Tavasz 2017

UNIVERSITAS SCIENTIARUM SZEGEDIENSIS
UNIVERSITY OF SZEGED
Department of Software Engineering

Számítógép-hálózatok 2. gyakorlat
OSI modell, Ethernet alapok

Bordé Sándor

Tartalomjegyzék

Bevezetés

A mai alkalommal megismerkedünk a hálózati referenciamodellekkel, megemlítjük az OSI és TCP/IP modelleket. Végül áttekintjük az Ethernet szabvány alapjait és az ehhez kapcsolódó fogalmakat.

Hálózati szoftver, réteges tervezés

A számítógép-hálózatok a fejlődésük során egyre összetettebbek és bonyolultabbak lettek, ezért elengedhetetlen volt valamilyen strukturáltság bevezetése. A minél jobb átláthatóság érdekében a hálózatok feladatait, szerepeit egymásra épülő rétegekre osztották fel. Mindegyik rétegnek két feladata van:

1. Valamilyen szolgáltatást nyújt a közvetlenül alatta és felette található rétegnek
2. A szolgáltatás megvalósításának részleteit elrejti a többi réteg elől

Ez a felosztás az informatikában nem ismeretlen, több helyen is előfordul (pl. objektum orientált paradigma). Ennek a felosztásnak a következménye, hogy az egyes rétegek egymástól függetlenek lesznek. A hálózati eszközök gyártóinak, szoftverek fejlesztőinek csak arra kell figyelni, hogy betartsák a rétegek közötti kommunikációra vonatkozó szabályokat (protokoll), aminek köszönhetően anélkül cserélhetjük ezeket, hogy a felsőbb és alsóbb rétegekhez hozzányúlnánk.
Ahhoz, hogy a rétegek zavartalanul együttműködhessenek, pontosan definiálnunk kell minden rétegnek a feladatát (milyen szolgáltatásokat nyújt) és az egymással való kommunikációnak a módját (hogy kapcsolódnak egymáshoz). Az előbbinek a leírására használjuk a referencia modelleket, az utóbbit pedig a protokollok definiálják. A protokollokra a félév során több példát is fogunk látni, most nézzük meg a modelleket kicsit részletesebben.

Referencia modellek

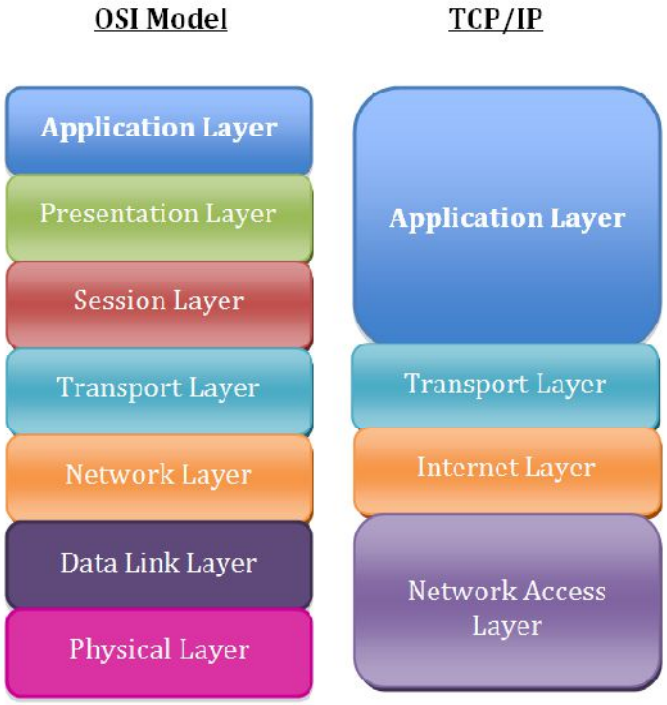
Ahogy az előző bekezdésben szerepelt, a referencia modellek arra szolgálnak, hogy leírják a hálózati architektúra rétegeit, illetve azok feladatait. A két legfontosabb referencia modell az OSI és a TCP/IP.

OSI modell

Az OSI modell az ISO (International Standards Organization), szabványokkal foglalkozó szervezet ajánlásán alapszik. Ez egy hét rétegű elméleti modell, ami definiálja, hogy egy hálózatot milyen rétegekre érdemes felosztani, és melyik réteg mit csináljon (a hogyan kérdésével viszont nem foglalkozik).
A modellnek nem része, de készítettek az egyes rétegekhez protokollokat is, azonban ezeket ma (különböző okok miatt) sehol nem használják. Az ok, ami miatt mégis szerepel itt az az, hogy a modell és az egyes rétegek feladatainak leírása elég általános, így jól használható a hálózatok megértéséhez.
Ez a modell hét réteget határoz meg (ld. lejjebb a képen), de ez a felosztás egy kicsit erőltetett: az 5. és 6. rétegnek nem sok feladata van, az alsó három pedig túltelített. A gyakorlat során az alsó 3 réteggel fogunk foglalkozni (ami valójában 4, mert a 2. rétegnek van egy alrétege is). Az egyes rétegek pontos leírását megtaláljátok a könyvben (*Andrew S. Tanenbaum: Számítógép-hálózatok*) illetve az előadás anyagában.

TCP/IP modell

Ez a modell az OSI modellel pont ellentétes sorsra jutott: a protokolljai széles körben elterjedtek (a nevét is a két legnépszerűbb protokolljáról, a TCP-ről és az IP-ről kapta), azonban maga a modell nem túl hasznos.
Ez a modell csak négy rétegből áll (ld. kép), viszont a rétegek feladatai nagyjából megfeleltethetők az OSI modell rétegeinek. Az egyes rétegek részletes leírását szintén a könyvben találjátok.



1. ábra OSI és TCP/IP modell

A gyakorlaton az OSI modell szerint haladva az alsó három réteget fogjuk átvenni, illetve megismerkedünk néhány TCP/IP modellben definiált protokollal.

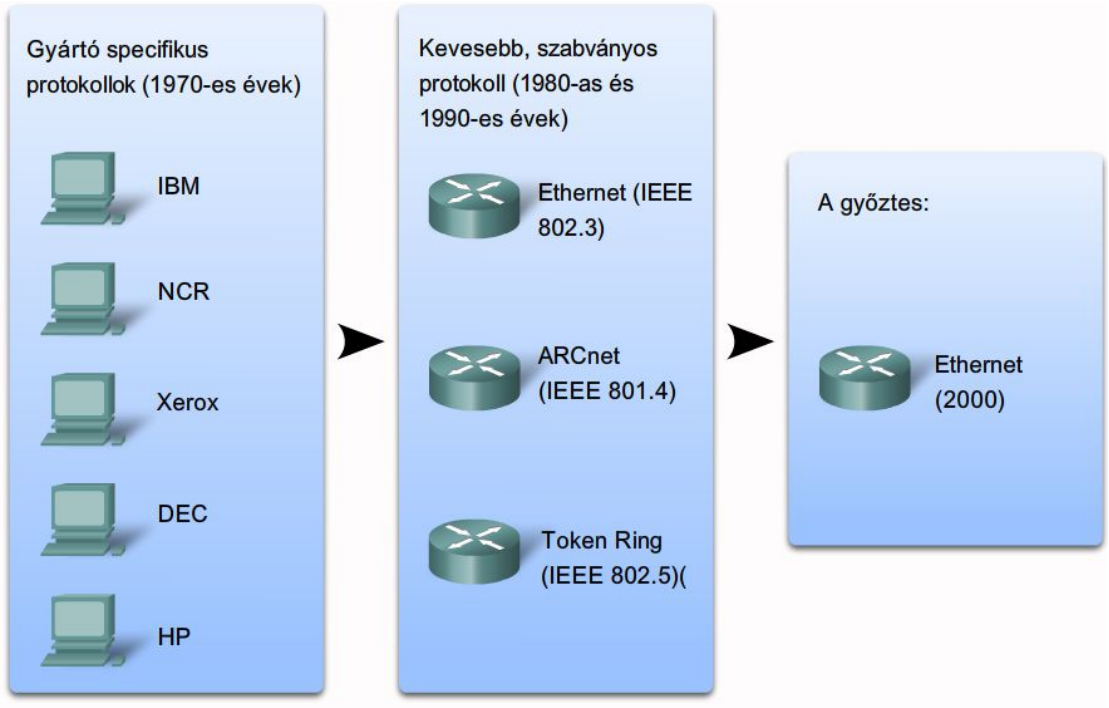
Ethernet

A számítógépek közötti kommunikációban (akárcsak az emberek közötti kommunikáció során) fontos a protokollok (szabályok) betartása. Ha nem azonos protokollt követnének az egyes eszközök, akkor nem értenék egymást – mintha más nyelvet beszélnének. A vezetékes helyi hálózatokon használt leggyakoribb protokoll az *Ethernet*.

Az Ethernet kialakulása

A számítógépes hálózatok kialakulásának kezdetén az egyes eszközök gyártói saját módszereiket használták a hálózati eszközök összekapcsolására és a köztük történő kommunikációra. Azonban, ahogy a hálózatok egyre jobban terjedtek, olyan szabványokra lett szükség, amiket betartva a különböző gyártók eszközei együtt tudnak működni egymással. A szabványok kialakítása egyébként számos előnnyel jár: egyszerűbb a fejlesztés, tervezés, kisebb a gyártóktól való függés, így nő a gyártók közötti verseny.

Bár helyi hálózatoknál nem létezik hivatalos protokoll szabvány, a legelterjedtebb technológia (*Ethernet*) *de facto*[1] szabvány lett.



2. ábra Szabványok egységesítése

A hálózati szabványokat az *IEEE* bizottságai kezeli, ők felelnek az átviteli közegekre, kommunikációs protokollokra vonatkozó szabályok jóváhagyásáért. Az egyes szabványok kapnak egy kódszámot, ami a felelős bizottságot jelöli (pl. a **802.3** az *Ethernet*ért felelős bizottság).

Az *Ethernet* 1973-ban jött létre, és az elterjedésének köszönhetően gyorsan fejlődésnek indult. Az *Ethernet* fejlődésének főbb állomásait a mellékletben láthatjátok.

Fizikai címzés – MAC cím

Mint minden kommunikációban, a hálózaton is egy üzenet küldőjét és címzettjét egyértelműen azonosítani kell. (A valós életben erre használhatjuk a személyek neveit.) Az egyértelmű azonosításnak köszönhetően csak az érintett eszközök dolgozzák fel az üzenetet és válaszolnak rá, a többiek figyelmen kívül hagyják.

Számítógépes hálózaton az ilyen jellegű címzésre szolgálnak a *MAC* (*Media Access Control – közeghozzáférés-vezérlési*) címek. Minden hálózati eszköznek van MAC címe, amit gyártáskor kap. Ez egy megváltoztathatatlan, egyedi azonosító. Üzenet küldésekor az üzenet fejlécébe bekerül a címzett és a küldő MAC címe is. Mindenki, aki kap egy üzenetet, megvizsgálja a címzett címét. Ha ez megegyezik a sajátjával, akkor feldolgozza, és továbbítja a megfelelő alkalmazásának. Ha nem egyezik, akkor figyelmen kívül hagyja.

[1] A *de facto* szabványok olyan szabványok, melyek az adott technológia széles körű elterjedtsége miatt váltak szabvánnyá. Ezzel szemben a *de jure* szabványok bizottságok által deklarált, dokumentumban rögzített szabványok.

Amikor egy Ethernet hálózaton egy állomás üzenetet küld egy másiknak, akkor egy, a szabványban megadott keret szerkezetére formázzák az üzenetüket. Ezeket a kereteket más néven *PDU*- nak (*Protocol Data Unit*) is hívhatjuk. Egy ilyen keret legalább 64, legfeljebb 1528 bájt méretű lehet. Ami ennél kisebb vagy nagyobb, azt a fogadó nem dolgozza fel.

Az Ethernet keret felépítése

Előtag	SFD	a cél MAC-címe	a forrás MAC címe	Hossz/típus	Beágyazott adat	Keretellenőrző összeg
7	1	6	6	2	46-től 1500-ig	4

IEEE 802.3 Ethernet keret mezői

Bájtok	Mező név
7	Előtag
1	Keretkezdet
6	a cél MAC címe
6	a forrás MAC címe
2	Hossz/típus mező
46-től 1500-ig	Beágyazott adat
4	Keretellenőrző összeg (CRC)

3. ábra Egy Ethernet keret szerkezete

Ethernet hálózatok hierarchiája

Mivel csak *MAC* cím szerinti üzenetcímzés túlságosan nehézkes lenne, valamint az *Ethernet* hálózatok sok szórásos adatforgalmat is generálnak (tehát gyakran küldenek olyan üzenetet, amit a hálózat összes állomása megkap), szükségessé vált az *Ethernet* hálózatok hierarchikus felosztása. Ennek segítségével jobban kezelhetők az egyes hálózatok, és biztosítható, hogy a helyi forgalom tényleg helyi maradjon.

Ebben a hierarchikus sémában már használhatunk az állomások helyét is tartalmazó logikai címzést (IP címek). Az IP címeket arra használhatjuk, hogy megllapítsuk a küldő és a fogadó állomás helyét. Az egy hálózatba tartozó eszközök címének hálózati része megegyezik, egy hálózaton belül a hostok címe egyedi.

A hierarchikus tervezés rétegei

Hozzáférési réteg

Ez egy helyi Ethernet hálózat. Az állomások számára kapcsolódást biztosít, rendszerint switcheken vagy hubokon keresztül. A hozzáférési réteg egy hálózatában az IP cím hálózati része megegyezik. Ha a címzett IP címének hálózati része azonos a küldőével, akkor az üzenet helyben marad. Ellenkező esetben az elosztási réteg felé továbbítódik.

Elosztási réteg

Ez a réteg biztosít kapcsolatot az alsóbb réteg beli *Ethernet* hálózatok között. Az információáramlást és a hálózatok közötti kapcsolatot routerek szabályozzák. Szintén a routerek határozzák meg, hogy mely forgalom lépjen tovább a felsőbb, központi rétegbe.

Központi réteg

Ennek a rétegnek a feladata annyi, hogy nagy sebességű, redundáns kapcsolatot biztosítson hálózatok között. A célja a gyors adatszállítás.

Hubok

Az egyik legegyszerűbb hálózati eszköz a hub, a hozzáférési rétegben helyezkedik el. Több portja van, amiken keresztül egy hálózat állomásai csatlakozhatnak hozzá. Nem tudják dekódolni a hozzájuk érkező üzeneteket, nem tudják megállapítani a címzetett. Éppen ezért, ha egy üzenet érkezik hozzá, akkor azt fogadja, regenerálja, és minden portjára csatlakozó eszköznek továbbküldi. Mivel csak az az eszköz dolgozza fel és válaszol az üzenetre, akinek valójában szólt, így ez egy működőképes megoldás.

Azonban a hub összes portja egy csatornán végzi az üzenetek küldését-fogadását, ezért a csatlakozó állomásoknak osztozniuk kell a sávszélességen. Ha mégis egyszerre több állomás próbál üzenetet küldeni, akkor az üzenetek összeütköznek és megsérülnek. Mivel a hub nem tudja értelmezni az üzenetet, így sérülten is továbbküldi.

Egy *ütközési tartományba*[2] tartozó gépek észlelik, ha sérült az üzenet. Ilyenkor a küldők rövid várakozás után megpróbálják újraküldeni az üzenetet. Azonban látszik, hogy minél több állomás van egy ütközési tartományban, annál gyakoribb lehet az ütközés, annál több lesz az újraküldés, és ezáltal az adatforgalom. Ezért ajánlott minél több ütközési tartományt kialakítani a hálózatunkban.

Switch

A *switchek* használatáról már röviden volt szó korábbi alkalommal. Ezek az eszközök szintén a hozzáférési rétegben használt eszközök. Azonban a switch már képes arra, hogy csak egy adott állomásnak továbbítsa a kapott keretet. Ezt úgy valósítja meg, hogy dekódolja az üzenetet, kiolvassa a címzett *MAC* címét, és továbbítja az adott eszköznek.

A *switch* csatlakozott eszközök *MAC* címét egy úgynevezett *MAC-cím* táblában tárolja. Üzenet fogadáskor kikeresi a címzett címét ebből a táblából. Ha megtalálja, akkor felépít egy átmeneti kapcsolatot a küldő és fogadó állomás között. Ezen a kapcsolaton csak ez a két állomás osztozik, így elkerülhető az ütközés.

Ha a *switch* nem találja a cél *MAC* címét a táblában, akkor nem tud egyedi áramkört felépíteni a küldő és fogadó gép között, ezért „*elárasztást*” alkalmaz: mindenkinek elküldi az üzenetet. Ez után az állomások összehasonlítják a címzett címét a sajátjukkal, és amelyiknek egyezik, az feldolgozza.

A *MAC-cím* táblát a *switch* automatikusan építi fel: minden érkező üzenetet megvizsgál, és ha a küldő címe még nincs a táblában, akkor beleteszi.

Előfordulhat olyan eset, hogy a *switch* egy portjához egy *hub* csatlakozik. Ekkor a hubra csatlakozott összes állomás MAC címét a hub portjához rendeli a

[2] Ütközési tartomány: Az a terület, ahol elhelyezkedő állomások ütközés következtében sérült üzeneteket kaphatnak.

címtáblában. Ha egy olyan üzenetet kap, amelyiknek a küldője és fogadója is a hubra csatlakozik, akkor figyelmen kívül hagyja. Ha a hubon ütközés során megsérült egy csomag, akkor azt megkapja a switch is, azonban nem továbbítja azt.

Szórásos üzenetküldés

Előfordulhatnak olyan esetek egy helyi hálózaton, hogy minden eszköznek szeretnénk eljuttatni egy üzenetet. Az *Ethernet* keretbe viszont egy MAC címet írhatunk. Ennek az áthidalására alkalmas a szórásos (*broadcast*) üzenet. Ez egy olyan üzenet, amelynek a *MAC* címe egy csupa 1-esekből álló 48 bites cím, a FFFF.FFFF.FFFF

Ezt a címet minden állomás a sajátjaként ismeri fel, tehát ha kap egy ilyen üzenetet, akkor feldolgozza azt. Ha egy eszköz ilyen típusú üzenetet küld, akkor a switchek és hubok a helyi hálózat minden állomására továbbítják azt. Ezért szokás a helyi hálózatot szórási tartománynak is nevezni.

A túl nagy hálózatok túl nagy szórási tartományt – és így túl nagy adatforgalmat – okoznak. Ezért célszerű a hálózatunkat több hálózatra bontani.

ARP (Address Resolution Protocol)

Egy helyi hálózatba kapcsolt állomás akkor fogad egy üzenetet, ha a címzett *MAC* címe megegyezik a sajátjával. Azonban – a korábban említett okok miatt – a hálózati alkalmazások *IP* címet használnak az üzeneteik címzésére. Ha a küldő csak a cél *IP* címét tudja, akkor meg kell határoznia a hozzá tartozó *MAC* címet. Ezt az *ARP* segítségével teheti meg.

Az *ARP (Cím Feloldó Protokoll)* egy IP protokoll három lépésben deríti ki a célgép MAC címét.

1. A küldő elkészít és kiküld a hálózatra egy üzenetet, melynek a MAC címe a szórásos cím. Ez a keret tartalmazza a célgép (már ismert) IP címét.
2. A hálózatban található összes állomás megkapja ezt (mivel a szórásos címet mindenki sajátjaként ismeri fel), viszont csak az küld választ, akinek az IP címe is megegyezik a keretben találhatóval. Ebben a válaszban elküldi a saját MAC címét az ARP üzenetet készítő állomásnak.
3. A küldő gép így már ismeri a célgép *MAC* címét is. Hogy ez megmaradjon, az úgy nevezett ARP táblájába elmenti az *IP-MAC* párost. Innentől kezdve bármikor tud ennek az állomásnak *ARP* kérés nélkül is üzenetet küldeni.

Elosztási réteg

Már többször szó volt róla, hogy a növekvő hálózatunkat érdemes kisebb hozzáférési rétegbeli hálózatokra osztani. Ilyen felosztási szempontok lehetnek pl:

- fizikai elhelyezkedés
- logikai funkció
- biztonsági követelmények
- alkalmazásokra vonatkozó követelmények

Az elosztási réteg feladata, hogy a hozzáférési réteg független hálózatait összekapcsolja egymással. Ez a felelős azért, hogy a helyi hálózatnak szóló forgalom maradjon is helyben, és ebbe az elosztási rétegbe csak más hálózatokba irányuló keretek jussanak. Az ide tartozó eszközöket hálózatok összekötésére tervezték, nem egyéni állomások összekapcsolására (arra valók a switchek, hubok).

Forgalomirányítók (routerek)

A forgalomirányítók olyan hálózati eszközök, melyek a helyi hálózatokat kötnek össze egymással, irányítják a forgalmat, és a hatékony működéshez szükséges feladatokat végeznek. Ha érkezik hozzájuk egy üzenet, akkor fogadják és dekódolják azt. Azonban nem csak a MAC címet tartalmazó keretet értelmezik, hanem belenéznek a csomag többi részébe is. Innen kiolvashatják a küldő és a célgép IP címét. Az IP címből megállapítja a hálózat címét, és a legjobbnak vélt útvonalon továbbítja a csomagot a cél felé.

Minden olyan esetben elkerülhetetlen a routerek használata, amikor a küldő és célgép IP címének hálózati része eltér.

A továbbítás irányát egy táblából határozza meg. Ebben a forgalomirányító táblában szerepel az összes közvetlenül csatlakoztatott hálózat (és az interfész, amin kapcsolódnak), valamint olyan útvonalinformációk, melyeket nem ér el közvetlenül. Csomag fogadásakor, miután megállapította a célgép hálózatát, kikeresi a táblából az útvonalat és elküldi arra a csomagot.

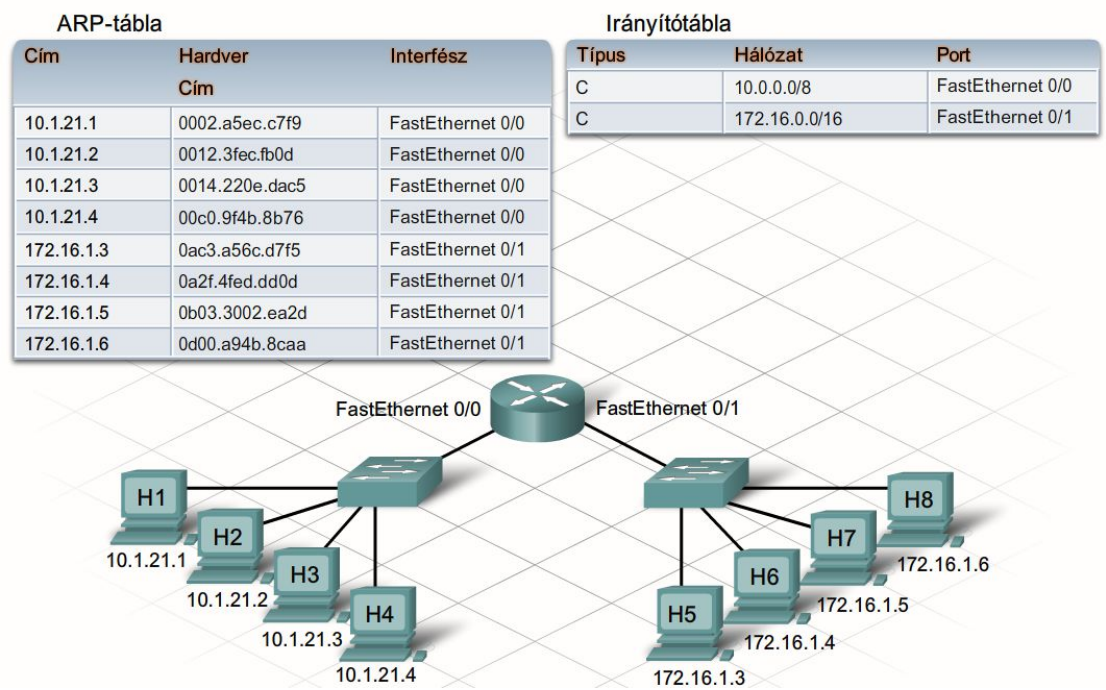
A routerek nem továbbítják a szórásos fizikai címre érkező csomagokat, így biztosítja, hogy a szórásos üzenet nem jut ki a helyi hálózatból.

Routing table

A csomagok továbbítására szükség van ARP és forgalomirányító táblákra is. Az irányítótáblák nem foglalkoznak a hostok egyedi címével, őket csak az érdekli, hogy juttatható el a hálózatukhoz a csomag legegyszerűbben.

Az irányítótábla bejegyzései kétféleképpen jöhetnek létre: vagy dinamikusan frissülnek vagy rendszergazdák írják be őket kézzel (ilyen volt előző alkalommal a static routing).

Ha a router nem tudja meghatározni, hogy merre kell küldeni a csomagot, akkor eldobja azt. Lehetőség van egy alapértelmezett irány megadására, ahova az ismeretlen hálózatra menő csomagokat továbbítja.



4. ábra Példa egy router tábláira

Ha a router kap egy csomagot, akkor azt két féleképpen továbbíthatja

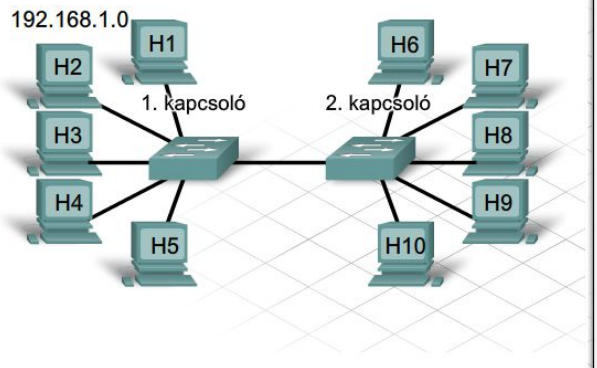
1. ha a célhálózat közvetlenül csatlakozik valamelyik interfészére
2. egy másik routernek kell továbbadni

Küldéskor létre kell hoznia egy üzenetet, melyben szerepelni kell MAC címnek. Ha saját hálózatába kell küldeni, akkor ez a MAC cím a célállomás címe lesz. Ha routernek továbbítja a csomagot, akkor pedig a következő router megfelelő interfészének a MAC címét kell belehelyezni a csomagba.

A router adott interfésze tagja annak a hálózatnak, amelyik csatlakozik hozzá, így mindegyik hálózathoz egy saját ARP táblát tart fenn. Ebben eltárolja a hálózat összes állomásának IP-MAC címét.

Hálózat felosztása – pro és kontra

Egy bizonyos méret felett érdemes meggondolni, hogy jobban járunk-e a hálózatunk felosztásával, vagy helyezzük el inkább az összes állomást egy szegmensben?



Az összes állomás egyetlen helyi hálózati szegmensre helyezése

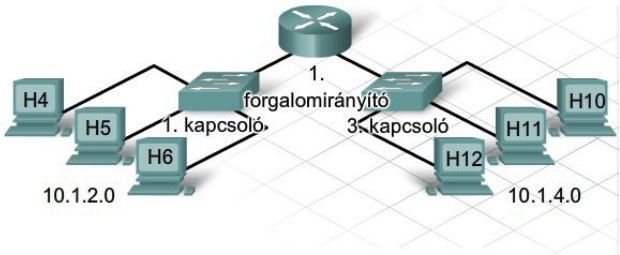
Előnyök:

- Egyszerű hálózatokban megfelelő
- Kisebb bonyolultság és alacsonyabb hálózati költség
- Annak engedélyezése, hogy az állomások "lássák" egymást.
- Gyorsabb adatátvitel - közvetlenebb kommunikáció
- Könyebb eszköz hozzáférés

Hátrányok:

- Minden állomás egyetlen üzenetszórási tartomány része, ami nagyobb forgalmat és kisebb teljesítményt eredményez a szegmensen

5. ábra Érvek-ellenérvek egy hálózat esetén



Az állomások távoli hálózati szegmensre helyezése

Előnyök:

- Alkalmasabb a nagyobb és összetettebb hálózatokban
- Felosztja az üzenetszórási tartományokat és csökkenti a forgalmat
- Minden szegmensen növeli a teljesítményt
- Más, helyi hálózati szegmensen lévő állomások számára az eszközök láthatatlanok lesznek
- Növeli a hálózati biztonságot
- Megkönnyíti a hálózat szervezését

Hátrányok:

- Forgalomirányítás szükséges (elosztási réteg)
- A forgalomirányító lassítja a szegmensek közötti forgalmat
- Bonyolultabb és költségesebb (forgalomirányítót igényel)

6. ábra Érvek-ellenérvek több szegmens esetén

Beugró kérdések (NEM LESZNEK SZÁMONKÉRVE!!!)

1. Miért lett szabványos az Ethernet?
2. Mi a kódszáma az Ethernet szabványért felelős bizottságnak?
3. Mi igaz a MAC címre?
4. Mely eszköz NEM tartozik a hozzáférési rétegbe?
5. Mi a hub hátránya?
6. Mit csinál a switch, ha nem ismeri a címzett MAC címét?
7. Mire szolgál az ARP protokoll?
8. Mire való az elosztási réteg?
9. Mit csinálnak a routerek a szórásos címre érkező csomagokkal?
10. Mi történik akkor, ha a router egy olyan csomagot fogad, amelyiknek nem ismeri a célhálózatát és nincs hozzá tartozó útvonal?

Melléklet

Az Ethernet szabványok

Év	1973	1980	1983
Szabvány	Ethernet	DIX szabvány	IEEE 802.3
Leírás	A Xerox corp.-nál dolgozó Dr Robert Metcalf találta fel az Ethernetet.	A Digital Equipment Corp, az Intel és a Xerox (DIX) kiadta a koaxiális kábelen 10 Mbit/s sebességgel működő Ethernet szabványt.	10 Mbps Ethernet vastag koaxiális kábelen

Év	1985	1990	1993
Szabvány	IEEE 802.3a	IEEE 802.3i	IEEE 802.3j
Leírás	10 Mbps Ethernet vékony koaxiális kábelen	10 Mbps Ethernet csavart érpáron (TP)	10 Mbps Ethernet optikai szálon

Év	1995	1998	1999
Szabvány	IEEE 802.3u	IEEE 802.3z	IEEE 802.3ab
Leírás	Fast Ethernet: 100 Mbps Ethernet csavart érpáron (TP) vagy optikai szálon (különböző szabványok)	Gigabit Ethernet optikai szálon	Gigabit Ethernet csavart érpáron

Év		1999	2002	2006
Szabvány		IEEE 802.3ab	IEEE 802.3ae	IEEE 802.3an
Leírás		Gigabit Ethernet csavart érpáron	10 Gigabit Ethernet optikai szálon (változó szabványok)	10 Gigabit Ethernet csavart érpáron (TP)