

továbbítódik a csomag a lista következő eleméhez, de a router-ek által kijelölt útvonalon.

- *Útvonalrögzítés*. A csomag által érintett állomások IP címe rögzül a csomagban.
- *Időbényeg*
- *Stream ID*. Egy 16 bites azonosító, főként más, folyam (kapcsolat) orientált hálózatokkal való együttműködés segítése miatt.

11.5.1. Datagrammok fragmentálása és összerakása

A fragmentáció akkor következik be, ha haladási útvonalon a következő link-en az *MTU* kisebb, mint a csomagméret. Ekkor a router (vagy maga a feladó) több darabra tördeli a csomagot, mindegyik darabba beleírja, hogy ez az eredeti csomag hányadik byte-jától kezdődő információkat tartalmazza és ad a csomagnak egy egyedi azonosítót. Az azonosító fragmentbe belekerül és jelzi a vevőnek, hogy mely darabok alkotják az eredeti csomagot.

A router a kapott darabokat egyesével feladja és a hálózatra bízza őket. A nagyobb fragmentek esetleg később még tovább darabolódnak egy még kisebb *MTU*-jú link-en. A vevő feladata a csomag összevárasa és összerakása. A feladó egy bit (*DF=Don't Fragment bit*) beállításával kérheti, hogy csomagját ne darabolják, ez esetben ha az *MTU* túl kicsi a csomag továbbításához, a csomagot eldobják és erről *ICMP* üzenetben tájékoztatják a feladót (lásd lejjebb).

Az IP csupán azt követeli meg, hogy az alatta lévő hálózat képes legyen minimum 68 byte-os IP csomagok továbbítására, ez tehát a minimálisan szükséges *MTU*. A TCP/IP implementációk különböznek egymástól a *datagramm* méretének megválasztásában, azonban a szabvány szerint legalább 576 oktet nagyságú *datagrammokat* választanak, ha nem biztosak abban, hogy a nagyobb méretet útközben mindenhol megértik. Ez az elégé konzervatív megközelítés abból fakad, hogy az összerakást megvalósító kódok sokszor hibásak. A tervezők kerülni igyekeznek a fragmentálást. Mindegyikük másként gondolkodik arról, hogy mikor biztonságos a nagyobb méret. Néhányan csak a lokális hálózatra esküsznek, de vannak olyanok is, akik az egész hálózatra kiengednek ilyen *datagrammokat*. Az 576 oktet elégé biztonságos ahhoz, hogy mindenki támogassa.

11.5.2. Az IP címzési rendszere

Az IP 32 bites címeket használ, a címeket byte-onkét, egymástól ponttal („.”) elválasztva, tízes számrendszerben írjuk. (Például 152.66.208.40)

Minden cím egy hálózati és egy állomásszámból áll. A hálózat száma azonosítja azt a hálózatot, melyen a cél található, az állomásszám pedig azon belül magát az állomást. Kezdetben a hálózat száma 7 bites, az állomás száma pedig 24 bites volt, minthogy kevés, de népes hálózatokra számítottak. Később ezt a címformátumot A osztályú címnek nevezve még két címosztályt vezettek be, a B és C osztályt. Ezekben nagyobb hely volt a hálózat száma részére (14 és 22 bit) és kisebb az állomás számára (16 és 8 bit), több, de kisebb hálózat számára címteret biztosítva. Sajnálatos módon a legtöbb jelenlegi hálózat számára a B osztály sok, a C osztály kevés állomás bekapcsolását teszi lehetővé, ami miatt a B osztály kimerülni látszik. Ezzel a problémával később még foglalkozni fogunk.

11.4. ábra. Az IP címkiosztása

Az Internet *Multicast* számára van fenntartva a D osztály, az ebben levő 28 hasznos bit strukturálatlan és egy cím egy multicast csoportot jelöl. Az E osztályú címek későbbi felhasználásra vannak fenntartva.

Az IP címtartományok osztályok szerint csoportosítva:

Class A ==> 1.0.0.0 - 126.0.0.0

7-bites *NET_ID* és 24-bites *HOST_ID*. Az A osztályú címek nagy méretű hálózatok számára vannak fenntartva, és hálózatonként $16777216 (2^{24})$ hostot tudnak megcímezni.

Class B ==> 128.xxx.0.0 - 191.xxx.0.0

14-bit *NET_ID*, 16-bit *HOST_ID*, ez 65536 megcímzhető hostot jelent.

Class C ==> 192.xxx.yyy.0 - 223.xxx.yyy.0

21-bit *NET_ID*, 8 bit *HOST_ID*, hálózatonként 254 címet jelent.

Class D ==> 224.xxx.yyy.zzz - 239.xxx.yyy.zzz (multicast IP)

Az IP címekben a 0 és a 255 speciális jelentéssel bír. A 0 az olyan gépek számára van fenntartva, amelyek nem tudják a hálózati címüket. Bizonyos helyzetekben lehetséges, hogy egy számítógép nem tudja, melyik hálózatra csatlakoztatták. A 0.0.0.23 például egy olyan számítógép címe, amelynek *hosts*áma 23, de nem tudni, hogy melyik hálózaton.

A 255-t üzenetszórásra (*broadcast*) használják. Az üzenetszórás lényegében egy olyan üzenet, amelyet az adott hálózaton minden számítógép lát. Olyankor használatos, amikor a "címzett ismeretlen". Tegyük fel például, hogy egy, a hálózatra kapcsolt számítógép nevére van szükségünk, mert az Internet címét szeretnénk tudni. Mondjuk, hogy a legközelebbi névszolgáltatónak nem tudjuk a címét. Ilyenkor segít az üzenetszórás. Előfordulhat az is, hogy egy információt több rendszerrel meg szeretnénk osztani. Ilyenkor hatásosabb az üzenetszórás, mintha az érdekelt rendszerekhez külön küldenénk *datagrammokat*.

Az üzenetszórás megvalósításához egy olyan IP címet kell formálni, amelyben a hálózatot jelölő részbe a küldő hálózat címét, a gépet jelölő részbe pedig csupa egyes bitet (azaz 255-t) írunk. A 193.6.4 hálózaton ez így nézne ki: 193.6.4.255. Az üzenetszórás tényleges megvalósítása az adott közegtől függ. Az Arpanet-en és két gép közötti hálózatokon nem lehet üzenetszórást alkalmazni, ellentétben az Ethernet alapú hálózatokkal, ahol a csupa egyes bitból álló Ethernet című üzenetet az azon a hálózaton lévő minden számítógép veszi. A

255.255.255.255 gyakorlatilag az egész Internet megcímzésére szolgál, de ilyen IP csomagokat a *routerek* nem engednek át.

Az állomások számára fenntartott mezőt gyakran két részre osztják, egyik rész az alhálózat (subnet) azonosítja, másik pedig azon belül magát az állomást.

A 127-tel kezdődő címek a visszairányítás(loopback) címei, a hálózat belső tesztelésére használhatók csak. A 10-zel és 192-vel kezdődő IP címek minden az aktuális alhálózatra mutatnak, és a hálózat irányító eszközök az ezekre a címekre érkezett csomagokat minden a belsőhálózat felé küldik.

11.5.3. Az alhálózatok címzése (*Subnet masking*)

Mivel egy B típusú osztály esetén 65534 cím kiosztását jelenti egy hálózatban, ez nehezen kezelhető hálózat kialakulásához vezetne. Emiatt a hálózatokat alhálózatokra (subnet) bontják. Azt, hogy az állomás számára rendelkezésre álló biteket (B osztály esetén 16) hogyan osztják fel a hálózat és a tényleges állomás azonosítója között, a rendszer szempontjából teljesen mindegy, minden össze egy alhálózati mask (subnet mask, netmask) megadása szükséges, amely azonosítja az alhálózatot.

1. PÉLDA:

Egy adott gép címe alapján, hálózatának címét keressük. A gép a balu.sch.bme.hu (152.66.208.40, B osztályú cím) és a hozzá tartozó netmask 255.255.248.0 A két IP cím bitenkénti ÉS kapcsolatát elvégezve kapjuk a hálózat címét:

10011000 01000010 11010000 00101000 –gép címe 152.66.208.40
11111111 11111111 11111000 00000000 –netmask 255.255.248.0
----- AND művelet
10011000 01000010 11010000 00000000 -hálózat címe 152.66.208.0

Tehát a hálózatának címe: (152.66.208.0). Ez az alhálózatban összesen $6 \times 254 = 2032$ hostból állhat.

(Megjegyzés):

Az IP címosztályok is meghatároznak egy alapértelmezett netmaskot:

Class A - 255.0.0.0

Class B - 255.255.0.0

Class C - 255.255.255.0

Újabban létezhetnek változó hosszúságú alhálózatok is, tehát egy hálózatban lehet olyan alhálózat, melynek azonosítására az állomásszám felső 8 bitjét használjuk, és lehetnek olyanok, ahol a felső 12 bitet. Természetesen az alhálózatok számait úgy kell kiosztani, hogy a felső 8 bitból el lehessen dönteneni, hogy ez most egy 8 vagy 12 bites alhálózati szám. Ez akkor lehet hasznos, ha sok eltérő méretű alhálózatunk van és fix beosztás esetén nem elegendő a címtér. A módszer viszont egy fokkal bonyolultabb routing protokollt és adminisztrációt igényel.

Egy alhálózaton levő állomások szomszédosnak számítanak, tehát router közbeiktatása nélkül tudnak kommunikálni, egy közös link-en vannak. Lehetséges azonban, hogy egy link-

en több *alhálózat* is legyen, azonban egy alhálózat nem tartalmazhat több link-et, hiszen azok között az átjárás csak router-en át lehetséges. Ha egy link-en több *alhálózat* van, akkor a különböző alhálózaton lévő állomások, bár közvetlenül is kommunikálhatnának, mégis *router-t* vesznek igénybe.

11.5.4. Az IP útvonal-keresési rendszere (*IP routing*)

Egy IP csomag rendeltetési helyére juttatásának mikéntjét az útvonal-választás (routing) kifejezés jelöli. A részletek nagymértékben függenek az adott implementációtól, viszont egy-két dolgot általanosságban el lehet mondani.

Az IP alapállapotban azzal a feltevéssel él, hogy a rendszerek valamelyen lokális hálózatra kapcsolódnak. Feltessük, hogy a rendszer a saját hálózatán keresztül csomagokat tud küldeni egy másik rendszernek. (Ethernet alapú hálózat esetén egyszerűen a célállomás Ethernet címét kell megkeresnie, majd a csomagot ki kell adnia a hálózatra.)

A probléma akkor jelentkezik, amikor egy másik hálózaton lévő rendszerhez kell küldeni a csomagot. Itt lépnek be az átjárók (gateway). Az átjáró egy olyan hálózati eszköz, amely egy hálózatot két vagy több másikkal köt össze. Ez a gyakorlatban legtöbbször egy olyan számítógépet jelent, amelynek több hálózati interfésze van. Ez a számítógép a két hálózat között átjáróként üzemelhet. A hálózati szoftvert úgy kell beállítani, hogy az átjáró a két hálózat között dcsomagokat tudjon küldeni. Ha egy gép egy hálózatról olyan csomagot küld az átjáró felé, amely egy másik hálózaton lévő gépek egyikének szól, akkor azt az átjáró továbbítja a célállomás felé.

A főbb kommunikációs központokban több átjáró is található, amelyek különböző hálózatokat kötnek össze egymással. (A legtöbbször speciálisan erre a feladatra készített átjárókat alkalmazznak, amelyek megbízhatóbban, és sokkal hatásosabban működnek az általános célú átjáróknál. Sok cég kínál ilyen rendszereket.)

Az IP szerinti útvonal-választás teljes mértékben a célállomás hálózati számán alapszik. A hálózatba kötött minden egyes számítógép rendelkezik egy táblázattal, amelyben a hálózati számokat tárolják. minden hálózatszámhoz tartozik egy átjáró, amelyen keresztül az adott hálózathoz eljuthatunk. Azt észre kell venni, hogy az átjáró nincs feltétlenül arra a hálózatra kötve: egyszerűen csak az a legjobb út, amelyen keresztül az adott hálózathoz el lehet jutni.

Amikor egy számítógép csoamgot akar küldeni egy másiknak, akkor először azt ellenőrzi, hogy a fogadó nincs-e a saját hálózatán. Ha ott van, akkor a csomagot közvetlenül neki küldi el. Ha nincs ott, akkor a rendszer keresni kezdi a táblázatban a célállomás hálózati számát, és a csoamagot annak a hálózatnak az átjárója felé küldi. A hálózati számokat és átjárókat felsoroló táblázat esetenként igen nagy terjedelelmeire tehet szert.

Az Internet például több száz hálózatot foglal magába. Különböző stratégiákat dolgoztak ki annak érdekében, hogy az útvonal-választási táblák méretét a lehető legkisebb értéken tartsák. Az egyik ilyen módszer az alapértelmezett útvonalak használata. Gyakran fellép az az eset, hogy egy hálózatból csak egyetlen átjárón keresztül lehet kijutni.

Egy ilyen átjáró például egy Ethernet alapú lokális hálózat és egy gerinchálózat között létesíthet kapcsolatot. Ilyenkor persze nincs szükség arra, hogy az útvonal-választási táblában

az összes külső hálózat szerepeljen. Az átjárót egyszerűen alapértelmezettnek definiáljuk, és így a választott útvonallal nem rendelkező csomagok egyenesen az átjáróhoz kerülnek.

Egy így beállított átjáró akkor is használható, ha egy hálózaton több is működik belőle. Az átjárókat úgy terveztek, hogy a "Nem ez a legjobb átjáró -- használ inkább ezt és ezt." üzenetet generálni tudják. A hálózati szoftverek többsége ezt az üzenetet használja arra, hogy az útvonal-választási táblájába bejegyzéseket helyezzen el. Az IP szakértők többsége azon a véleményen van, hogy a hálózati számítógépek ne próbálják meg az egész hálózat forgalmát nyomon követni. Ehelyett azt ajánlják, hogy alapértelmezett átjárókat használjanak, és rájuk támaszkodjanak az útvonalak megállapításánál, ahogy azt a fentiekben is leírtuk. Arról nem volt szó, hogy az átjárók hogyan határozzák meg az útvonalakat.

Az esetükben a fenti stratégia nem használható, hiszen az útvonal-választási táblázatunknak megfelelően teljesnek kell lennie. Ezért valamiféle útvonal-választási protokoll jelenléte szükséges, amely azt írja le, hogy az átjárók hogyan találhatják meg egymást, és hogyan frissíthetik az adatbázisukat a különböző hálózatokhoz vezető (legjobb) útvonalról.

11.5.5. Példák útvonalválasztásra

1. Vegyük ki a célgép IP címét a *csoamgból*, nevezzük ezt: *ipdest*-nek
2. indulunk az útvonal kiválasztási tábla elejéről (majd folytassuk a többi bejegyzéssel):
Számítsuk ki a hálózati címrészt az *ipdest*-ből:

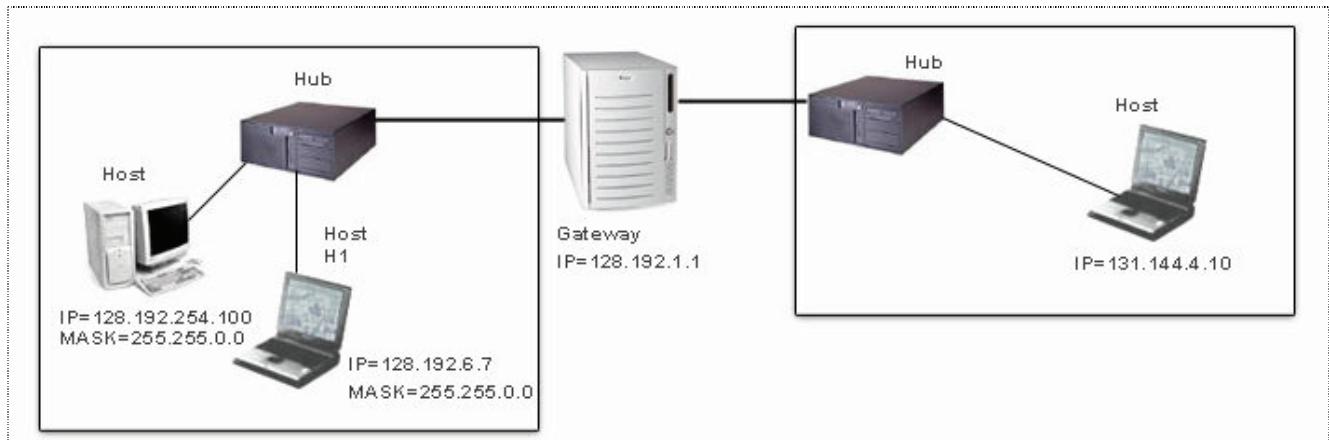
ipnet = AND (*netmask*, *ipdest*)

Ha az *ipnet* azonos a hálózati címmel (network address), küldjük a *csoamgot* a következő router-re (*next-hop*)

Ha nem azonosak, akkor ismételjük meg az első két lépést.

Ha a táblázat egyetlen bejegyzésével sem egyezik meg, akkor adjunk hibaüzenetet

11.5. ábra. Hálózat host útkereséséhez:



Útkeresési tábla a H1-es host-hoz:

entry	netmask	net-address	next-hop	hop-count	comments
1	255.255.0.0	128.192.0.0	128.192.6.7	0	DCN
2	0.0.0.0	0.0.0.0	128.192.1.1	1	DR

11.5.6. Példák.

1.Példa:

A csomag ipdest=128.192.254.100

A hálózat címrész kiszámítása az ipdest-ből és a táblázat első sorában szereplő netmask-ból.

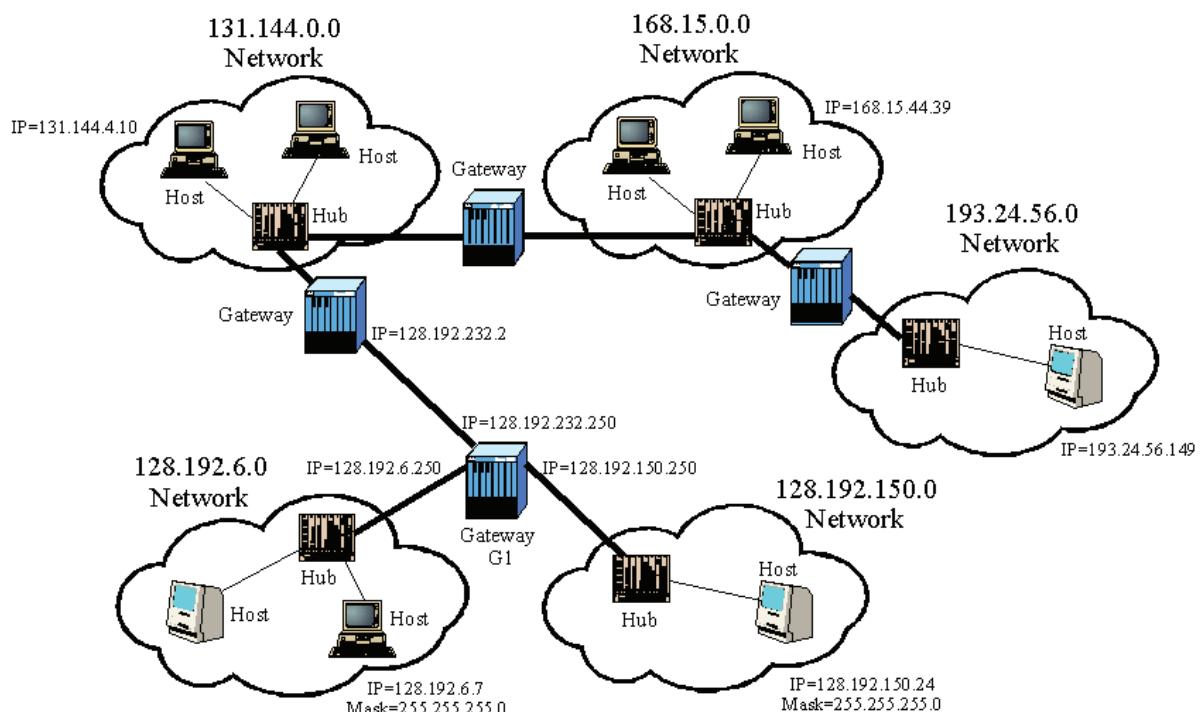
```
...ipdest = 10000000 11000000 11111110 01100100 (128.192.254.100)
netmask = 11111111 11111111 00000000 00000000 (255.255.0.0)
AND művelet -----
ipnet = 10000000 11000000 00000000 00000000 (128.192.0.0)
```

Az ipnet és a net-address összehasonlítása

128.192.0.0 és 128.192.0.0 **azonosak**

Mivel azonosak, tovább küldjük a következő router-re: next-hop=128.192.6.7

Hálózat átjáró útkeresése



A G1-es átjáró útkeresési táblája:

entry	netmask	net-address	next-hop	hop-count	comments
1	255.255.255.0	128.192.6.0	128.192.6.250	0	DCN
2	255.255.255.0	128.192.7.0	128.192.7.250	0	DCN
3	255.255.255.0	128.192.150.0	128.192.150.250	0	DCN

4	255.255.255.0	128.192.232.0	128.192.232.250	0	DCN
5	255.255.255.255	131.144.4.10	128.192.232.2	1	HSR
6	255.255.0.0	168.15.0.0	128.192.232.2	2	NSR
7	0.0.0.0	0.0.0.0	128.192.232.2	1	DR

2. példa:

A csomag ipdest=128.192.150.24 Olyan bejegyzést keresünk a táblában, amely netmask-jából és az ipdest-ből generált címrész azonos a sor net-address bejegyzésével, majd elküldjük a csoamgot a megfelelő címre (next-hop):

bejegyzés	netmask	AND(128.192.150.24)	net-address	eredmény
1	255.255.255.0	128.192.150.0	128.192.6.0	nem azonos
2	255.255.255.0	128.192.150.0	128.192.7.0	nem azonos
3	255.255.255.0	128.192.150.0	128.192.150.0	direkt küldés

3. példa:

1. A csomag ipdest=168.15.44.39

2. Olyan bejegyzést keresünk a táblában, amely netmask-jából és az ipdest-ből generált címrész azonos a sor net-address bejegyzésével, majd elküldjük a csomagot a megfelelő címre (next-hop):

bejegyzés	netmask	AND(168.15.44.39)	net-address	eredmény
1	255.255.255.0	168.15.44.0	128.192.6.0	nem azonos
2	255.255.255.0	168.15.44.0	128.192.7.0	nem azonos
3	255.255.255.0	168.15.44.0	128.192.150.0	nem azonos
4	255.255.255.0	168.15.44.0	128.192.232.0	nem azonos
5	255.255.255.255	168.15.44.39	131.144.4.10	nem azonos
6	255.255.0.0	168.15.0.0	168.15.0.0	küldés:128.192.232.2

4. példa:

A csomag ipdest=193.24.56.149 Olyan bejegyzést keresünk a táblában, amely netmask-jából és az ipdest-ből generált címrész azonos a sor net-address bejegyzésével, majd elküldjük a csomagot a megfelelő címre (next-hop):

bejegyzés	netmask	AND(193.24.56.149)	net-address	eredmény
1	255.255.255.0	193.24.56.0	128.192.6.0	nem azonos
2	255.255.255.0	193.24.56.0	128.192.7.0	nem azonos
3	255.255.255.0	193.24.56.0	128.192.150.0	nem azonos
4	255.255.255.0	193.24.56.0	128.192.232.0	nem azonos
5	255.255.255.255	193.24.56.149	131.144.4.10	nem azonos
6	255.255.0.0	193.24.0.0	168.15.0.0	nem azonos
7	0.0.0.0	0.0.0.0	0.0.0.0	küld:128.192.232.2

11.5.7. Network Address Translation

A fentebb már említett 192-vel vagy 10-zel kezdődő IP címek egy olyan közös címkészlet részei, amit több host tud egyidejűleg használni a *NAT* segítségével. Ez a funkció már előre be van építve a proxy szolgáltatókba, routerekbe, vagy számítógépek operációs