Számítógépes hálózatok
Jegyzet

Ekart Csaba

2017/2018 ősz

Tartalomjegyzék

1. Hálózatok alapjai

2. Internet protokollok és programok

3. Az adatkapcsolati réteg

3.1. Az adatkapcsolati réteg feladatai

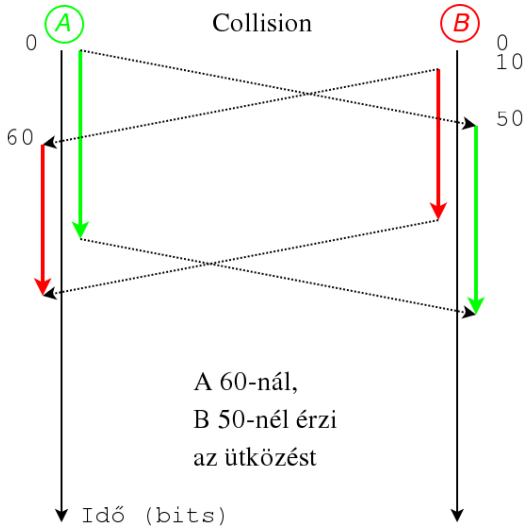
Az adatkapcsolati réteg az OSI hivatkozási modellek második rétege, melynek feladata a hibamentes átvitel biztosítása a szomszéd gépek között, a hibák felismerésével, és javításával. Amennyiben egy időben többen is hozzáférnek a fizikai réteghez, képes a hozzáférések vezérlésére (Link Acces Control) Az adatokat tördeli (data frame-ek), illetve továbbítja, hibajavítást és forgalomszabályozást végez.

3.2. Ethernet

Az Ethernet, a DEC, az Intel és a Xerox cégek által kidolgozott alapsávú LAN specifikáció. Számos kábeltípuson legalább 10 Mb/s sebességgel működtethető. Fejlesztése az 1970-es években indult, a Xerox Palo Altoban található kutató laborjában. A 80-as évek elejére a Digital az Intexl és a Xerox közösen fejlesztették tovább az Ethernetet, hogy megszülethessen az Ethernet II. 1985-ben megjelenik az IEEE 802.3 szabvány (a névben található 802 az 1980 februárjára utal). Ez kissé eltér az Ethernet II-től, végül azonban olyan szinten elterjedt lett, hogy máig érkeznek hozzá updateok, melyek egyre gyorsabbá és gyorsabbá teszik a technológiát.

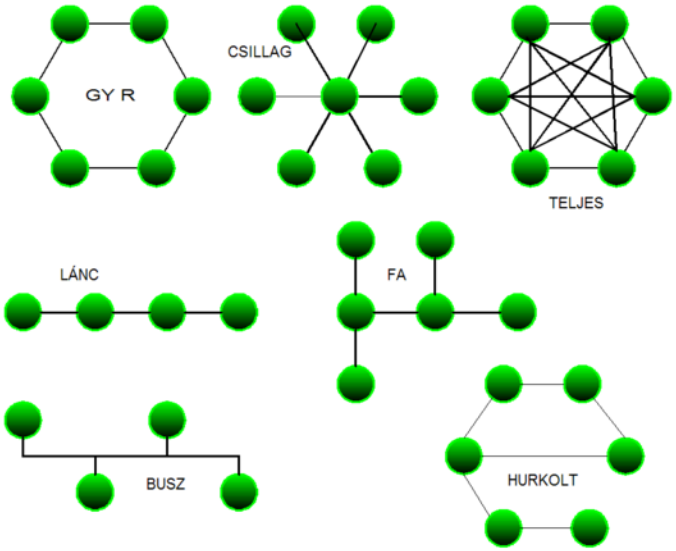
3.3. CSMA/CD

A CSMA/CD a Carrier Sense Multiple Acces with Collision Detection (Vivő Érzékeléses Többszörs Hozzáférés, Ütközéses Detektálással) egy az informatikában használt kommunikációs protokoll, melyben az adni kívánó eszköz ellenőrzi, hogy a csatornán ad e valaki. A Carrier Sense arra utal, hogy az egyes állomások képesek érzékelni a csatornák foglaltságát, és nem kezdenek adásba, ameddig más ad, míg a Multiple Acces egyszerűen úgy fogalmazható meg, hogy a vevők "hagyják elmenni a fülük mellett" a nem nekik szóló csomagokat, de az összeset figyelik (snoopolják). A Collision Detection az a technológia, mely ha adás közben észreveszi hogy ütközés (collision) van, azaz más is ad, megáll, de még 32 ún. "zajbitet" kikürtöl, majd véletlen idejű várakozásba kezd. Ha újra ütközés van újra vár, de hosszabb ideig.



Az ábrán látható módon akkor lép fel ez az esemény, amennyiben a két fél adásba kezd, azonban a latency (válaszidő) miatti csúszás azt eredményezi, hogy egyszerre kezdenek beszélni, ezt azonban észrevéve megoldják a helyzetet a fent ismertetett módszer segítségével.

3.4. Hálózati topológiák



3.5. Az ethernet, mint fizikai réteg

Az alábbi ethernet kábelek technológiája szerint az alábbi típusokat különböztethetjük meg:

- **10base2:** vékony (thin) ethernet, busz topológia jellemző. Már régen elavultnak számít, azonban még mindig találkozhatunk ilyennel. Egyetlen berendezés hibája leütheti az egész hálózatot
- **10baste-T** Szintén elavult, a 10base2-hoz hasonlóan. Cat3 kábelezéssel 10 Mb/s sebességre is képes
- **100base-TX** Manapság a leggyakoribb típus, ezzel találkozhatunk a legtöbbször. Cat5 csavart érpáron 100 Mb/s sebességre képes. Az UTP kábel 8 eréből csak négy használatos, melyből 2-2 adásra, illetve vételre alkalmas. Időnként cross kábelekre van szükség, hogy az állomás eltudja dönteni, melyek az adó és vevő kábelek.

- **1000base-T** 1000 Mb/s sebességre képes Cat5 csavart érpáron. Itt már mind a 8 ér használatos, melyből mind a négypár ad és vesz is (kb. 250 Mb-al), és nincs szükség crosskáblere :)
- **1000base-TX** Akár 1 Gb/s Cat6 csavart érpáron, melyen 2 érpár használatos. Azonban se a technológia, se úgy általában a Cat6 nem terjedt el.

3.6. Kábelek

Rézkábelek

Két fajta rézkábelt különböztetünk meg nagy általánosságban. Az első kategória az UTP (Unshielded Twisted Pair), mely az elterjedtebb, illetve az ScTP (Screen Twisted Pair).

Optikai kábelek

Az optikai kábelek a réz kábelekkel szemben a fény segítségével közvetítenek információt, kihasználva a teljes visszaverődés jelenségét. Az optikai kábelek két fő típusa: q

100base-TX Manapság a leggyakoribb típus, ezzel találkozhatunk a legtöbbször. Cat5 csavart érpáron 100 Mb/s sebességre képes. Az UTP kábel 8 eréből csak négy használatos, melyből 2-2 adásra, illetve vételre alkalmas. Időnként cross kábelekre van szükség, hogy az állomás eltudja dönteni, melyek az adó és vevő kábelek.

- **Multimódusú: (MMF- Multi-Mode Fiber)** Az ilyen típusú optikai kábelekben a fény több úton halad az tlagosan 50-100 micros átmérőjű kábelekben. Előnye, hogy viszonylag olcsó, viszont a kábelhossz nem haladhatja meg a 2 km-t. A nagyságrendekből következik, hogy leginkább épületeken belül alkalazható.
- **Single Módusú: (SMF - Single-Mode Fiber** A fény nem szórodik ("pattog") a kábelben összevissza, hanem egyenesen halad, ezért alkalmaznak lézert. Előnye, hogy sokkal nagyobb rávokon is használható marad, azonban a kábel átmérőjének vékonysága (10 mikron), illetve a lyukba való "nehezebb betalálás" miatt viszonylag drága.

3.7. Media Acces Control

A MAC, azaz a közeghozzáférés-vezérlő a hét rétegű OSI modell Adatkapcsolati rétegének egy alrétege. Biztosítja a címzést és vezérli a közeghozzáférést, ami számos, egy osztott közeget használó többes hozzáférésű hálózaton belüli csomópont számára teszi lehetővé a kommunikációt - így az ethernetnek is egy rétege, funkcióhalmaza. A címzésen kívül a különböző hibák detektálása (Bit hiba, protokoll hiba, médium hiba) is feladata.

3.8. Frame struktúra

Az Ethernet hálózatokon az adatok úgynevezett keretekben (frame, illetve data frame-nek is szokták nevezni) kerülnek továbbításra. A keretek lényegében részekre osztott bit sorozatok, melynek főbb részei a cél számítógép azonosítója, a forrás számítógép azonosítója, maga a küldendő adat, valamint egy ellenőrző kód mely a keret hibátlan megérkezésének megállapítására szolgál. Az Ethernet keretek maximális mérete 1582 byte lehet. Ez az érték a küldendő adaton kívül a keretinformációkat is tartalmazza. Egy ábra segítségével szemléltetnénk egy Ethernet frame logikai felépítését, ugyanakkor meg kell jegyeznünk, hogy az ábrán látható frame a különböző Ethernet szabványoknál eltérhet.

Preambulum (7 byte)
Start Frame Delimiter (1 byte)
Cél cím (6 byte)
Forrás cím (6 byte)
Hossz vagy típus (2 byte)
Adat (max 1500 byte)
Pad (tömítés - ha kisebb, mint 46 byte)
CRC (4 byte)

A preambulum (előtag) által hordozott kezdőinformációt az ethernet framek küldésének időszinkronizációjához használják. Gyakran együtt említik a Start Frame Delimiterrel.
A cél állomás címe és a feladó számítógép címei jelentik a MAC címet. Fontos megjegyezni, hogy nem feltétlenül a célszámítógép címe látható itt, ez attól függ, hogy ugyanazon az ethernet hálózaton vagynk e. Ebben az esetben különböztethetjük meg az unicast címzést (egyetlen állomásnak), a multicastot (több állomásnak), és a broadcastot (minden állomásnak az etherneten).
A típus rész az ethernet keretben arra szolgál, hogy a felsőbb rétegeket informálja arról, hogy az adat rész milyen protokollt használ.
A pad rész arra ügyel, hogy az adat legalább 46 byte legyen. Ha kisebb lenne kiegészítjük.
A CRC a cél címtől az adat vagy a pad végéig számolja a küldő és a fogadót is. AMennyiben hibát jelez a feladó eldobja a csomagot.

3.9. MAC címek fajtái

MAC cím	Cím mező
Világállandó	*0:**:**:**:**:** *4:**:**:**:**:** *8:**:**:**:**:** *C:**:**:**:**:**
Lokálisan kiosztható	*2:**:**:**:**:** *6:**:**:**:**:** *A:**:**:**:**:** *E:**:**:**:**:**
Multicast	*1:**:**:**:**:** *3:**:**:**:**:** *5:**:**:**:**:** *7:**:**:**:**:** *9:**:**:**:**:** *B:**:**:**:**:** *D:**:**:**:**:** *F:**:**:**:**:** Kivéve a broadcast cím
Broadcast	FF:FF:FF:FF:FF:FF

3.10. Repeater, HUB

A repeater és a HUB ethernet szegmenseket köt össze, a fizikai jelek ismétlésével kommunikál, továbbítja a beérkezett adatokat. A repeaterek a tulajdonképpeni fizikai jellel dolgoznak, anélkül hogy bármi módon megpróbálnák értelmezni az átvitelre kerülő adatokat. Ez az OSI modell 1. szintjének, a fizikai rétegnek felel meg.
A hub a hálózati szegmensek egy csoportját egy hálózati szegmensbe vonja össze, és egyetlen ütközési tartományként láttatja a hálózat számára. Az egyik csatlakozóján az érkező adatokat továbbítja az összes többi csatlakozó felé.

3.11. A switch és a bridge

A switch egy aktív hálózati eszköz, mely a rácsatlakoztatott eszközök között adatáramlást valósít meg, többnyire az OSI modell adatkapcsolati rétegében dolgozik. A fizikai rétegbeli feladatokat ellátó hubokkal szemben az ethernet switchek az adatkapcsolati rétegben megvalósított funkciókra támaszkodnak. A portok között nem fordul elő ütközés, ezért saját sávszélességgel gazdálkodhatnak, nem kell osztozni a többiekkel. Megtanulja hogy az egyes interfészeken milyen MAC-címek vannak, így csak arra küldi tovább a frame-t, amerre kell. Előnye a repeaterrel szemben, hogy kíméli a sávszélességet, és a hibás frameket nem továbbítja. Lehallgatás ellen is védelmet jelenthet.

3.12. A törpe és az óriás frame

Kétféle frame-et különböztethetünk meg a méretük alapján

- **Runt (törpe) frame:** A slot timenál (64 byte) kisebb (46 byte adat). A kártya eldobja.
- **Giant (óriás) frame:** Az 1518 bytenál nagyobb frame.

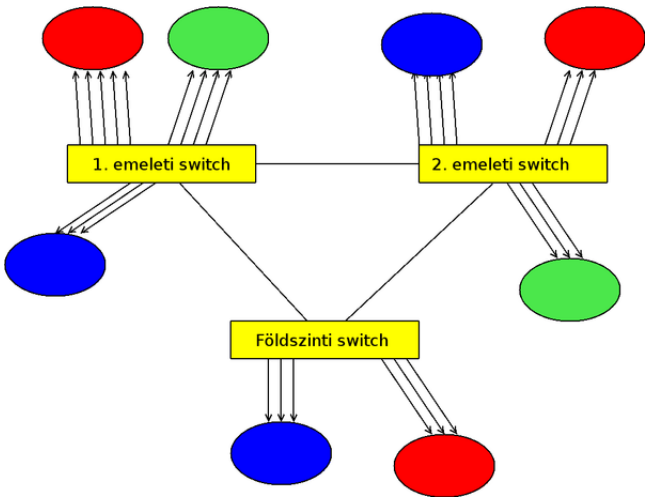
3.13. Link halmozás (aggregation)

Link halmozásnak nevezzük, ha két vagy több fizikai összeköttetést logikailag egynek tekinthetünk. Az aggregált összeköttetés a magasabb szintek számára egynek látszik.

3.14. Virtual LAN

Virtual LAN-ról akkor beszélhetünk, ha egy fizikai ethernetet logikailag több részre osztunk. Ekkor csak valamilyen magasabb réteg segítségével (pl. routerrel) kommunikálhatunk az egyes VLAN-ok közt. Előnyei közé tartozik a biztonság, a jó kezelhetőség, és az erőforrás takarékosság.
A VLAN tageket azért használjuk, hogy az ethernet frameket újra ethernetbe csomagoljuk. Ez összeáll:

- A cím mezők után 4 extra byte
- 2 byte: 802.1Q típus
- 12 bit: VLAN id



3.15. Spanning Tree protokoll (feszítő fa)

Az STP tulajdonképpen fizikailag létező redundáns útvonalakkal rendelkező hálózaton teszi lehetővé, hogy minden cél csakis egy útvonalon legyen elérhető. Ha kör található a hálózati topológiában, akkor a csomagok körbe körbe tudnának vándorolni egy végtelen keringés során (broadcast storm), mely felemészti mind a

kapcsoló, mind a számítógép erőforrásait. A módszer során a switchek kiválasztanak egy rootot, ami a legkisebb serial numbert birtokló lesz. A rootból minden más eszközhöz kiválasztják a legrövidebb utat, majd azokat az összeköttetéseket, amelyek nem szerepeltek kikapcsolják. Mivel az elemek redundánsak, ha kiesik egy eszköz vagy link van rá esély, hogy az egész hálózat élve marad.

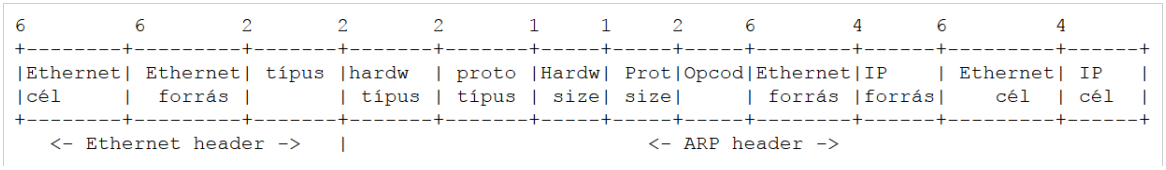
4. ARP, RARP, BOOTP, DHCP

4.1. Hogyan tudja meg a link layer (ethernet) címet egy hálózati állomás?

4.1.1. ARP

Az **ARP (Adress resolution Protocol)**, azaz a cífeloldási prtokoll az informatikában a számítógépes hálózatokon használatos módszer az IP-címek és fizikai címek egymáshoz rendeléséhez. Elsősorban az etherneten használják.
Felmerülhet a kérdés, hogy miért nem használjuk a MAC címeket, akkor nem kellene ekkora "hűhó"-t csapni, és ezen gondolkodni. A probléma azonban, hogy a MAC cím nem strukturális nem tudjuk hol van az akinek küldeni akarunk.

4.2. Az ARP csomagformátum



- 4 byte - 32 bites sorokból áll
- Az információk amiket tárolunk egy ARP csomagban
  - **Hardver típus:** általában ethernet.
  - **Protokol típus:** Általában IP (0x800).
  - **Hardver cím hosszúság:** Úgy találták ki az ARP-t, hogy ne mcsak etherneten és IP-n működjön, tehát muszáj megadni. Ez ethernet cím 6 byte hosszúságú.
  - **Protokoll hossza:** Attól is függ, hogy milyen fajta az IP, de általában 4 byte.
  - **Opcode:** Attól függ, hogy milyen típusú az adatkérésem: 1 - , ha kérdés, 2 - , ha válasz, 3 ha RARP request, 4 - , ja RARP válasz

Ezeket az információkat broadcastelem. A target hardware address üres marad, mert azt nem tudom. Ő észreveszi, hogy neki szól ez a csomag, mert felismeri a saját IP-címét, és kitölti a hiányzó mezőt. Ő már tudja, hogy a választ hova kell küldeni, ezért az már unicast.

Probléma Ha mindenki ezt használja az nem elég hatékony, túl sok csomag utazik egy hálózatban. Ezt csak akkor csinálom ha tényleg nem tudom kiről van szó, egyébként betesszük a cache-be és elraktározzuk. Ha ott van, akkor inkább innentől kezdve kivesszük onnan a címeket.

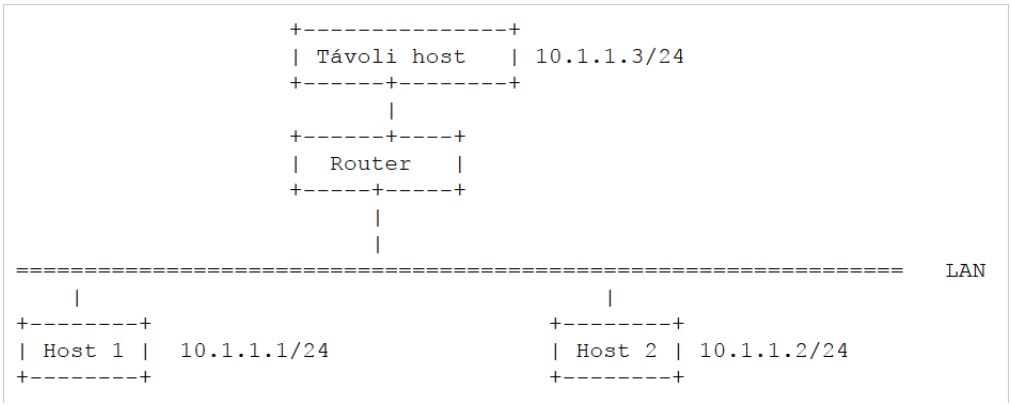
4.3. ARP kérés nem létező hostra

Amennyiben a broadcastünkre nem érkezik válasz, még a biztonság kedvéért megprobáljuk párszor, de egy idő után feladjuk, és egy felsőbb réteggel közüljük, hogy a művelet sikertelen volt.

4.4. Proxy ARP

A Host1-ből küldenék a távoli hostnak csomagot (pl. képet). Feladom a hálózatra a broadcast üzenetem, de senki nem válaszol, hiszen a broadcast üzeneteket a routerek nem továbbítják. Amúgy se mennénk sokra ha megtudjuk a hardver címet, mert ha másik hálózatbban van a célpont, akkor azt a hajunkra kenhetjük, úgy se tudjuk a cím alapján neki elküldeni.
Tehát először a routerhez juttatjuk a csomagot, aki megvizsgálva a kérésünket megállapítja, hogy az ő hálózatában lévő címet kerewssük e, és azt hazudja magáról hogy ő a címzett. A host elküldi a routernek, majd ó tovább küldi a tényleges címzetnek.

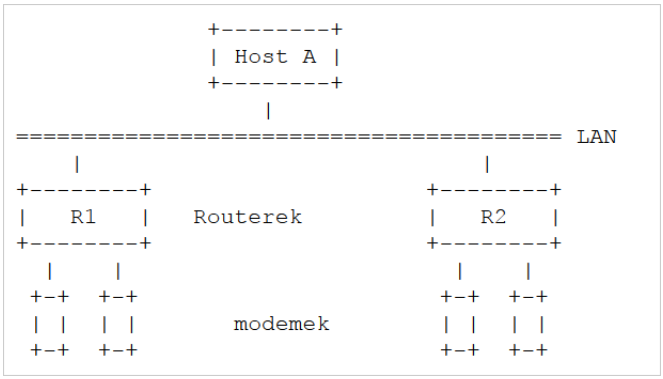
Probléma Sajnos ez nem mindig a legjobb megoldás, maximum kis hálózatokban. Erre találták ki a Default Gatewayt. A host nem adja fel az ARP kérést, mert tudja, hogy bonyolult és inkább a default gatewaynek küldi az üzenetet, ami majd rendelkezik annak a sorsáról.



4.5. UNARP

Ha az egyik gép például megtanulta a cachéből, hogy hol van egy gép, és melyik routeren keresztül elérhető, szembesülni kel lazzal a problémával, hogy mi van ha ezt a gépet átkötjük egy másik hálózatra. Ekkor a host összezavardik.

Megoldás Válaszüzenetet küldünk, tehát broadcastként mindenki, aki megkapja kitörli a saját cachéjéből az adatot.

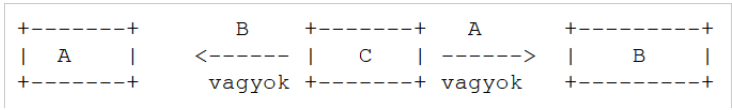


4.6. Gratuitous ARP

Akkor merül fel a kérdés, ha egy adott cím létezik már a hálózatban, ezért a saját IP címére kiad egy ARP kérést, amelyre ha kap választ, akkor a cím nyilván foglalt.

4.7. ARP cache poisoning

Abban az esetben beszélünk ARP cache poisoningről, ha az ARP cache tartalmát hamis üzenetekkel megváltoztatják. Az ARP cachébe hamis infó kerül, ami miatt másnak küldjük a dolgokat.
Ehhez kapcsolódó téma a **Man In The Middle támadást**, mely összezavarja az egymásnak üzenő feleket, és elhiteti a másikkal ,hogy ő az akinek üzenni akar. Ekkor a kér fél nem egymásnak fogja küldeni az adatokat, hanem a támadónak.



Az IP címeket sajnos nem úgy tervezték, hogy alapból fel legyenek készülve efféle biztonsági résekre, azonban elég jó megoldások léteznek ennek megakadályozására (pl. bevasalás)
Az olyan helyzetekben ahol a forgalom nagy része például egyetlen router felé irányul könnyű és igen célszerű támadási módszer lehet.

4.8. Ettercap

Az ettercap egy ARP hamisításon alapuló eszköz, hallgatózásra, Man In The Middle támadások végrehajtására alkalmas. Grafikus felülettel is rendelkezik, pl. a Debian linux része alapból. Diagnosztikai és hibakeresési céllal elég jól felhasználható. Tipikus Script Kiddie eszköz.

4.9. Mi van ha a saját IP-nket nem tudjuk?

Ha bekapcsoljuk egy hálózatba az eszközt, mi van ha ne mtudja a saját IP címét. Manuálisan megoldható lenne persze a kalibrálás, de örülnénk ha magától kitalálná.

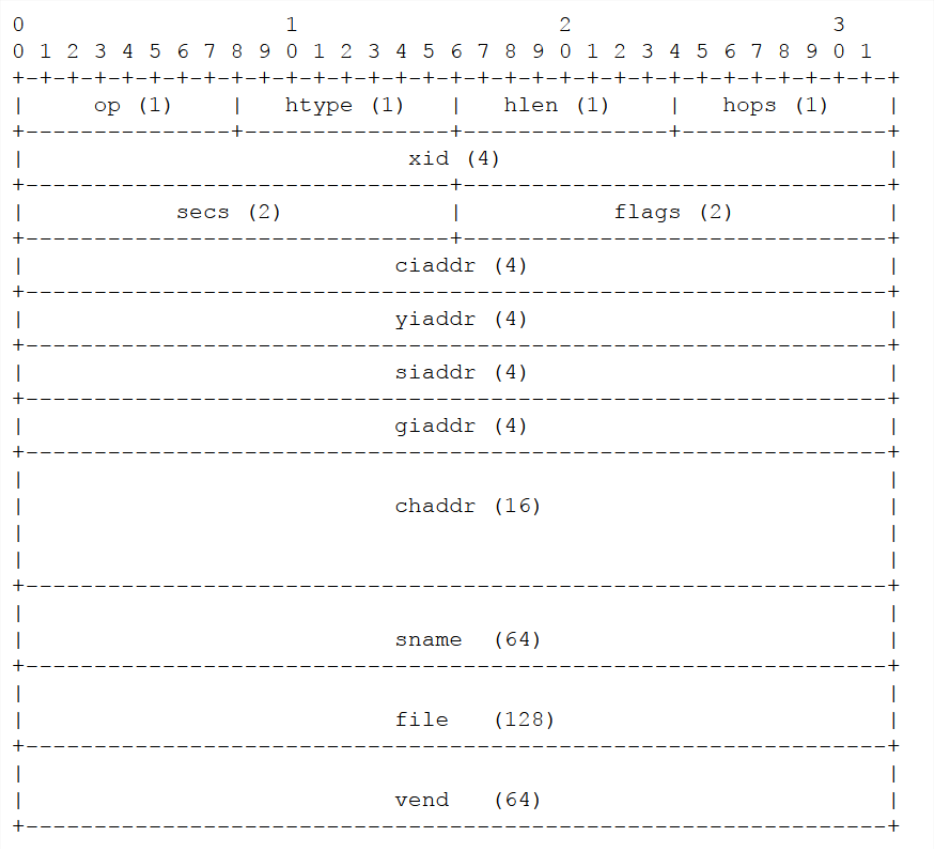
4.9.1. RARP

A legegyszerűbb megoldás a problémára a RARP. Broadcastelünk, melyben megpróbáljuk megtudni a sjaát IP-címünket. Gyakorlatilag úgy töltjük ki az ARP csomagot, hogy a saját adataink hiányoznak belőle, majd broadcastelünk. A RARP szerver megkapja ezt az üzenetet, és készségesen ad egy szabad IP-címet a kérőnek. A válasz természetesen már unicast és tartalmazza az IP és az ethernet címet is.

Hátrány Hátránya, hogy kevés dologra alkalmas, ezzel még nem fog tudni működni a hálózatban, hiszen csak az IP-címét tudta meg. Tudnia kéne a default gatewayt és a netmaskot is.

4.9.2. BOOTP

Talán egy fokkal jobb megoldás, mint a RARP. Az IP címen kívül visszad netmaskot, router címet, boot server host címet, boot fájlnevet stb. Annak ellenére, hogy broadcast üzeneteket használ elég hatékony.



A rendszer felépítése

- **opcode**: 1 - request, 2 reply
- htype, hlen: mint arp-nél
- hop count: a kliens 0-ra állítja, proxy szerverek (= bootp-t közvetítő router-ek) eggyel növelik
- xid: tracnsaction id. Ezzel derül ki, hogy mi mire válasz
- secs: az első bootp kérés óta eltelt idő (a a kliens nem kap választ exponential backoff szerint újra próbálkozik)
- flags: Itt kérheti a legfelső biten a kliens, hogy a BOOTP reply is broadcast legyen
- ciaddr: Client IP address. Kérésben a kliens kitöltheti: ezt kérem
- yiaddr: Your IP address. Ezt a címet kapja a kliens
- siaddr: Server IP address. A következő szerver IP címe, akivel a boot folytatható
- giaddr: Gateway IP address. Ha relé (bootp átengedésre konfigurált router) van, annak a címe
- chaddr: a kliens hardware (ethernet) címe - akkor van jelentősége, ha reléken át éri el a szervert a kliens
- sname: server host name - Annak a szervernek a neve, ahonnan majd az operációs rendszert letöltheted
- file: boot fájlnév (Az operációs rendszeredet tartalmazó fájl, amit le kell töltened)
- vend: különböző kiegészítések (vendor specific information)

4.9.3. DHCP

Még egy fokkal jobb mint a BOOTP. Kompatibilis fele, az üzenet formátum teljesen megegyezik, csak a vend helyett az options szó használatos. Fő előnye, hogy dinamikusan lehet osztani az IP-címeket

- Olyat is lehet osztani, amely eg yidő után lejárhat
- Van egy adatbázisa, amibe be vannak jegyezve a kioszthtató IP címek
- Ha érkezik egy kérés, ő engedélyt ad a kérőnek, hogy az IP-t használha egy bizonyos ideig

Ez a rendszer a dinamikussága miatt előnyös, nehezebben fogynak el az IP-k, és feltételezhetjók, hogy nem nagoyn lesz olyan, hogy mindenki egyszerre van a hálózaton. Mikor a kliens úgy dönt, hogy befejezi a dolgát átengedi az IP-t.

4.9.4. PXE- Preboot Execution Enviroment

Az Intel által készített alternatíva a DHCP-n alapul azt próbálja tovább fejleszteni. Nem foglalkozunk vele részletesen.

5. Adatkapcsolati link (réteg) folytatása

5.1. PPP

A Pont-pont protokoll (általánosan használt rövidítéssel: PPP az angol Point-to-Point Protocol kifejezésből) egy magas szintű adatkapcsolati protokoll kétpontos vonalakhoz. Széleskörűen alkalmazott megoldás az Internetben.

Feladatai:

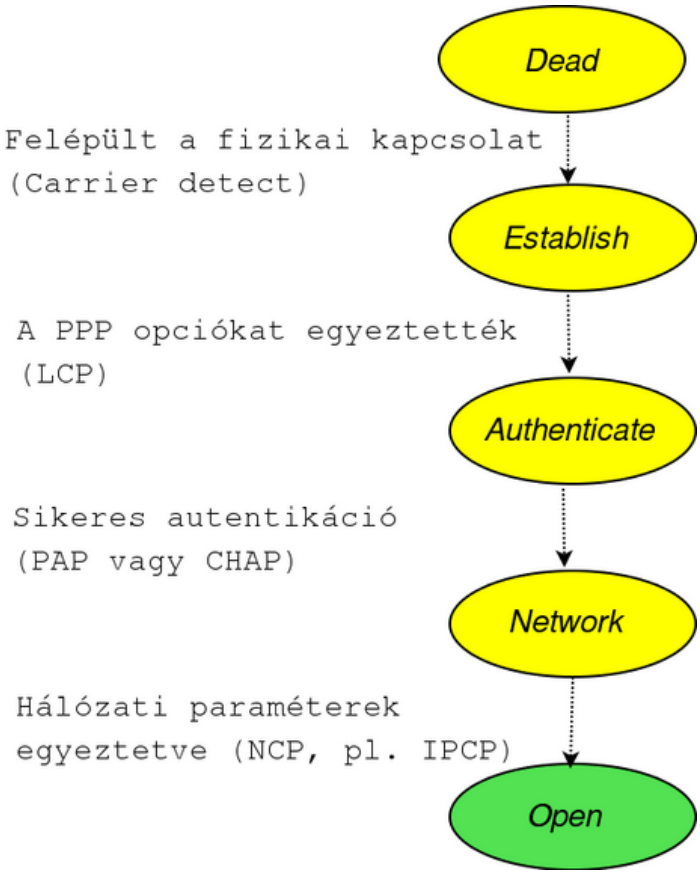
- Frame-ek elkülönítése
- Transzparencia (tetszőleges vyte folyamot át lehessen vinni.
- Hatékony sávszélesség kihasználás
- Hibafelderíítés (CRC)
- Több fajta protokollt támogasson, ne csak az IP-t
- Magasabb protokoll paraméterek egyezését oldja meg (pl. IP címek)
- Többféle fizikai médiumon működhessen

5.1.1. PPP frame szerkezet - ISO HDLC

Flag (1-byte)	Address (1-byte)	Control (1-byte)	Protokoll (2-byte)	Adat	CRC (2 byte)	Flag (1-byte)

- Flag: "Kereteket elválasztó bájt", a frame kezdetét és végét jelzi (jellemzően 0x7e)
- Adress: Egy cím jelzés, igazából azért van PP alapján nem kéne, de mivel felkészültek többféle protokollra ezért úgy döntöttek legyen. (mindig 0xFF)
- Control: Szintén nem olyan fontos.
- Protocol: Ez már érdekesebb, meghatározza hogy az ezt követő adatok hogyan értelmezendők.
- Adat: Általában max. 1500 byte. Mivel a flag jelzi a kezdetet meg a véget, ezért igyekszünk nem használni. Ezért vannak excape byteok. Ha ilyen byteot akarunk küldeni elé teszünk egy escape byteot: 0x7D. Majd XOR-oljuk 0x20-szal. Tehát pl. 7E-ből 7D 5E lesz.
- CRC: a hagyományos ellenőrző kód
- flag: Lezáró bájt

5.1.2. PPP állapotok



Segédprotokollok röviden

- LCP (Link Control Protocol):
  - Kapcsolat felépítés, bontás
  - Paraméterek egyeztetése (Autentikálás, tömörítás, sallangok elhgyása)
- PAP: Password Authentication Protocol:
  - Kliens küldi az azonosítót és jelszót
  - Szerver válaszol hogy rendben van e.
  - Nem biztonságos, lehallgatható, visszajátszható.
- CHAP (challange Handshake Authentication Protocol)
  - Előállít egy random számot (challange)
  - A kapott challengeből és jelszóból választ képez
  - A szerver ellenőrzi
  - Nehezebben lehallgatható, a random szám mindig változik.
- NCP (Network Control Protocol)
  - Hálózati paraméterek egyeztetése.
  - IP esetén IPCP

5.1.3. PPoE

- PPP over Ethernet
- ADSL-nél használatos
- A kommunikációhoz szükséges, mikor IP-nk nincsen még

5.2. Loopback interfész

- Ha egy kliens és egy szerver ugyanazon az eszközön fut, és elindítom a browser-t tudom böngészni ezt a szervert.
- Ehhez nem kell hálózat, mégis tudok futtatni hálózati programokat.
- TCP-IP-vel kommunikálnak de az én gépemen belül Loopback interfésszel: 127.0.0.1
- Minden tekintetben hasonlóan viselkedik mint egy valódi interfész.
- Nem csak számítógépeknél, hanem más dobozoknál, switchek, routerek stb.

5.3. MTU - Maximum Transmission Unit

- A fizikai médium rendszerint korlátozza az átvihető frame méretét.
- Célszerű ennél nem nagyobb csomagokat használni felső rétegen
  - Nem tudhatjuk, hogy a célállomásig milyen közegen, milyen MTU-val megy át a csomag.
  - Elvben lehet a legkülönbözőbb

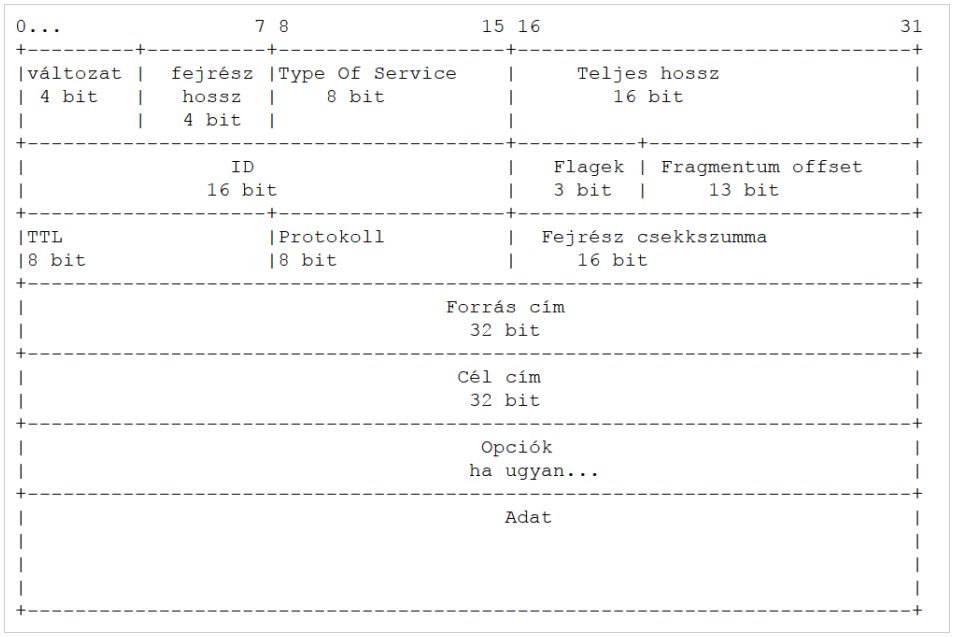
6. Internet Protokoll (IP)

Az internetprotokoll (angolul Internet Protocol, rövidítve: IP) az internet (és internetalapú) hálózat egyik alapvető szabványa (avagy protokollja). Ezen protokoll segítségével kommunikálnak egymással az internetre kötött csomópontok (számítógépek, hálózati eszközök, webkamerák stb.). A protokoll meghatározza az egymásnak küldhető üzenetek felépítését, sorrendjét stb.

6.1. Tulajdonságok

- Nem kapcsolat orientált, az egyes csomagokat a hálózati réteg egymástól függetlenül kezeli. Nincs kapcsolat felépítés, kapcsolat bontás.
- Best effort, decentralizált nem megbízható.
- A felsőbb rétegek feladata, hogy megbízható kapcsolatorientált kommunikáció legyen.

6.2. Rétegek



- Hossz
  - Max 65535 byte
  - MTU korlátozza
- ID
  - A csomagra jellemző egyedi szám
  - Régen statikus volt, ezért megjósolhatóvá vált, visszaélésre adott módot
  - Manapság véletlen szám (tűzfalak tovább randomizálják)
- Flag-ek
  - IP darabolásnál van szerepük
- Fragmentum offszet
  - Ha fragmentált az IP fatagram, azt mutatja ez a darab hova illik

  - Mértékegység: 8 byte
- TTL - Time To Live
  - Az időt hop-ban méri
  - Felső korlátot ad a közbülső routerekre
  - Minden router fekrementálja
  - Ha 0 eldobja a csomagot, ICMP üzenetet köld issza a feladónak
  - Ha nem lenne végtelen ideig keringhetnének a csomagok.
- Protocol
  - Az IP feletti protokollt adja meg (ICMP, TCP, UDP)
- Checksum
- Forrás és célcím
  - Az IP réteg szempontjából a legfontosabb ennek alapján továbbítja (routeolja a csomagot)
  - Tűzfalak még ezt is módosíthatják.
  - Pontozott decimális jelölés

Hivatkozások