22. fejezet – Az IPv4 protokoll 2, CIDR és Vezérlő és útválasztó protokollok

Az IP címek – ellentétben a MAC címekkel – hierarchikusak, azaz magunk határozhatjuk meg (természetesen bizonyos korlátok között), így lehetőségünk van lokalizációs illetve priorizálási szempontok figyelembe vételére is. Az IP cím egyszerre utal egy hálózatra és azon belül egy hosztra. Pontosabban az IP cím nem egy hosztot azonosít, hanem egy hosztnak egy adott hálózati kártyáját (NIC – Network Interface Card), más megfogalmazásban egy interfészét. Különösen szerver gépek esetében jellemző a több hálózati kártya használata. Tehát célszerű a címet két részre bontani, hálózati azonosítóra és a hosztot (pontosabban a hoszt hálózati kártyáját) azonosító címre. A rendelkezésünkre álló 32 bites címet, azaz 4*8bites címet több különböző módon használhatjuk fel.

Osztály	8 bit	8 bit	8 bit	8 bit
"A"	0 Hálózat (7)	Hoszt (24)		
"B"	1 0 Hálózat (14)	Hoszt (16)		
"C"	1 1 0 Hálózat (21)	Hoszt (8)		
"D"	1 1 1 0 Többszörös cím (Többesküldés) / Multicast (28)			
"E"	1 1 1 1 Jövőbeli használatra fenntartott / Reserved (28)			

Osztály	Hálózat		Hoszt (NIC) hálózatonként	
"A"	1-127	2^7-2 = 126 db	0.0.1 - 255.255.255	2^{24}-2 = 16777214 db
"B"	128.0 - 191.255	2^{14} = 16384 db	0.1 - 255.255	2^{16}-2 = 65534 db
"C"	192.0.0 - 223.255.255	2^{21} = 2097152 db	1 - 255	2^8-2 = 254 db
"D"	224.0.0.0 - 239.255.255.255			
"E"	240.0.0.0 - 255.255.255.255			

Osztály	Teljes címformátum	Adatszórás (Broadcast)	Decimális / Bináris
"A"	001.000.000.000 - 127.255.255.255	xxx.255.255.255	127_{10} = 0111 1111_2
"B"	128.000.000.000 - 191.255.255.255	xxx.xxx.255.255	128_{10} = 1000 0000_2
"C"	192.000.000.000 - 223.255.255.255	xxx.xxx.xxx.255	192_{10} = 1100 0000_2
"D"	224.000.000.000 - 239.255.255.255	-	224_{10} = 1110 0000_2
"E"	240.000.000.000 - 255.255.255.255	-	240_{10} = 1111 0000_2

Speciális esetek:

- A 0.0.0.0 cím nincs használatban, ugyanis az összes hoszt a bekapcsolás (indulás) pillanatában ezt használja.
- A 255.255.255.255 az adatszóró (Broadcast) címek speciális esete, mely lehetővé teszi az adatszórást a helyi hálózaton, jellemzően egy LAN hálózaton belül.
- Az adott hálózaton kioszthatő hosztok darabszáma esetén mindig figyelembe kell venni, a fentiek szerint 2db cím (a 000 és a 255) kiesését.
- A 127.xxx.xxx.xxx címek visszacsatolásos (Loopback) tesztelésre vannak fenntartva.

A fentiekből látszik, hogy a leggondosabb és leglogikusabb tervezéssel és előrelátással sem sikerült a mai értelembe életszerű osztályozást kialakítani, anno 1981-ben. A probléma az, hogy a legtöbb céges felhasználó szempontjából az „A” osztály lehetséges hosztjainak száma túl nagy (sok esetben a „B” osztályú hálózatok is csak részben kihasználtak), a „C” osztály lehetséges hosztjainak száma pedig túl kevés. Ma már az látszik, hogy szerencsésebb lett volna a „C” osztályú hosztok esetében 8 helyett 10 bitet alkalmazni, így 254 helyett 1022 lenne csatlakoztatható hosztok száma.

Az „A”, a „B” és a „C” osztály esetében is kijelölésre került privát (Private) tartomány, melyben szereplő privát címek, közvetlenül az Internetről nem érhetők el. Az Internet elérése a hosztokról (azaz a fordított irány) azonban megfelelő útválasztással és átjáró használattal megoldott. A privát tartományok tehát megtöbbszörözik az Internetre kapcsolható hosztok számát, és jellemzően abban az esetben használatosak, amikor egy adott felhasználó hosztjait nem kell az Internet felől elérni.

Osztály	Privát IP tartomány	Hálózatok és Hosztok (NIC) száma
"A"	10.0.0.0 - 10.255.255.255	1db hálózat, 16777214 db hoszt (NIC)
"B"	172.16.0.0 - 172.31.255.255	16 db hálózat, hálózatonként 65534 db hoszt (NIC)
"C"	192.168.0.0 - 192.168.255.255	256 db hálózat, hálózatonként 254 db hoszt (NIC)

Hálózati maszk (Netmask), alhálózati maszk (Subnet Mask) és a CIDR

Az IP címekhez hasonlóan a hálózati maszk is 32 bites. A hálózati maszk segítségével korlátozhatjuk a hálózatunkon használható IP címek számát. Maga a hálózati maszk bináris formában mindig 1-esekből álló sorozattal kezdődik, és 0-ákból álló sorozattal végződik, tehát a hálózati maszkban 0 értéket semmiképpen sem követhet 1-es érték. Az IP cím és a hálózati maszk közti ÉS (AND) művelet a hálózat címét adja vissza, az IP cím és a hálózati maszk NEGÁLTja (Wildcard) közti ÉS művelet pedig a hoszt címét a hálózaton belül. A hálózati maszk segítségével a teljes cím szétválasztható a hálózat címére, illetve a hoszt címére. A hálózati maszk segítségével a statikus osztályba sorolás, azaz a hálózat/hoszt határ dinamikusan módosítható.
A hálózati maszk az IP címhez hasonlóan négy, pontokkal elválasztott decimális számmal (0-255) írható le, de szokásos jelölése még az, amikor csak a benne lévő 1-esek darabszámára, vagyis az előtag (Prefix) hosszára hivatkozunk, az IP cím végén, egy perjel „/” után írva.

Osztály	Alapértelmezett hálózati maszk	Bináris ábrázolás	1-esek száma
"A"	255.0.0.0	11111111.00000000.00000000.00000000	/8
"B"	255.255.0.0	11111111.11111111.00000000.00000000	/16
"C"	255.255.255.0	11111111.11111111.11111111.00000000	/24

Az alhálózati maszk a hálózati maszk által meghatározott IP címtéren belül független alhálózatok, blokkok létrehozását teszi lehetővé. A blokk kezdőcíme a hálózat címe, utolsó címe pedig az adatszóró (Broadcast) cím – ezt a két címet a hosztok nem használhatják. Ez a változó blokkméretű elosztás, az osztály nélküli (más megközelítésben: tartományon belüli) forgalomirányítás (CIDR – Classless Inter-Domain Routing), mely 1993. óta van használatban.

Alhálózati maszk	Bináris ábrázolás	Prefix	Hosztok max. száma
255.255.255.255	11111111.11111111.11111111.11111111	/32	0 db
255.255.255.254	11111111.11111111.11111111.11111110	/31	1 db
255.255.255.252	11111111.11111111.11111111.11111100	/30	2 db
255.255.255.248	11111111.11111111.11111111.11111000	/29	6 db
255.255.255.240	11111111.11111111.11111111.11110000	/28	14 db
255.255.255.224	11111111.11111111.11111111.11100000	/27	30 db
255.255.255.192	11111111.11111111.11111111.11000000	/26	62 db
255.255.255.128	11111111.11111111.11111111.10000000	/25	126 db
255.255.255.0	11111111.11111111.11111111.00000000	/24	254 db
255.255.254.0	11111111.11111111.11111110.00000000	/23	510 db
255.255.252.0	11111111.11111111.11111100.00000000	/22	1 022 db
255.255.248.0	11111111.11111111.11111000.00000000	/21	2 046 db
255.255.240.0	11111111.11111111.11110000.00000000	/20	4 094 db
255.255.224.0	11111111.11111111.11100000.00000000	/19	8 190 db
255.255.192.0	11111111.11111111.11000000.00000000	/18	16 382 db
255.255.128.0	11111111.11111111.10000000.00000000	/17	32 766 db
255.255.0.0	11111111.11111111.00000000.00000000	/16	65 534 db
255.254.0.0	11111111.11111110.00000000.00000000	/15	131 070 db
255.252.0.0	11111111.11111100.00000000.00000000	/14	262 142 db
255.248.0.0	11111111.11111000.00000000.00000000	/13	524 286 db
255.240.0.0	11111111.11110000.00000000.00000000	/12	1 048 574 db
255.224.0.0	11111111.11100000.00000000.00000000	/11	2 097 150 db
255.192.0.0	11111111.11000000.00000000.00000000	/10	4 194 302 db
255.128.0.0	11111111.10000000.00000000.00000000	/9	8 388 606 db
255.0.0.0	11111111.00000000.00000000.00000000	/8	16 777 214 db
254.0.0.0	11111110.00000000.00000000.00000000	/7	33 554 430 db
252.0.0.0	11111100.00000000.00000000.00000000	/6	67 108 862 db
248.0.0.0	11111000.00000000.00000000.00000000	/5	134 217 726 db
240.0.0.0	11110000.00000000.00000000.00000000	/4	268 435 454 db
224.0.0.0	11100000.00000000.00000000.00000000	/3	536 870 910 db
192.0.0.0	11000000.00000000.00000000.00000000	/2	1 073 741 822 db
128.0.0.0	10000000.00000000.00000000.00000000	/1	2 147 483 646 db

A CIDR leírását az RFC1700 dokumentum tartalmazza. A már korábban az osztályba sorolásra használt /8, /16 és /24 mellett bevezetett többi előtag hossz megjelenése nagyban hozzájárult az IPv4 címek elfogyásának időbeli késleltetéséhez, hiszen hatékonyabb címkiosztást tett lehetővé, akár különböző méretű hálózatok esetében is folyamatosan tölthető fel, osztható ki a címtér. Az egyetlen ökölszabály az, hogy a hálózatok mérete kettő valamelyik hatványa (2^x) legyen, illetve az, hogy a hálózatok, a méretet meghatározó kettő hatványának a többszöröseire, mint határokra legyenek illesztve. Ettől kezdve az IP cím felépítése már „előtag + hoszt cím" modellként értelmezendő.
Semmiképpen sem szabad arról megfeledkezni, hogy az IP-protokoll számára az IP-cím és az alhálózati maszk csak együtt értelmes, mert az IP-cím mindig két részből áll. Az alhálózati maszk hiányában a hoszt nem tudja meghatározni az őt tartalmazó hálózat címét, ami pedig az útválasztáshoz elengedhetetlen.

A hálózat, és az alhálózat közötti különbség fizikai és logikai megközelítésben érthető meg. Azaz hálózatról fizikailag összekötött hosztok esetében beszélünk, az alhálózat pedig a hálózatban összekötött hosztok logikai (azaz pl. alhálózati maszkkal történő) blokkokra történő szétválasztása. A blokkok közötti átjárhatóság közvetlenül nem biztosított.

A hierarchikus címzésnek – a hálózati és a hoszt cím szétválasztásának – előnye, hogy az útválasztók a számukra érdektelen hoszt címeket nem kell, hogy táblázataikban tárolják. Egy hálózaton belül az összes hoszt hálózati címe azonos, az útválasztáshoz, azaz a célhálózat megtalálásához, elég csak ezt tárolni. A nem kellő körültekintéssel történő hálózatkiosztás viszont pazarló lehet, azaz ha túl nagy alhálózatot jelölünk ki, és így sok kihasználatlan IP cím kerülhet lefoglalásra.

Gyakorlati példák:

1. Legyen egy belső használatú IP cím: 192.168.100.1, és legyen a hozzá tartozó hálózati maszk: 255.255.255.0. Az IP címet jelölhetjük így is: 192.168.100.1/24.

Bináris formában az IP cím:	11000000 10101000 01100100 00000001
A hálózati maszk:	11111111 11111111 11111111 00000000
Ezekből ÉS kapcsolattal a hálózat címe:	11000000 10101000 01100100 00000000

   A hosztok számára marad az utolsó 8 bit, így elvileg 2^8 = 256 db IP cím osztható ki. Magában a 192.168.100.0/24 jelölésű hálózatban elvileg 256 hosztot jelölhetnénk ki, de mivel a 0 a hálózatot, a 255 (ami binárisan csupa 1-esből áll) pedig a Broadcast-ot jelöli, 256-2 = 254 kioszthatő hoszt (NIC) IP címünk áll gyakorlatilag rendelkezésre.

A hálózati maszk megváltoztatásával szűkíthetjük a hálózaton belül kiosztható IP címek számát, a létrehozható alhálózatok számát pedig bővíthetjük. Ha a hálózati maszkot a következő – a definíció szerint alhálózati maszkra – 255.255.255.248-ra cseréljük, a következő történik.

A hosztok számára marad az utolsó 3 bit, így elvileg $2^3 = 8$ db IP cím osztható ki. Magában a 192.168.100.0/29 jelölésű alhálózatban elvileg 8 hosztot jelölhetnénk ki, de mivel a 0 a hálózatot, a 7 (ami binárisan csupa 1-esből áll) pedig a Broadcast-ot jelöli, 8-2 = 6 kioszthatő hoszt (NIC) címünk áll gyakorlatilag rendelkezésre.

Az alhálózat IP címe:	192.168.100.0/29	11000000 10101000 01100100 00000000
Az alhálózati maszk:	255.255.255.248	11111111 11111111 11111111 11111000
A legkisebb IP cím:	192.168.100.1	11000000 10101000 01100100 00000**001**
A legnagyobb IP cím:	192.168.100.6	11000000 10101000 01100100 00000**110**
A Broadcast IP cím:	192.168.100.7	11000000 10101000 01100100 00000111

Viszont lehetőségünk van a következő szabad IP címtől újabb alhálózatot definiálni, azaz például a 192.168.100.8/29 jelölésű alhálózatot. Ez esetben az alhálózat címe a 192.168.100.8, a 6 db kioszthatő cím pedig a 9-10-11-12-13-14. A 192.168.100.15 (amiben a 15 binárisan csupa 1-esből áll) pedig a Broadcast-ot jelöli.

Az alhálózat IP címe:	192.168.100.8/29	11000000 10101000 01100100 00001000
Az alhálózati maszk:	255.255.255.248	11111111 11111111 11111111 11111000
A legkisebb IP cím:	192.168.100.9	11000000 10101000 01100100 00001**001**
A legnagyobb IP cím:	192.168.100.14	11000000 10101000 01100100 00001**110**
A Broadcast IP cím:	192.168.100.15	11000000 10101000 01100100 00001111

Mivel egy „C” osztályú hálózat blokkokra osztásáról van szó, ezzel a módszerrel, ez esetben összesen $2^5 = 32$ db alhálózatot definiálhatunk, egyenként $2^3 - 2 = 6$ db kioszthatő IP címmel. Az IP cím utolsó 8 bitjéből az első 5 bit az alhálózat sorszámát, az utolsó 3 bit pedig a alhálózaton belüli IP címet jelöli. A 32. alhálózat adatai:

Az alhálózat IP címe:	192.168.100.248/29	11000000 10101000 01100100 11111000
Az alhálózati maszk:	255.255.255.248	11111111 11111111 11111111 11111000
A legkisebb IP cím:	192.168.100.249	11000000 10101000 01100100 11111**001**
A legnagyobb IP cím:	192.168.100.254	11000000 10101000 01100100 11111**110**
A Broadcast IP cím:	192.168.100.255	11000000 10101000 01100100 11111111

Hasznos segítség a hálózatok tervezéséhez egy IP kalkulátor, ami hasonló hálózatok definiálásában segít: http://jodies.de/ipcalc

2. Egy nemzetközi vállalat rendelkezik 8192 db IP címmel, amit 4 különböző telephelyén (A, B, C, D) szeretne használatba venni. Az IP címek a 212.32.0.0 címtől kezdődően állnak rendelkezésre.

Telephely	Első elvi cím	Utolsó elvi cím	Igényelt hoszt	Optimális hoszt	Hálózat címe
A	212.32.0.0	212.32.7.255	2 000 db	2 048 db	212.32.0.0/21
B	212.32.8.0	212.32.11.255	1 000 db	1 024 db	212.32.8.0/22
C	212.32.12.0	212.32.15.255	1 000 db	1 024 db	212.32.12.0/22
D	212.32.16.0	212.32.31.255	4 000 db	4 096 db	212.32.16.0/20

„A” hálózat IP címe:	212.32.0.0/21	11010100 00100000 00000000 00000000
„A” alhálózati maszk:	255.255.248.0	11111111 11111111 11111000 00000000
„A” legkisebb IP címe:	212.32.0.1	11010100 00100000 00000**000 00000001**
„A” legnagyobb IP címe:	212.32.7.254	11010100 00100000 00000**111 11111110**
„A” Broadcast IP címe:	212.32.7.255	11010100 00100000 00000111 11111111
„B” hálózat IP címe:	212.32.8.0/22	11010100 00100000 00001000 00000000
„B” alhálózati maszk:	255.255.252.0	11111111 11111111 11111100 00000000
„B” legkisebb IP címe:	212.32.8.1	11010100 00100000 00001**000 00000001**
„B” legnagyobb IP címe:	212.32.11.254	11010100 00100000 00001**011 11111110**
„B” Broadcast IP címe:	212.32.11.255	11010100 00100000 00001011 11111111
„C” hálózat IP címe:	212.32.12.0/22	11010100 00100000 00001100 00000000
„C” alhálózati maszk:	255.255.252.0	11111111 11111111 11111100 00000000
„C” legkisebb IP címe:	212.32.12.1	11010100 00100000 00001**100 00000001**
„C” legnagyobb IP címe:	212.32.15.254	11010100 00100000 00001**111 11111110**
„C” Broadcast IP címe:	212.32.15.255	11010100 00100000 00001111 11111111
„D” hálózat IP címe:	212.32.16.0/20	11010100 00100000 00010000 00000000
„D” alhálózati maszk:	255.255.240.0	11111111 11111111 11110000 00000000
„D” legkisebb IP címe:	212.32.16.1	11010100 00100000 0001**0000 00000001**
„D” legnagyobb IP címe:	212.32.31.254	11010100 00100000 0001**1111 11111110**
„D” Broadcast IP címe:	212.32.31.255	11010100 00100000 00011111 11111111

Jusson eszünkbe a CIDR korábban említett ökölszabálya! Például a „D” hálózat esetében, ha bármely okból is 212.32.17.1 IP címnél jelöltük volna ki a hálózat IP címét, akkor csak a /24-es maszkot használhattuk volna, azaz csak 256-2 db hosztot tudtunk volna kiosztani!

„Dx” hálózat IP címe:	212.32.17.0/24	11010100 00100000 00010001 00000000
„Dx” alhálózati maszk:	255.255.255.0	11111111 11111111 11111111 00000000
„Dx” legkisebb IP címe:	212.32.17.1	11010100 00100000 00010001 **00000001**
„Dx” legnagyobb IP címe:	212.32.17.254	11010100 00100000 00010001 **11111110**
„Dx” Broadcast IP címe:	212.32.17.255	11010100 00100000 00010001 11111111

A CIDR bevezetésének az útválasztásra gyakorolt hatása az előző példa segítségével érthető meg legegyszerűbben. Az egyes telephelyek közelében lévő útválasztók mindegyikének ismernie kell az egyes telephelyeken lévő hálózatok IP címének előtagjait. Ezek az előtagok (a telephelyek földrajzi elhelyezkedés függvényében) más-más vonalakon történő kapcsolódást jelenthetnek az útválasztókban, azaz telephelyenként ez egy-egy bejegyzést jelent az útválasztók táblázataiban.
Távoli útválasztók esetében azonban az útválasztás logikája kicsit egyszerűsödik. Induljunk ki abból, hogy a közelben (az országon belüli) útválasztók átadják táblázataik tartalmát a távoli (például egy másik ország) útválasztói felé. Ez esetben azonban egy olyan helyi útválasztó, mely mind a négy telephely felé rendelkezik bejegyzéssel – azaz ismeri a továbbmenő vonalat – a távoli útválasztó számára egy összefoglaló címet juttat el. Ezt azért teheti meg, mert a távoli útválasztó számára elég ezen közeli útválasztó megtalálása és az összefoglaló cím tárolása. A négy cég felé vezető irányokat elég, ha a közeli útválasztó ismeri. Ez az összefoglaló cím esetünkben a 212.32.0.0/19.

A négy hálózat összefoglaló IP címe:	212.32.0.0/19	11010100 00100000 00000000 00000000
A négy hálózat hálózati maszkja:	255.255.224.0	11111111 11111111 11100000 00000000
A négy hálózat legkisebb IP címe:	212.32.0.1	11010100 00100000 000**00000 00000001**
A négy hálózat legnagyobb IP címe:	212.32.31.254	11010100 00100000 000**11111 11111110**
A négy hálózat Broadcast IP címe:	212.32.31.255	11010100 00100000 00011111 11111111

Erre a cím összefogásra, csoportosításra (Aggregation) azért volt lehetőségünk, mert azonos régióban kerültek kiosztásra az egymást követő IP címek. Maga a címcsoportosítás folyamata automatikus, az útválasztók kezelői beavatkozás nélkül képesek azt elvégezni. Amennyiben az egyes telephelyek az Internet topológiájában távol vannak egymástól, például különböző kontinenseken helyezkednek el, akkor ez az előny elveszik.
A csomagokat tehát vagy a klasszikus útválasztás módszereivel meghatározott legjobb útvonal irányába, vagy a leghosszabb egyező előtag irányába (Longest Matching Prefix) kell küldeni.

Hálózati címfordítás (NAT)

A címfordítás, mint igény szintén az IPv4 címek belátható időn belüli elfogyásának következtében merült fel. Az IPv4 címek 32 bites hosszából fakadó korlátja, az, hogy az elvileg kiosztható egyedi IP címek száma $2^{32} = 256^4$, azaz összesen „4 294 967 296 db", ráadásul ez a szám már magába foglal jó pár ki nem osztható címet is (Broadcast, Loopback, Private). Tekintettel az Internet folyamatos térhódítására a négy milliárd nem is tűnik olyan nagy számnak. Az IPv4 címek elfogyásának időbeli késleltetéséhez a CIDR 1993-as megjelenése nagyban hozzájárult, amit a 2001-ben a NAT megjelenése követett. A címfordítás technológiája miatt nem került gyorsabban bevezetésre az IPv6 szabvány, amely kifejlesztésének egyik oka az IPv4 fogyatkozó címtartományának kiváltása volt. Hosszabb távon természetesen az IPv6 bevezetése a megoldás.

A hálózati címfordítás (NAT – Network Address Translation) a címfordításra képes hálózati eszközök (útválasztók, tűzfalak) kiegészítő szolgáltatása, mely lehetővé teszi a belső hálózati hosztok közvetlen kommunikációját tetszőleges protokollokon, keresztül külső hálózati (jellemzően Interneten található) hosztokkal. A kommunikációhoz tehát a belső hálózat hosztjainak így nem kell nyilvános IP címmel rendelkezniük. A NAT leírását az RFC3022 dokumentum tartalmazza.

A hálózati címfordítást végző eszköz egy belső hálózatban lévő hosztokról érkező csomagokat az Internetre továbbítás előtt úgy módosítja, hogy azok feladójaként saját magát tünteti fel. Ezért az azokra érkező válaszcsomagok is hozzá kerülnek majd továbbításra, amiket – a célállomás címének visszamódosítása után – a belső hálózaton elhelyezkedő eredeti feladó hoszt részére ad át. A címfordítás tehát egy aktív hálózati eszközt igényel, amely folyamatosan figyeli az érkező csomagokat és azok feladói és címzettjei alapján elvégzi a szükséges módosításokat. A címfordítást általában egy tűzfal végzi el, amely megfelelően szétválasztja a külső Internetet a belső hálózattól. Innen származik a külső, illetve belső hálózat elnevezés is. A belső hálózatnak olyan címtartományt kell adni, amelyet minden hálózati eszköz a nemzetközi szabványoknak megfelelően belsőnek ismer el, és így azokat nem irányítja közvetlenül a külső hálózat felé. A privát, vagy belső tartományokról már volt szó, ezek azok:

Osztály	Privát IP tartomány	Hálózatok és Hosztok (NIC) száma
"A"	10.0.0.0 - 10.255.255.255	1db hálózat, 16777214 db hoszt (NIC)
"B"	172.16.0.0 - 172.31.255.255	16 db hálózat, hálózatonként 65534 db hoszt (NIC)
"C"	192.168.0.0 - 192.168.255.255	256 db hálózat, hálózatonként 254 db hoszt (NIC)

A címfordítás segítségével megoldható, hogy akár egy egész cég teljes belső hálózati forgalma egyetlen külső IP cím mögött legyen, azaz gyakorlatilag egyetlen külső címet használ el egy több száz hosztból álló hálózat. A belső forgalomban természetesen szükség van az egyedi belső címekre, de erről csak a címfordítást végző hálózati eszközöknek kell tudnia, kifelé ennek részleteiről már nem láthatók információk. Így létrejöhet egy olyan konfiguráció is, hogy egy viszonylag nagy cég teljes külső címfoglalása csak kb. 10-20 db IP cím, míg a belső forgalmukban akár több ezer belső IP cím is lehet. Nagy előnye ennek a technikának, hogy ugyanazt a belső tartományt nyugodtan használhatja bárki más is, amíg mindegyik egyedi külső cím mögé van fordítva. Akár az összes NAT-ot használó cég belső hálózatában lehet minden gép a 10.0.0.0 vagy a 192.168.0.0 tartományban, ha kifelé valóban egyedi címmel látszanak.

Az Internet vezérlő protokolljai

A hálózati rétegben nem kizárólag az adatok továbbítására szolgáló IP protokoll használatos, hanem számos egyéb protokoll is. Ezek vezérlési, címszervezési illetve kényelmi feladatokat látnak el. A leggyakrabban a következő protokollokkal találkozhatunk.

- ICMP (Internet Control Message Protocol / Internetes vezérlőüzenet protokoll)
  Az ICMP egy olyan protokoll, mely a hibákról és azok típusáról ad tájékoztatást, illetve a hálózati diagnosztika esetén is használható. Leírását az RFC792 dokumentum definiálja. A szabvány 8 biten ábrázolja az ICMP üzenetek típusait, azaz elvileg 256 féle üzenet létezhet. A 256 lehetséges üzenetből azonban csak 40 féle üzenet van definiálva. Ezek közül is csak a leggyakoribb 11 db üzenet kerül megemlítésre.
  - „0 – Echo Replay” (Ping)
    A „8”-as típusú (visszhang csomag) csomagra érkező válasz.
  - „3 – Destination Unreachable”
    A célállomás nem érhető el, a csomagot nem lehet kézbesíteni. Ennek az üzenetnek 16 altípusa van.
  - „4 – Source Quench”
    Ez egy útválasztók által küldhető üzenet, a forrás elnyomás, ami azt jelzi, hogy az útválasztónak nincs elég memóriája a kérés feldolgozására, ezért kéri a bejövő forgalom csökkentését.

- „5 – Redirect Message”
  Egy valószínűleg rosszul irányított csomaggal kapcsolatos üzenet másik hálózat vagy hoszt felé. Célja, hogy az adott hosztnak küldött üzenetek a megfelelő irányba legyenek elküldve. Ennek az üzenetnek 4 altípusa van.
- „8 – Echo Request” (Ping)
  Visszhang kérése, azaz annak ellenőrzése, hogy a keresett hoszt elérhető-e.
- „9 – Router Advertisement”
  Az útválasztó saját adatainak hirdetése a többi (közeli) útválasztó felé.
- „10 – Router Solicitation”
  A (közeli) útválasztók adatainak kérelmezése.
- „11 – Time Exceeded”
  Egy csomag vagy darab (Fragment) érvényességi idejének (TTL) lejártára figyelmeztető üzenet. Ennek az üzenetnek 2 altípusa van.
- „12 – Bad IP Headers”
  Érvénytelen IP fejrészre, vagy hibás paraméterre figyelmeztető üzenet. Ennek az üzenetnek 3 altípusa van.
- „13 – Timestamp”
  Ugyanaz, mint a „8”-as (Ping) de időbélyeggel együttes kérésről van szó. Célja az időszinkronizáció.
- „14 – Timestamp Reply”
  Ugyanaz, mint a „0”-ás (Ping) de időbélyeggel együttes válaszról van szó. Célja az időszinkronizáció.

- ARP (Address Resolution Protocol / Címfeloldási protokoll)
  Az IP címeket a hálózati kommunikáció során valamely módszerrel mindenképpen az adatkapcsolati rétegben használatos fizikai MAC címekké kell alakítani, hiszen a keretek a fizikai MAC címek segítségével érik el a célállomásokat. Az ARP az IP címek és fizikai címek egymáshoz rendelésének módszere. Segítségével az IP cím ismeretében hozzájuthatunk a 48 bites (az eszköz gyártója által meghatározott) fizikai MAC címhez. Az ARP leírását az RFC826 dokumentum tartalmazza.
  Az ARP protokoll az összerendelt adatokat a memóriájában (ARP Cache) tárolja. Amennyiben egy keresett összerendelés itt nem található meg, akkor azt fel kell kutatni a hálózaton. Ez egy speciális Ethernet Broadcast üzenet küldésével történik az ff:ff:ff:ff:ff:ff MAC címre, (ez egy adatkapcsolati régben lezajló folyamat, nem összekeverendő az IP Broadcast-tal) melyet az összes, a szegmensbe bekapcsolt hoszt megkap. A keresett IP címet mindegyik hoszt összehasonlítja a saját IP címével, és egyezés esetén az érintett hoszt egy ARP választ küld a kérdezőnek.

A kérdező ebből a válaszból olvassa ki a szükséges IP cím és Ethernet cím összerendelést. Az összerendelés ezután bekerül az ARP memóriájába, és ott egy megadott ideig (ARP Refreshtime) megőrzésre kerül. Egy adott hoszt ARP memóriájában tehát csak az adott Ethernet szegmensen levő hosztok IP cím és Ethernet cím összerendelései találhatók, mert egy másik szegmensen levő hoszttal a kommunikáció már (általában) útválasztón keresztül történik.

Két hoszt a következő négy alapesetben veszi igénybe az ARP protokollt:

- Ha a két hoszt ugyanazon a hálózaton található, és az egyik szeretne csomagot küldeni a másik számára.
- Ha a két hoszt különböző hálózaton található, és így útválasztón vagy az alapértelmezett átjárón (Default Gateway) keresztül érik el egymást.
- Ha egy útválasztónak tovább kell küldenie egy hoszt csomagját egy másik útválasztón keresztül.
- Ha egy útválasztónak tovább kell küldenie egy hoszt csomagját a címzettnek, ami ugyanazon a hálózaton található.

Az első esetben a két hoszt ugyanazon a fizikai hálózaton található, vagyis képesek közvetlenül kommunikálni egymással útválasztó igénybevétele nélkül is. A másik három eset – ami az Interneten leggyakoribb – az, amikor bármely két hoszt (jellemzően számítógép) több mint 3 ugrás (Hop) távolságra van egymástól.

- DHCP

  (Dynamic Host Configuration Protocol / Dinamikus hosztkonfigurációs protokoll)

  A DHCP protokoll feladata az, hogy a TCP/IP hálózatra csatlakozó hosztok automatikusan megkapják a hálózat használatához szükséges beállításokat, IP címet, a hálózati maszkot és az alapértelmezett átjáró IP címét. A protokoll leírását az RFC1541 és RFC2131 dokumentumok definiálják. Három féle IP cím kiosztási módszer használatos a DHCP segítségével.

  - statikus

    A kiosztás alapja egy, a MAC címekre épülő algoritmus, illetve lehetőség van manuális IP cím kiosztásra is.
  - automatikus

    Címkiosztás az IP tartomány megadásával.
  - dinamikus

    Címkiosztás az IP tartomány megadásával, és az IP címek „újrahasznosításával”. Az újrahasznosítás paramétere a bérleti idő (Lease Time), amely a már egyszer kiosztott IP cím újra kioszthatóságát jelenti. Csak a bérleti idő lejárta után osztható ki az adott IP cím másik hoszt részére.

DHCP szerverek használata esetén bárki, akinek fizikai kapcsolata van a hálózattal, könnyen juthat IP címhez, így a DHCP használata megkönnyíti a hálózati betöréseket is. Védelem nélküli (vagy nem kellően védett) vezeték nélküli hálózatok esetében a DHCP egyszerű hozzáférést biztosít a sugárzás hatókörén belül a hálózathoz – hiszen ez esetben fizikai kapcsolata sincs szükség. A behatoló így elérheti az Internet használatot és a (nem kellőképpen védett) megosztott erőforrásokat is.

Az útválasztás protokolljai (Routing Protocol)

Az útválasztás az a folyamat, ami során egy hálózati protokoll egy csomagja az útválasztók sorozatán keresztül a feladó hoszttól eljut a címzett hosztig. Mindenképpen szükség van arra, hogy az útválasztók kommunikáljanak egymással, hogy korábban tárgyalt útválasztó algoritmusok segítségével eldönthessék, hogy egy adott végcél (hoszt) felé melyik irányba kell továbbítani a csomagot. Tekintettel arra, hogy az Internet autonóm rendszerekből (AS) áll, az egyes rendszerekben más-más protokollok használatosak. Maguk a rendszerek is szétválaszthatóak az útválasztás szempontjából körzeten belüli (Intradomain Routing) illetve körzetek közötti (Interdomain Routing) útválasztást használó rendszerekre. Előbbieket belső átjáró protokollnak (IGP – Interior Gateway Protocol), utóbbiakat külső átjáró protokollnak (EGP – Exterior Gateway Protocol) nevezzük. Az útválasztás protokolljai a kommunikáció módját és az útvonal kiválasztásának mikéntjét is meghatározzák. Más megfogalmazásban az útválasztás protokolljai a korábban tárgyalt útválasztó algoritmusok gyakorlati megvalósításának módjai.

- RIP (Routing Information Protokoll)
  Az első IGP protokoll, az útválasztási információs protokoll (RIP) egy távolságvektor alapú protokoll, amely első verziójában maximum 15 ugrással (Hop) valamint egy időzítő segítségével és a hálózati útvonalak költségei alapján igyekezett az útválasztás feladatát megoldani. 1988-ban vezettek be, és leírását az RFC1058 dokumentum tartalmazza. A maximum 15 ugrás a kompatibilitás miatt a későbbi verziókban is megmaradt, de a protokoll eszköztára már a CIDR lehetőségeihez is alkalmazkodott. Legnagyobb problémája, hogy nem mentes a végtelenig számolás problémájától, a hurokmentességtől és hogy az egyre nagyobb hálózatok kiszolgálására csak korlátozottan alkalmas.

- OSPF (Open Shortest Path First)
  Az OSPF szintén IGP protokoll – a nyílt hozzáférésű, a legrövidebb utat preferáló protokoll – melyet 1990-ben vezettek be, és leírását az RFC2328 (v1) és RFC1247 (v2 1991) dokumentumok tartalmazzák. Az OSPF főleg a RIP hibáinak a kijavítását célozta meg sikerrel, hiszen az OSPF egy kifinomultabb, kevesebb sávszélességet igénylő hurokmentes megoldást kínál. A távolság vektoros útválasztás (Ditance Vector Routing) módszere helyett az OSPF a kapcsolatállapot alapú útválasztás (Link State Routing) módszerét használja.
- BGP (Border Gateway Protocol)
  A határátjáró protokoll (BGP) tulajdonképpen egy EGP protokoll, hiszen a különböző AS-ek közötti útválasztás a feladata. A BGP-nek is komoly evolúciója van, első verziója 1989-ben jelent meg, leírását az RFC1105, RFC1163, RFC1164 dokumentum tartalmazta. Ezeket követte az RFC1267 (v2 1991), RFC1771 (v3 1995, ez már a CIDR lehetőségeihez is alkalmazkodott) és az RFC4271 (v4 2006) dokumentum.
  A BGP segítségével, felhasználás jellege miatt tetszőleges topológiákat is tudnunk kell támogatni, de közben gondoskodni kell a hurokmentességről is. A távolság vektoros útválasztás itt optimálisan azért nem használható, mert nem mindig a legolcsóbb útvonal a kívánatos. A kapcsolatállapot alapú útválasztás pedig azért használhatatlan, mert ehhez az egész Internet topológiáját tárolni kellene, ami még az AS szinten is megoldhatatlan. Az IETF ezért alkotott meg egy közbülső, új megoldást, az út-vektorokat (Path Vectors). A módszer lényege az, hogy minden terjesztett útvonalban a célpontig vezető teljes útvonalat leírjuk. Így a hurokmentességet minden útválasztó könnyen ellenőrizhet. Ha egy megkapott útvonalban már szerepel, akkor azzal az útvonallal már nem foglalkozik a továbbiakban. Emellett nincs szükség valamilyen, az egész Internetben egységes költség definiálására, hiszen mindenki a teljes útvonalat saját szempontjai szerint pontozza. Az eljárás legfőbb előnye a hatékonyság, egyetlen hátránya a nagy memóriaigény, az útválasztók tábla bejegyzéseinek jelentős növekedése.

Többesküldés (Multicast) az Interneten

Az eddigiekből már kiderült, hogy a „D” osztályú címek a Multicast céljára vannak fenntartva. Minden „D” osztályú cím tehát egy hoszt csoportot jelöl, így – elvileg – akár egyszerre sok millió ügyfélnek küldhetünk IP csomagokat. A gyakorlatban ez azonban szinte kivitelezhetetlen, hiszen minél több hosztról beszélünk, annál változatosabb földrajzi eloszlásban helyezkedhetnek el az egyes hosztok. Azaz elküldhetjük a

csomagokat, de arra semmi garancia sincs, hogy azok minden érintett hoszthoz meg is érkeznek. Kijelenthetjük tehát, hogy a Multicast mint feladat, nem tökéletesen megoldott, hiszen a Multicast alapesetben úgy valósítható meg, hogy minden a csoporthoz tartozó útválasztó számára egyesével elküldjük a Multicast csomagokat, miközben az is fontos lenne, hogy egy csomag csak egyszer haladjon végig egy útvonalon. Az útválasztóknak azt a feladatot kell megoldaniuk, hogy megvizsgálják az összes „D" osztályú címmel feladott csomagot és kiszűrjék azokat, melyek nekik nem szólnak. Valamilyen módon azonban az útválasztók tudomására kell hozni, hogy az adott útvonalon van-e olyan hoszt, amely tagja a megcímzett Multicast csoportnak.

Ennek az összetett feladatnak a megoldására hozták létre az Internetes csoportkezelő protokollt (IGMP – Internet Group Membership Protocol) 1989-ben, melynek a leírását az RFC1112 (v1), RFC2236 (v2, 1997), RFC3376 (v3, 2002) és RFC4604 (2006) dokumentumok tartalmazzák. A feladat nem egyszerű, ahogyan azt a protokoll evolúciója is jelzi. Az IGMP olyan pont-multipont alkalmazások esetében használatos, mint a Video Streaming vagy a csoportos játék, és célja az igénybevett erőforrások hatékonyabb kihasználása. Az IGMP protokoll működésének lényege az, hogy az érintett útválasztók lekérdező- és válaszcsomagok segítségével egy speciális többesküldés-feszítőfát (Multicast Spannig Tree) hoznak létre. Tehát kétféle IGMP üzenet létezik, az egyik segítségével az útválasztók kérdezik le a csoporttagságot, a másikkal pedig az hosztok válaszolnak, egy-egy választ küldve minden csoporthoz, melynek tagjai. A válaszokból áll össze a csoporttagságokat tartalmazó táblázat.