. Másik ilyen lehetőség a portmap használata.

TCP kapcsolat esetén a hálózati kapcsolat maga az igény szerinti kapcsolatkiépítési mód miatt egy egyenrangú, ún. peer-to-peer kapcsolat. Csak maguk a TCP/IP-re épülő applikációk azok, amik a kliens-szerver modellt használják.

A TCP/IP fejlődése

1968	USA Hadügyminisztérium Defense Advanced Research Projects Agency (DARPA): cél olyan hálózatközi protokoll kifejlesztése, amely lehetővé teszi inhomogén helyi hálózatok összekötését, több kapcsolat egyidejű, megbízható kihasználását. (ISO ekkor még nem létezik).
1970-72	ARPANET 50 host, FTP, TELNET SMTP. Alap: NCP (Network Control Program).
1978	TCP/IP mai formában felváltja az NCP-t. Pont-pont összeköttetések.
1980-83	Internet: az ARPANET TCP/IP alapokra áll át.
1980	Berkley: megjelenik a BSD 4.1 (új: rlogin, rsh, rcp), TCP/IP Unix környezetben.
1985	AT&T SYS V is beépíti a BSD TCP/IP részeit.
1986	BSD 4.3 kommunikációs standard a Unixban.
1987-től	NSFNET, EBONE, CREN, EARN, RARE bővülése, gyors elterjedés
1989	180-nál több gyártó, 1000 feletti TCP/IP termék, újabb applikációk (NFS, X, adatbázisok)
1991	Integrációs irány az USA-ban: Internet -> National Research and Education Network (NREN)
1995	Information Super Highway
ma	Gyors bővülés, tömeges használat elterjedése, már nem csak kutatási célok. >100M host, >500M felhasználó (már nem pontos ! ;-) !!!)
jövő	Globális hálózat, IPng, Network Computing (?), adatbiztonság (?).

Szabványok az Interneten

Az Internet szabványai sokszor már egy működő változat birtokában adták meg (talán ezért is használható a TCP/IP ...).

A szabványok de facto leírását az ún. RFC-k (Request for Comment, megjegyzések kérése a szabvány kapcsán) adják meg.

Az RFC-k a sri-nic.arpa gépről, anonymous FTP segítségével érhetőek el (rfc-index.txt, rfcxxx.txt, ien-index.txt, ien-xxx.txt állományok).

TCP/IP szolgáltatások

A leggyakrabban a következő TCP/IP szolgáltatásokat használják a számítógépek között:

- Állomány átvitel, azaz File Transfer Protocol (ftp) .
- Távoli bejelentkezés egy gépre, ezt a Network Terminal Protocol (telnet) teszi lehetővé.
- Elektronikus levelezés, ami lehetővé teszi elektroniku üzenetek küldését más számítógépekre (is).
- Távoli nyomtatás, ami lehetővé teszi más gépekhez kötött nyomtatók használatát, így egy adott felhasználói csoport viszonylag kevés nyomtatóval is jól kiszolgálható.
- Távoli programfuttatás (RPC). Segítségével lehetővé válik programok futtatása a távoli gépen. Az AIX esetén a shellből érhetjük el egy más gépen futó program be- és kimenetét. Ezzel a másik géphez kötött eszközöket is közvetlenül a gépünkről elérhetjük pl. backup készítéséhez.
- Network file rendszerek (NFS,RFS,AFS), amelyek lehetővé teszik egész állományrendszerek elérését más gépek számára.
- Hálózaton keresztül használható grafikus ablak (window) rendszerek (ilyen az X11 rendszer is).
- Név kiszolgálók (name server): ezek az egyedi gépek neveit és címeit tartalmazzák egy intézményen belül. Segítségükkel nem kell minden host címét a helyi gépen tárolni, az a központi név szerverről név alapján elérhető.
- Terminál szerverek, amelyek speciális célszámítógépek, ahonnan távoli gépekre jelentkezhetünk be. A terminálok vagy modemek ezekhez csatlakoznak, így nem szükséges egy hosthoz bejelentkezni csak azért, hogy egy másik gépet pl. telnet-tel elérjünk.

Az ISO/OSI hálózati modell

A hálózatok elterjedésével párhuzamosan elméletileg is elkezdtek kidolgozni a hálózati kapcsolatok egyes funkcionális rétegeinek felosztását. Az egyik általános felépítést az OSI (Open Systems Interconnection Reference Model) adta meg, amelyet az ISO (International Standards Organization) is támogat.

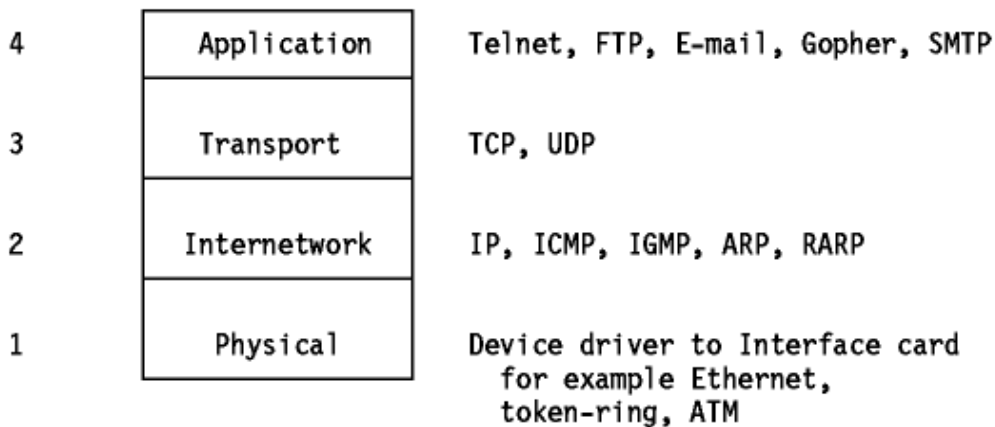
Az ISO/OSI modell egy elméleti modell, amelyet a (pl. közben vagy korábban) megvalósított hálózati implementációk nem mindig követnek (a TCP/IP protokoll például kevesebb réteggel dolgozik).

Az OSI rétegek a következők:

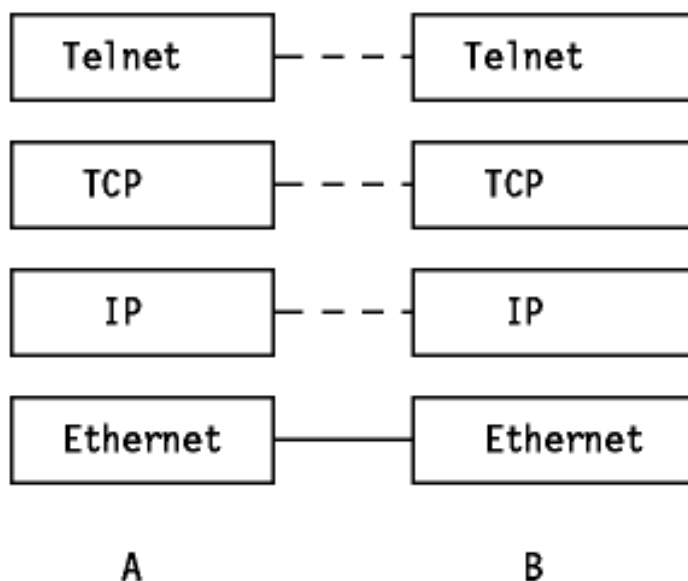
alkalmazási	Application	az egyes hálózati funkciók elérését teszi lehetővé, pl. mail, ftp, telnet, WWW.
megjelenítési	Presentation	az egyes, gépek közötti adatkonverziókat végzi el, (esetleg tömörít, tikosít). Például ilyen az XDR (eXternal Data Representation) vagy a EBCDIC - ASCII konverzió.
viszonyréteg	Session	kapcsolatot létesít a két végprogram között, a sikertelen kapcsolatok kezelése. Például ilyen az RPC (Remote Procedure Call).
szállítási	Transport	Feladata a viszonyrétegtől kapott adatokat csomagokká szabdalja ill. visszaalakítja az üzenetet. Például ilyen a TCP (Transmission Control Protocol), UDP (User Datagram Protocol).
hálózati	Network	A csomagok irányítását, fragmentálását, a kapcsolatok kiépítését és megszakítását végzi. Ilyen pl. az IP (Internet Protocol).
adatkapcsolati	Data Link	Az adatcsomagokat adja meg, vezérli a vonal hozzáférését, az adatok beágyazását és a hibajavítást.
fizikai	Physical	Az elektromos kapcsolatért felelős, megadja az elemi csomagok átvitelének módját.

A TCP/IP protokollok általános felépítése

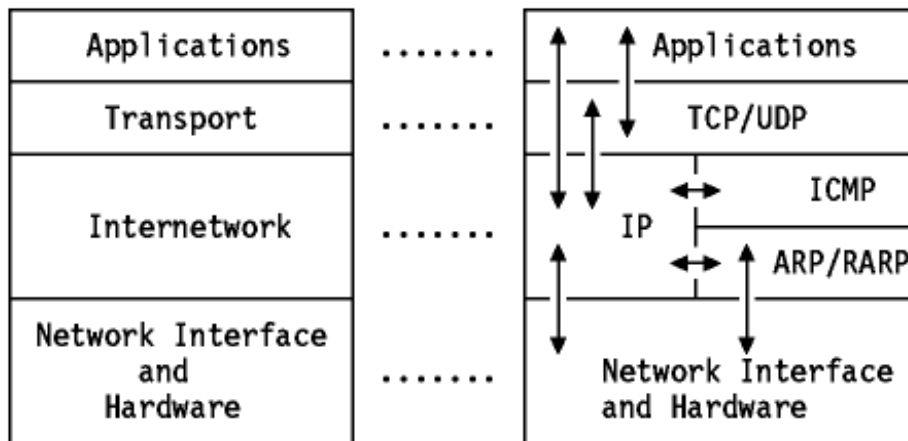
A TCP/IP protokollt a következő 4 egymásra épülő réteg alkotja:



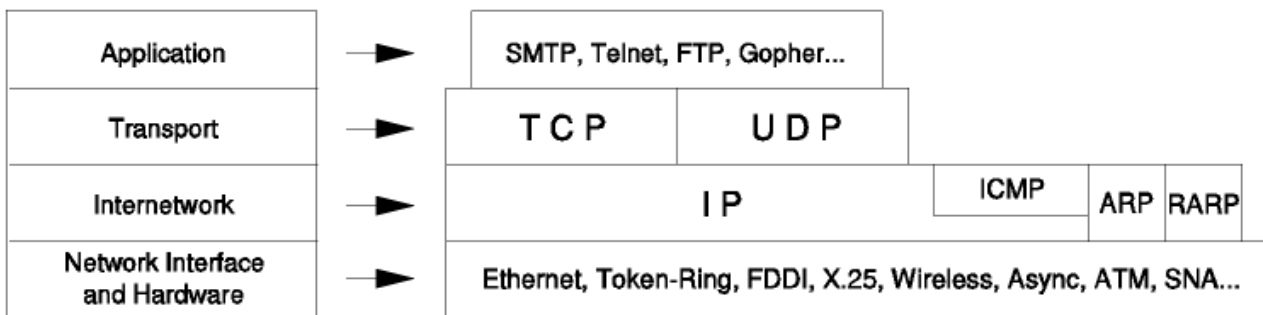
Minden szintnek külön feladata van. Két, egymással kommunikáló host esetén az egymásnak logikailag megfelelő host szintek (mindkét oldalon) kommunikálnak egymással:



A kapcsolatok a következők:



Az egyes szintek feladatai a következők:



alkalmazási Application

Egy felhasználói program, ami egy másik processzel van kapcsolatban. Például a TELNET, az FTP (File Transfer Protocol) vagy az SMTP (Simple Mail Transfer Protocol) ilyen.

szállítási Transport

A két végpont közötti adatátvitelt biztosítja. Adatokat fogad a felette lévő alkalmazási rétegtől, majd azokat (hálózaton átvihető méretű) darabokra vágja szét, ezután átadja ezeket a csomagokat a hálózati rétegnek. A célhoston a szállítási szint feladata a beérkező csomagok eredeti sorrendbe rendezése. Mivel egyszerre több folyamat is futhat, ezért a szállítási réteg feladatát az adatok hálózati rétegre történő multiplexelése / demultiplexelése. Ilyenre példa a összeköttetés-orientált TCP (Transmission Control Protocol) és az összeköttetés-mentes UDP (User Datagram Protocol)

hálózati Internetwork

A réteg biztosítja a csomagok (datagrammok) átvitelét a két gép közötti hálózaton. Ennek a feladata a csomagoknak az útvonalkijelölés (routing) is, azaz a forrás hosttól a cél hostig történő elirányítása,. Erre példa az IP (Internet Protocol), amely egy olyan összeköttetésmentes protokoll, amelyik nem feltételezi az alsó rétegek megbízható adatátvitelét.

adatkapcsolati Network Interface /
Data Link

Az aktuális hálózati hardverhez kapcsolódó réteg. Biztosítja az adatok fizikai átvitelét. Például ilyen az IEEE 802.2, az Ethernet V2, az X.25, ATM, FDDI stb. .

Megjegyzendő, hogy néhány (elsősorban hálózat elemző/kezelő) alkalmazás nem használja mind a négy szintet. Ilyen pl. a ping parancs, ami az ICMP-re alapozódik, és csak az alsó két szintet használja.

Hálózati eszközök

Nagy (WAN) hálózatok létrehozásához a következő eszközöket használhatjuk:

repeater (ismétlő)	a fizikai szinten működik, csak azonos típusú közeg esetén használható. Pl. az Ethernet hálózat fizikai mérete három ok miatt maximált: a jel csillapodása és a futási idők limitálják a maximális távolságot, a véletlenszerű csomagküldés pedig a forgalom növekedése miatt a maximálisan üzemeltethető berendezések számát limitálja. A jel csillapításán repeater használatával segíthetünk (jelerősítő).
Switch	
bridge (híd)	Az adatkapcsolati szintek összekapcsolására használható, működik különböző fizikai közegek (MAC) esetén is. Pl. Ethernet hálózat esetén nagyobb távolságoknál a futási idők túlságosan nagyok lesznek, ezért ilyenkor a csomagok ütközését tárolás/továbbítás módszerrel kell elkerülni két távoli szegmens között. Erre a célra a bridge szolgál, ami csak pl. a két szegmens közötti forgalmat engedi át, így a helyi forgalom nem zavar a másik szegmenst. A bridge képes kiszűrni (és eldobni) a hibás csomagokat.
router (kapcsolat átirányító)	Két hálózatot kapcsol össze a hálózati szinten. Vizsgálja a címzést, és csak a két hálózat közötti átmenőforgalmat bonyolítja le. Képes lehet topológiai (hálózat változása) és protokollbeli változások követésére (pl. DECNET és TCP/IP). A TCP/IP hálózati nyelvben a router és gateway fogalma keveredik (IP router, IP gateway, Internet gateway). Ekkor mindig router funkcióra kell gondolnunk.
gateway (kapuállomás)	Különböző típusú hálózatokat köt össze, miközben protokoll konverziót is végez az alkalmazási szinten (OSI modell esetén). Megjegyzendő, hogy a vasfüggöny (firewall) funkció TCP/IP esetén határozottan ebbe a körbe tartozik.
tűzfal	

2. A Fizikai réteg

Az Ethernet hálózat

Az Ethernet a helyi (LAN) hálózatok leggyakoribb közege. Szinte minden hálózatra köthető eszköznél választható felület.

Busz rendszerű, 10 Mbit/s sebességű (gyors Ethernetnél 100 Mbit/s).

Differenciális Manchester kódolás (bithatáron 1: van átmenet): jó hibatűrés, a DC szint 0.

CSMA/CD (Carrier Sense Multiple Access / Collision Detect) technika: egyszerre csak egy állomás küldhet csomagot. Ütközés esetén hatványszerűen növekvő véletlen késleltetés után újraküldés. Adás előtt és alatt folyamatos ütközés-figyelés.

A fizikai hordozó lehet

"vastag" koax	max. 500 méter hossz, max. 50 méteres AUI transceiver csatlakozás (vámpr).
vékony koax	max. 185 méter, közvetlen csatlakozás (T vagy úszóhártyás kábel. A transceiver általában a kártyán található. A régebbi AIX rendszereknél kézi átkapcsolású az Ethernet kártya a BNC/AUI között (a SMIT csal!).
sodrott érpár	bekötés repeater-be vagy Etherswitch-be.
üvegszál	bekötés repeater-be vagy Etherswitch-be.

Nagyobb távolság vagy megbízhatóbb működéshez (leválasztott alhálózatok/gépek) erősítő szükséges: ez a repeater (ismétlő).

Nagyobb igények esetén lehetőség van ún. Etherswitch (EtherStreamer Switch) használatára. Ez bármelyik két csatlakozási pontja között egyidejűleg teljes Ethernet sáv szélességű csatlakozást képes létesíteni (full duplex).

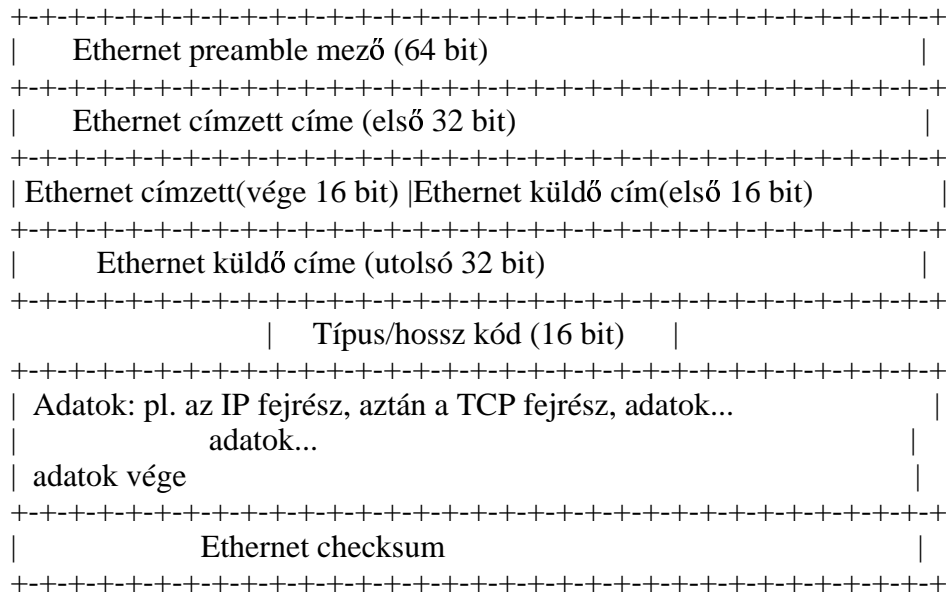
Lehetőség van az ún. Fast Ethernet használatára: itt 10 helyett 100 Mbit/s sebességű órajellel dolgozunk, a protokoll változatlan.

A repeater nem vizsgálja a csomagot (nincs hibajavítás), csak erősíti és szétküldi (protokollfüggetlen). Legfeljebb 4 repeater lehet bármelyik két végpont között (késleltetés!).

Minden Ethernet csatlakozónak egy 48-bites egyedi címe van. A címek kiosztását a gyártók végzik (első három byte adott). Bizonyos esetekben (pl. DECNET használatkor) egy fizikai csatlakozó több (logikai) Ethernet címet is használ. Természetesen egy host akár több Ethernet csatlakozóval is rendelkezhet!

Az Ethernet csatlakozó csak azokat az csomagokat figyeli a hálózaton, amelynek ő a címzettje, vagy amelyik egy ún. broadcast (mindenkinek szóló üzenet).

Az Ethernet csomagok felépítése a következő:



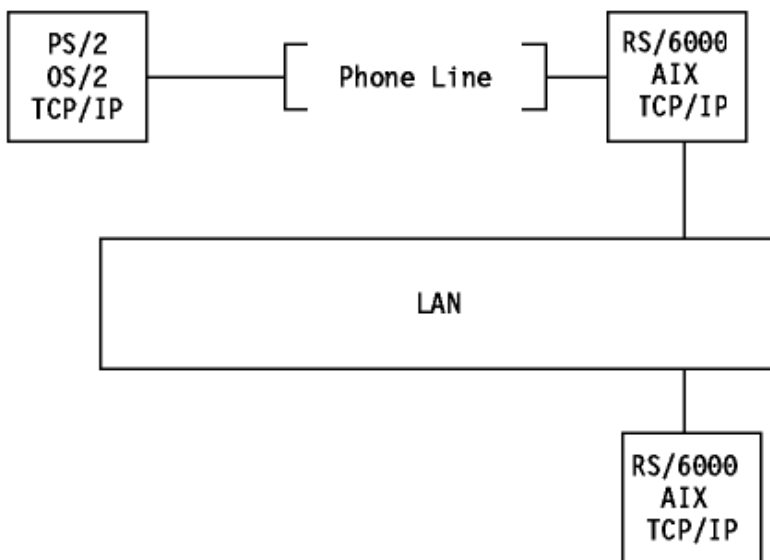
Preamble mező	A kezdeti szinkronizációra használt 64 bit.
Ethernet címzett címe	A címzett host adott portjának címe, összesen 48 bit.
Ethernet küldő címe	A csomagot küldő host adott portjának címe, összesen 48 bit.
Típus/hossz kód	A csomag típusa 16 bitben. Szabványfüggő: az Ethernet Version 2 (de facto szabvány) (DIX) esetén ez a típus (IP esetén 0800, ARP-nál 0806). Az IEEE 802.3 (formális szabvány) esetén a hosszat adja meg.
Adatok	Az átviendő adatok, 46-1500 byte közötti méretben.
Ethernet checksum	A csomagból számolt CRC (Cyclical Redundancy Check) érték, segítségével lehetséges a hibás csomagok kiszűrése.

Token Ring

Az FDDI (Fiber Distributed Data Interface) hálózat

ATM

Serial Line IP (SLIP) kapcsolat



PPP

A PPP (Point-to-point Protocol) a SLIP-hez hasonlóan soros átviteli protokoll. A PPP előnyei a SLIP-pel szemben a következők:

- többfajta protokoll (nem csak IP) átvitelét támogatja
- CRC hibaellenőrzés
- TCP és IP fejrész tömörítés (Van Jacobsen Header Compression)

A PPP az ajánlott sorosvonalis kapcsolati protokoll.

Sok szolgáltató dinamikus SLIP és PPP IP címkiosztást biztosít: a kapcsolat kezdetben pl. a 1.1.1.1 címmel indul, majd a szolgáltató az éppen üres IP címek közül egyet rendel hozzá a kapcsolathoz. A PPP általában automatikusan tudja ezt kezelni.

3. Az IP (Internet Protocol)

TCP/IP hálózatok esetén az Internet Protocol végzi el a datagrammok eljuttatását a forrástól a célig. Ezt címezéssel és a csomagok darabolásával (fragmentáció) végzi el. Az IP szint figyel a csomagok címezését. Egy host minden egyes TCP/IP hálózati csatlakozójának van egy ún. IP címe (Internet cím), ami egy 32 bites szám.

Az IP elrejti a hálózat fizikai megvalósítását egy virtuális hálózati kép létrehozásával. Ez egy összeköttetésmentes, csomagokat nem megbízhatóan (keveredés, ismétlődés, hiány) továbbító protokoll. A megbízhatóságot a felsőbb (pl. TCP) rétegeknek kell biztosítaniuk.

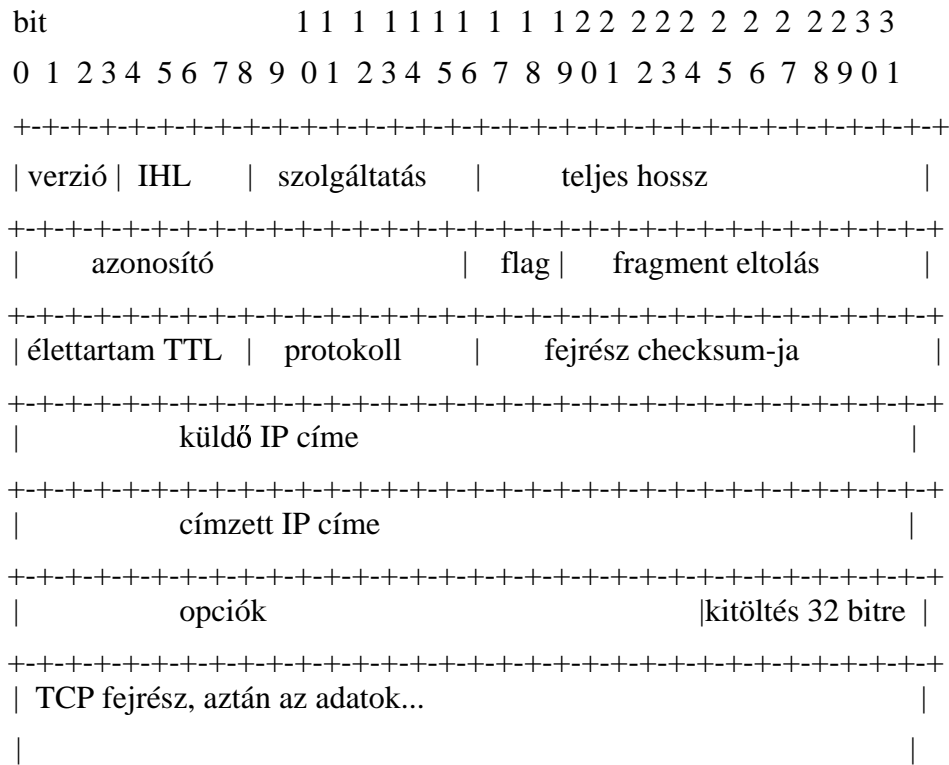
Az IP Datagram

Az Internet Datagram (IP Datagram) az Internet protokoll alapvető építőeleme. Egy - az IP információkat tartalmazó - fejrészből és a kapcsolódó adatmezőkből áll. A datagram átvitele a két végpont között egyenként történik, akár különböző utakon is. Az IP nem biztosítja a datagram megérkezését a címzethez.

Az IP datagramot a fizikai hálózat (pl. Ethernet) saját kerettel látja el, így az IP datagram mérete korlátozva van. Ethernet esetén ez 1500 byte, de lehet ennél kisebb is. Az IP képes kisebb fizikai csomagméret esetén feldarabolni a datagramokat, mindössze azt követeli meg (a hatékonyság érdekében), hogy a minimális méret legalább 576 byte legyen. A fragmentumok mindegyike saját IP fejrésszel rendelkezik, és a teljes adatfolyamot általában a fogadó oldal magasabb protokollja (pl. TCP) végzi el.

Az IP datagram formátuma

Az IP datagram fejrésze legalább 20 byte méretű:



verzió Az IP protokoll verziója. Jelenleg ez 4, az 5 a kísérleti a 6 pedig az IPng (IP The Next Generation, IPv6) verziót jelenti.

IHL Az IP fejrész mérete 32 bites hosszú szavakban.

szolgáltatás Ez meghatározza a szolgáltatás típusát (gyors, de megbízhatatlan, lassú, de biztos stb.). A byte a Precedence, a TOS és a MBZ mezőkből áll:

Precedence A prioritás mértéke:

000	normál
001	elsőbbségi
010	közvetlen
011	azonnali
100	sürgős azonnali
101	kritikus
110	internetwork vezérlő
111	hálózatvezérlő

TOS Megadja a késleltetést:

1000	minimális késleltetés
0100	leggyorsabb átvitel
0010	legmegbízhatóbb átvitel
0001	minimális pénzügyi költség
0000	normál

MBZ A bit további alkalmazásokra fenn van tartva („must be zero”)

teljes hossz A datagram teljes hossza byte-ban (fejrész+adat).

azonosító A küldő által a datagramhoz rendelt szám. A fragmentumok ugyanazzal az azonosítóval rendelkeznek.

flag	3 vezérlő bit:
	0 fentartott 0 érték
	DF Don't Fragment: 0 engedélyezi, 1 tiltja a fragmentációt.
	MF More Fragments: 0 jelzi, hogy ez az utolsó, a datagramhoz kapcsolódó fragmentum, míg 1 jelzi, ha még van fragmentum.
fragment eltolás	Jelzi, hogy az adat hol helyezkedik el az eredeti datagramban. Az érték 64 bit méretű adatokban méri a korábbi fragmentumokban átvitt tiszta adatmennyiséget. Ez 0 a nem fragmentált csomagokban.
élettartam	Time To Live: megadja hop-számban a datagram élettartamát. Minden router eggyel csökkenti a rajta áthaladó datagram TTL értékét. Ha ez 0 lesz, akkor törli a datagramot (és egy ICMP üzenetet küld vissza). A TTL megakadályozza hurkok képződését. A kezdeti érték tetszőleges, de max. 255 lehet, azaz a TCP/IP hálózat bármelyik két pontja között nem lehet 254-nél több router (a valóságban ez ritkán több 20-30 -nál, kis bolygó vagyunk ...).
protokoll	Az IP feletti protokollt azonosítja. Leggyakoribb értékei lehetnek:
	0 fenntartva
	1 Internet Control Message Protocol (ICMP)
	2 Internet Group Management Protocol (IGMP)
	3 Gateway-to-Gateway Protocol (GGP)
	4 IP beágyazás
	5 adatfolyam (stream)
	6 Transmission Control (TCP)
	8 Exterior Gateway Protocol (EGP)
	9 Private Interior Routing Protocol
	17 User Datagram (UDP)
	89 Open Shortest Path First Protocol
fejrész checksum	A fejrész ellenőző összege az adatok nélkül, a checksum mezőt 0-nak tekintve. Amennyiben a checksum nem egyezik, a datagram hibás és automatikusan törlődik.
küldő IP címe	A küldő 32 bites IP címe.
címzett IP címe	A címzett 32 bites IP címe.

opciók

A mező hosszúsága változó lehet. Típusai a következők:

típus byte

típus byte, hossz byte és további opcionális adatbyte-ok

A típus byte lehet:

fc Flag Copy: jelzi, hogy a fragmentált datagram esetén az opciók mező másolódjon (1) vagy ne (0).

class 2 bit, ami lehet

0 kontroll

1 fenntartott

2 hibajavítás és mérés

3 fenntartott

option number Az opciószám egy 5 bites érték:

- 0 Az opciók lista vége, a class=0, az fc=0 és nincs sem hosszúság, sem adat (00 hex byte).
- 1 NOP, üres művelet. A class=0, fc=0 és nincs sem hosszúság, sem adat (01 hex byte).
- 2 Biztonsági opció. Security. A class=0, fc=1, a hosszúság 11, és 8 byte adatot tartalmaz.
- 3 Loose Source Routing. A class=0, fc=1, a hosszúság változó az adatokkal. Az opció az IP routing során ellenőrző pontokat jelölhet meg.
- 4 Internet Timestamp. A class=2, fc=0, a hosszúság változó, legfeljebb 40 byte. Az idő átvitelére szolgál, msec-ben mérve 0 UT-tól kezdve (l. xntpd).
- 7 Record Route. A class=0, fc=0, a hosszúság változó az adatokkal. Az opció az IP routing egyes pontjainak rögzítésére utal.
- 8 Stream ID. A class=0, az fc=1, a hosszúság 4 és egy adata byte van. A SATNET használja.
- 9 Strict Source Routing. A class=0, fc=1, a hosszúság változó az adatokkal. Az opció az IP routing során követendő utat jelöli ki.

kitöltés A bitek a következő 32 bites határra egészítik ki a datagram IP fejrészét

adatok A magasabb szintű protokollnak átadandó adatok.

Fragmentáció

Az IP datagram útja során több fizikai hálózaton keresztül haladhat át. Ezeknek a maximális keretmérete különböző lehet (Maximum Transmission Unit, MTU). Ezért a hosszabb datagramokat az IP feldarabolja kisebbekre, majd ezek visszaállítása a cél hostnál történik meg. Az IP megköveteli, hogy minden kapcsolatnál az MTU legalább 68 byte legyen, ez alatti értéknél az adott hálózatnak kell a fragmentációt elvégeznie (a 68 byte a maximálisan 60 byte méretű IP fejrészből és 8 adat byte-ból áll). Az IP implementációknak nem kell tudniuk kezelni a 576 byte-nal nagyobb fragmentálatlan datagrammokat, de általában az alkalmazások 8192 byte körülíleg képesek erre (ez ritkán alacsonyabb 1500 byte-nál).

IP címtartományok

Az IP cím egy 4 byte-os integer, amelyik a network (LAN) azonosító részből és a host azonosítóból áll. Az IP cím teljesen független az Ethernet címtől, konfigurálható és az adott gép (hálózati csatlakozás) egyértelmű IP szintű azonosítását teszi lehetővé. A címtartomány a routing (útvonalkijelölés) számára egyszerű módon lett kialakítva. Minden, az Internethez kapcsolódó interfésznek egyéni IP címmel kell bírnia, ami a network cím (netid, domain) és a host ID (hostid) azonosítókból áll.

A címtartomány általában az ún. Dotted Decimal Notation-ban van feltüntetve: ekkor minden byte-ot egy decimális számmal jelölünk, és ezeket . -al választjuk el. Fontos tudni, hogy ha a számok 0-val kezdődnek, akkor a rendszer azokat oktálisként (és nem decimálisként) értelmezi, azaz pl. a 195.228.21.011 (oktális) cím a 195.228.21.9 decimális címnek felel meg (l. /etc/hosts „szép” formátumra hozása).

A hálózati azonosító alapján A, B és C osztályú IP címeket, valamint egy D ún. multicast (hostok csoportjának megcímezése) és egy fenntartott E tartományt különböztetünk meg:

osztály	első 4 bit	network bitek	host bitek	IP kezdet
A	0XXX	7	24	1 - 127
B	10XX	14	16	128 - 191
C	110X	21	8	192 - 223
D	1110	28	multicast	224 - 239
E	1111	28	fenntartott	240 - 255

osztály	network max.	host max.	címtartomány	network cím	host cím
A	128	16 777 214	1.*.*.* - 127.*.*.*	a	b.c.d
B	16 384	65 534	128.*.*.* - 191.*.*.*	a.b	c.d
C	2 097 152	254	192.*.*.* - 223.*.*.*	a.b.c	d

Az ún. network és broadcast címek minden network esetén fenn vannak tartva. Például a 195.228.21 C osztályú hálózat esetén a 195.228.21.0 és a 195.228.21.255 értékek fenn vannak

tartva az ilyen broadcast számára.

A 127-el kezdődő cím az ún. loopback címre utal, ami a 127.0.0.1. Ez a gép belső interfésze (lo0), amin keresztül saját magának csomagot küldhet a számítógép. Például a 195.228.21.4 cím esetén (connt.conet.hu) a 195.228.21 adja meg a hálózatot (conet.hu), míg a 4 a gép nevét (connt).

Világos, hogy az A osztályú címeket a legnagyobb hálózatok számára osztják ki, míg a C osztályú címek kicsi hálózatok számára elegendőek csak. Mivel a hostok számának gyarapodása miatt sok hálózat a B osztály méretébe csúszott, ezért a szabad B osztályok száma rohamosan csökkent (IP Address Exhaustion). A megoldás a problémára az IPv6 (IPng).

A címeket az Internet egyetlen központi szerve, a Network Information Center (NIC) adja ki.

A hostoknak a fenti 4-byte-os címek mellett egy - talán jobban megjegyezhető - névvel is el szokták látni. Ezeket a /etc/hosts állományba is be szokás jegyezni:

```
127.0.0.1    localhost
195.228.21.5 risc.conet.hu
195.228.21.1 conalf.conet.hu
195.228.21.2 router.conet.hu
195.228.21.4 connt.conet.hu
```

Sok szimbolikus név (pl. Internet) esetén nem lehet minden host nevét és IP címét ide beírni, ekkor a hálózatban található DNS (Domain Name Server) funkciót kell használnunk, ami a hostnév -> IP cím konverziót biztosítja.

Alhálózatok (subnetting)

A sztatikusan kiosztott IP címtartományok nem oldották meg az egyes hálózatok problémáját: pl. B osztályú címek esetén a lehetséges 64 k host azonosítóját felesleges a routernek tartalmaznia. E helyett a host címtartományból kiválaszthatunk egy részt (pl. egy byte-ot B osztály esetén), és ezzel további alhálózatokat hozhatunk létre egy szervezeten belül (természetesen ekkor routerek választják el az egyes alhálózatokat is). Az IP cím ekkor három részből áll:

(network cím)(alhálózat cím)(host cím)

Pl. a 157.181 hálózaton a 157.181.6 és a 157.181.81 különböző alhálózatokat (pl. különböző épületeket) jelöl.

Pl. a 195.228.21 C osztályú hálózat esetén a két alhálózat lehet a 195.228.21.1 - 195.228.21.14 és a 195.228.21.17 - 195.228.21.30 tartomány.

Az adott alhálózaton a broadcast/multicast üzenetek (csupa 1 ill 0) ugyanúgy kezelhetők, mint a „tisztá” IP osztályok esetén.

Az alhálózatokat létrehozhatjuk ugyanakkora mérettel (ugyanaz a subnet maszk) (static subnetting), de különböző méretet (maszkokat) is rendelhetünk hozzájuk (variable length subnetting). A korszerű hálózati routerek képesek egy adott hálózat esetén a kétfajta alhálózat struktúráját együtt kezelni.

Az IP címek közül bármelyik címtartományt felhasználhatjuk privát használat esetén, de ekkor tudnunk kell, hogy az Internethez így nem tudunk később sem csatlakozni (ill. csak teljes átcímzés vagy más, pl. vasfüggöny vagy proxy szerver segítségével). A NIC a következő (nem egyedi) címeket tartja fenn a privát hálózatok részére:

10	1 db A hálózat
172.16 - 172.31	16 folytonos B tartomány
192.168.0 - 192.168.255	256 folytonos C hálózati cím

A privát címzés egyben járulékos biztonsággal is szolgálhat.

Célszerű sorrend privát hálózat esetén először a belső hálózat megtervezése, majd ezután az esetleges külső kapcsolat kialakítása.

Az IP v6 /IP The Next Generation IPng

Az Internet gyors növekedéssel napjainkra 10 milliós nagyságrendű hostot köt össze egymással. A 32 bites címzés ellenére (ami 4 milliárd hostot jelenthet) a viszonylag egyszerű (és pazarló) hálózati címtartomány kiosztás címhiányhoz vezetett. Ezen az alhálózatok és a folytonos C tartományok bevezetése sem képes hosszab távon segíteni, ezért szükségessé vált az új IP struktúra létrehozása.

Az új IP version 6 (IP The Next Generation, IPng) a következők tulajdonságokkal bír:

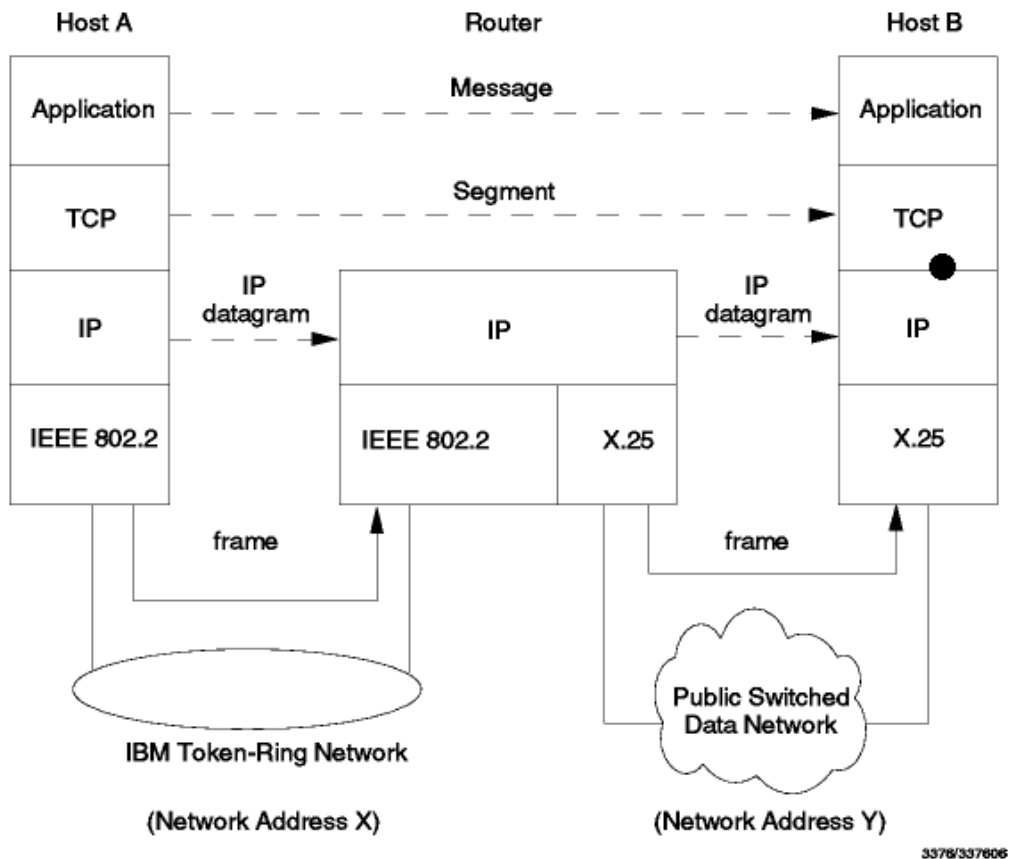
- nagy címtartomány (128 bit): kb. 10^{12} hálózat, kb. 10^{15} host.
- az IPng megengedi más protokollok becsomagolását
- az IPng egyidejű hang és kép átvitelére is képes
- az IPng megfelelő hitelesítési és titkosítási eszközökkel rendelkezik
- az IPng és a klasszikus IP között viszonylag egyszerű az átjárás, világos az átmenet és a kettő egyszerre is tud működni.

Az IPng az IP-ből kifejlesztett Simple Internet Protocol Plus (SIPP) algoritmusok alapján lesz kifejlesztve.

4. IP routing

Az IP szint fontos feladata a routing, azaz az IP csomag eljuttatása a forrás IP címről a cél IP címre.

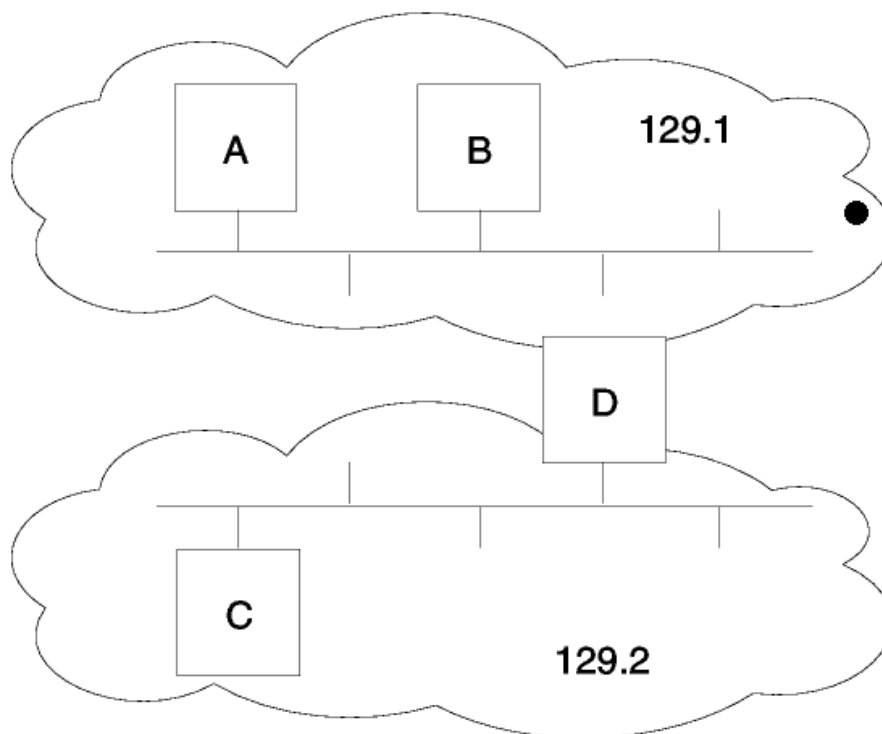
Az IP ezt a TCP/IP réteges felépítésének felhasználásával végzi el.



Az IP datagram az X hálózaton lévő A hostról az Y hálózaton lévő B hostot két fizikai hálózaton keresztül éri el.

Ha a két cím hálózati címe megegyezik (beleértve az esetleges alhálózatot), akkor az ARP alapján meghatározott fizikai címre kell elküldeni az IP csomagot. Ez a közvetlen (direct) routing.

Közvetett (indirect) routing esetén a cél host hálózata nincs közvetlenül összekötve a küldő hálózatával. Ilyenkor csak router segítségével lehet a kapcsolatot kiépíteni. A küldő host csak a legelső, a célhálózat irányába vezető routert kell, hogy ismerje: a csomag további irányítása a router(ek) feladata.



Közvetlen és közvetett IP route: Az A host közvetlen routinggal éri el a B és D hostokat, közvetetten pedig a C hostot. A D host a router a 129.1 és 129.2 hálózat között.

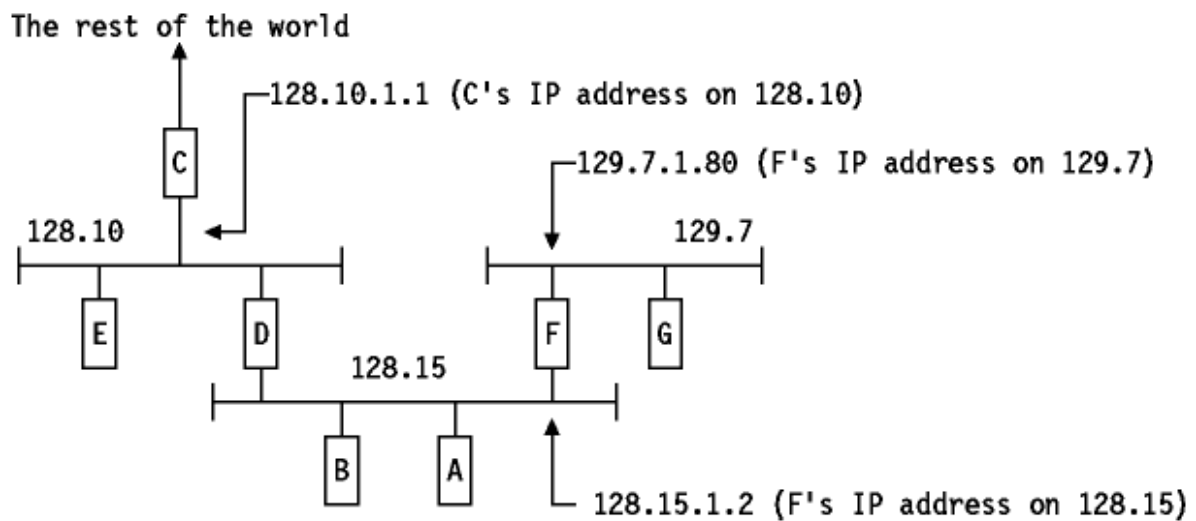
Az IP protokoll lehetőséget az az explicit, ún. source routing használatára: ekkor a küldő az IP csomagot ellátja a megadott célhost eléréséhez szükséges útvonaljelöléssel. Az IP ekkor tartalmazza, hogy milyen routereken keresztül, milyen sorrendben merre kell a csomagot (valószínűleg a célhoz) továbbítani. Ilyet használ pl. a Serial Line Internet Protocol (SLIP) protokoll, amelyik struktúrája miatt nem ismeri a két oldal IP címét. Általában azonban a routing a cél és a küldő host hálózati és alhálózati címei alapján történik.

Az IP routing tábla

Minden host az IP routing táblában tartalmazza a cél IP címek eléréséhez szükséges routing információt. A tábla három típusú elérést tartalmaz:

- közvetlen utat a helyi hálózathoz
- közvetett utakat az egy vagy több külső hálózaton található hostok eléréséhez
- a alap elérési utat (default route), amely az előző kettő által nem tartalmazott kapcsolatok kiépítésére használt.

Példa:



A D host routing táblája a következőket tartalmazza:

cél	útvonal
128.10	közvetlen kapcsolat (direct attachment)
128.15	közvetlen kapcsolat (direct attachment)
129.7	elérés a 128.15.1.2 routeren keresztül
default	a 128.10.1.1 router

Belső és külső routing

Az ARP protokoll

Az IP címek kapcsán látható volt, hogy az IP kapcsolat kiépítésekor feltétlenül szükség van az Internet cím alapján a távoli gép fizikai (pl. Ethernet) címére: ez kell a kapcsolat kiépítéséhez.

Ezt a feladatot az ARP protokoll (Address Resolution Protocol) valósítja meg, amely szigorúan véve nem IP protokoll.

Az ARP egy helyi cache táblát használ, és amennyiben az adott IP címhez tartozó fizikai cím itt nincs meg, akkor az ARP egy speciális csomagban szétküldi az célhost Internet címét a hálózaton.

Az ARP kérések ún. broadcast kérések, amiket az ff:ff:ff:ff:ff:ff Ethernet címre küld az ARP. Minden gép figyeli ezeket az ARP csomagokat, és ha azt látja, hogy őt szólították meg, akkor egy ARP csomaggal válaszol. Természetesen broadcast nélküli kapcsolatokon (pl. SLIP, X25, Serial Optical Channel Converter) az ARP üzenet nem kerül átvitelre.

A hardver cím és a routing információ (bridge esetén) a helyi gép ARP cache tárolójába kerül, így elkerülők a gyakori ARP kérések.

Az ARP kérésre válaszoló host automatikusan elmenti a kérdező hardver és IP címét az ARP cache táblába.

Az ARP tábla 20 perc után törli a nem aktívan használt bejegyzéseket.

A RARP protokoll

A Reverse Address Resolution Protocol (RARP) egy speciális protokoll, amely lehetővé teszi a hálózati eszközök számára IP címük megismerését a fizikai (pl. Ethernet) cím alapján. Ilyenek pl. a diszknélküli munkaállomások, terminálszerverek, X terminálok, nyomtatók.

Az Internet Control Message Protocol (ICMP)

Egy router vagy cél host az ICMP segítségével informálhatja a küldő hostot a datagrammal kapcsolatos problémákról.

A traceroute parancs

A traceroute parancs a hálózat ellenőrzéséhez használható. A program ICMP segítségével térképezi fel egy célhosthoz vezető hálózati utat.

A traceroute először egy IP datagrammot (igazából egy UDP csomagot egy nem használt portra) küld TTL=1 mezővel a célhoz. Az első router a TTL mezőt csökkenti, majd egy ICMP Time Exceeded üzenetet küld vissza. Ezután egy TTL=2 üzenetet küld ki a program, s. í. t. feltérképezi a célhoz vezető utat.

A Packet InterNet Groper (PING)

A ping a legegyszerűbb TCP/IP aplikáció, amely egy echo reply mezővel ellátott IP csomagot küld a célhost felé, és méri a visszatérési időt.

A ping az ICMP echo és echo válasz üzeneteit használja, és (természetesen) nem igényel külön szerveret.

Általában ha egy host ping segítségével elérhető, akkor pl. telnet vagy FTP is el tudja érni. A különböző biztonsági eszközök terjedésével (pl. vasfüggöny) ez már nem mindig igaz.

Az Internet Group Management Protocol (IGMP)

Az IGMP-t az IP hostok arra használják, hogy jelezzék csoporttagságukat minden közvetlenül szomszédos multicast router felé. Az IGMP ezért erősen asszimetrikus protokoll. Minden hostnak, amelyik multicast datagramot akar kapni, egy host csoporthoz kell csatlakoznia. Pl. a 224.0.0.1 üzenet minden adott alhálózaton elhelyezkedő host számára szól (azaz minden alhálózat esetén lokális).

Network menedzsment protokollok

SNMP A Simple Network Management Protocol (SNMP), amely az előző adatbázist kezeli.

Vasfüggöny (tűzfal)

Virtuális saját hálózatok (VPN)