Hálózatok (21. rész) – Az Ipv6

Az IP protokoll ma használt változata, az IPv4 felett eljárt az idő. Előbb-utóbb elfogynak a még ki nem osztott IP címek, és egyre kevésbé tud megfelelni a 21. század igényeinek. Hamarosan eljön tehát az IPv6 kora.

Már a 90-es évek elején, az internet robbanásszerű terjedésének kezdetekor látható volt, hogy kevés az a 32 bit, amelyen az *IP* címeket tárolják. Ugyan a *CIDR* bevezetésével (lást előző rész) egy kis idő nyerhető, de előbb vagy utóbb el fognak fogyni a még szabadon kiosztható *IP* címek.

Az internetbe kapcsolt gépek száma még ma is nagy léptékben növekszik, és ez várhatóan a jövőben sem fog változni. Viszont az új gépek nagy része valószínűleg nem újabb számítógépek bekötését fogja jelenteni (habár az Interneten jelenlévő számítógépek száma továbbra is exponenciálisan emelkedni fog). Az internet ma már új iparágak célpontja, mint például a telekommunikáció vagy a szórakoztató ipar, amelyek hihetetlenül nagyszámú eszközt szeretnének az internethez kapcsolni. Gondoljunk például az interneten keresztüli telefonálásra, vagy olyan televíziókészülékre, amely egyben internetes gépként is működik. Ezeknek az új eszközök bekötéséhez nem áll elegendő *IP* cím rendelkezésre.

A túl kicsi címtéren kívül más problémák is vannak az *IPv4*-el. Először is nem foglalkozik kellőképp a szolgálat típusával, minden csomagot ugyanúgy kezel, tartalmazzon az akár egy e-mailt, vagy egy valósidejű médiafolyamot.

Ezenkívül nem tartalmaz semmiféle hitelesítési és titkosítási szolgáltatást. Egy gép sosem lehet biztos abban, hogy a csomag tényleg attól érkezette, aki feladóként szerepel, ráadásul az átmenő csomagok tartalmába az néz bele, aki csak akar. Ha ez ellen tenni szeretnénk valamit, akkor azt csak alkalmazás szinten tehetjük meg, azaz olyan programokat kell használnunk, amelyek saját maguk gondoskodnak az átvitel titkosságáról.

Szükség volt még az *IPv4* csomagok fejlécének egyszerűsítésére is. A bonyolult, sok mezőből álló fejléc feldolgozása komoly teljesítményt igényel, így az útválasztóknak tovább tart feldolgozniuk egy-egy csomagot.

Világos tehát, hogy szükség volt egy új protokollra, amelynél nem állnak fent ezek a problémák. Ezért már 1990-ben elkezdtek dolgozni az új *IP* protokollon, amelynek eredménye az először 1993-ban publikált ***SIPP (Simple Internet Protocol Plus)*** lett, amit ma már csak ***IPv6*** néven emlegetnek.

(A logika azt diktálná, hogy az *IPv4* következő generációjának *IPv5* legyen a neve, de ez a név már sajnos akkor foglalt volt, egy kísérleti folyamalapú protokoll birtokolta). Minden bizonnyal ez a protokoll lesz az, amely egy nap kiváltja majd az *IPv4*-et (habár egy a váltás a gépek nagy száma miatt nem egyik napról a másikra fog bekövetkezni), ezért mindenképp érdemes közelebbről is megismerkednünk vele.

Prefix	Use
0000 0000	Reserved
0000 0001	Unassigned
0000 001	Reserved for NSAP Allocation
0000 010	Reserved for IPX Allocation
0000 011	Unassigned
0000 1	Unassigned
0001	Unassigned
001	Unassigned
010	Provider-Based Unicast Address
011	Unassigned
100	Reserved for Geographic-Based Unicast Addresses
101	Unassigned
110	Unassigned
1110	Unassigned
1111 0	Unassigned
1111 10	Unassigned
1111 110	Unassigned
1111 1110 0	Unassigned
1111 1110 10	Link Local Use Addresses
1111 1110 11	Site Local Use Addresses
1111 1111	Multicast Addresses

1. ábra Az IPv6-os címtartomány felosztása

Az IPv6 legfontosabb tulajdonságai

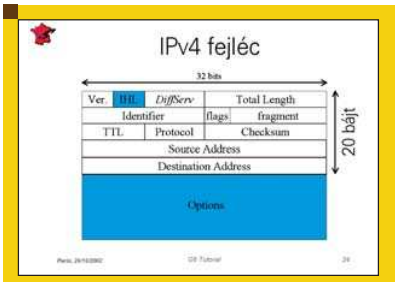
Először is, az ***IPv6*** 128 bites címekkel dolgozik. Ez elegendő ahhoz, hogy jó időre, hacsak nem örökre megszabaduljunk a kiosztható címek hiányából fakadó problémáktól.
Az ***IPv6*** fejléce egyszerűsödött. Míg az ***IPv4*** csomagok fejléce 13 mezőt tartalmaz, addig az ***IPv6*** fejléc csak 7-et. A legtöbb mező opcionális lett, azaz csak akkor szerepel a csomagban, ha tényleg szükség van rá.
Ez a megoldás elősegíti a többletterhelés csökkentését, mivel az útválasztók könnyen átugorhatják azokat az információkat, amelyek nem érdeklik őket. Az ***IPv6*** fejléc csupán a duplája az ***IPv4*** fejlécnek, ami nem mondható rossznak, ha figyelembe vesszük azt, hogy a forrás- és a célcím mérete megnégyszereződött.
Az ***IPv6*** az elődjénél sokkal jobban odafigyel arra, hogy mit szállít a csomag, azaz mi a szolgálat típusa. Igaz, erre 8 bit az ***IPv4***-ben is rendelkezésre állt, manapság azonban ez nem tűnik valami soknak, a jövőben meg biztosan nem lesz elegendő.
A legutolsó, ám egyáltalán nem elhanyagolható újítás a biztonság terén történő előrelépés. Végre a hálózati réteg szintjén is lehetőség van a hitelesítésre és a titkosításra.

Címzés az IPv6-ban

Mint már említettük, az ***IPv6*** 32 bites címek helyett 16 bájtos, azaz 128 bites címeket használ. 16 bájton rendkívül sok cím ábrázolható, olyan sok, hogy gyakorlatilag soha többé nem kell szembesülnünk a szabad címek hiányával. Az sem jelent problémát, hogy a címek elég gazdaságtalanul, hierarchikus módon kerülnek kiosztásra. Még így is a ***Föld*** minden négyzetméterére több ezer cím jut.
Az ***IPv6*** címeket különböző kategóriákba soroljuk az első bájtjuk, az úgynevezett ***format prefixük*** alapján.
Az *1. ábrán* látható táblázat mutatja, hogy milyen csoportokra is bontjuk a 16 bájtos címtartományt. (Fontos megjegyezni, hogy a címtérnek körülbelül csak a 16%-a van lefoglalva, a többi tartalékként, későbbi kihasználásra várnak).
Az ***IPv6*** két címkiosztási stratégiát definiál, és mindkét módszer számára fenntart egy-egy címtartományt. Ezek közül az elsők a 010-val

2. ábra Az IPv6 csomagok fejléce

kezdődő úgynevezett ***Provider based unicast address (szolgáltató alapú egyesküldésű címek)***. Ez a kiosztás némileg hasonlít arra, ahogy a telefontársaságok kiosztják ügyfelei között a telefonszámokat.
Az összes vállalat rendelkezik a telefonszámok egy bizonyos tartományával, amelyeket hozzárendel az előfizetők vonalaihoz. A telefonszámok első pár számjegye azonosítja a szolgáltatót, a többi pedig az ügyfelet. A gyakorlatban a szolgáltató azonosítása két lépcsős: először magát az országot kell azonosítani az előhívószámmal, majd utána következik a szolgáltató kódja.
A szolgáltató alapú címkiosztás is hasonló módon épül fel. A prefix utáni 5 bit meghatároz egy nyilvántartót, amely a hozzá tartozó címtartományt felosztja a szolgáltatók között. Ezután a szolgáltatót azonosító bitek következnek (hogy erre hány darab bit szolgál, az csak a nyilvántartótól függ). A maradék bitek pedig magát az interfészt azonosítják.
Ez a fajta kiosztás szöges ellentétben áll a mai ***IPv4***-es címkiosztással, amelyben a szolgáltatók nem játszanak főszerepet. A másik csoportot, a ***Geographic Based Unicast Addresses (Földrajzi alapon történő egyesküldésű címek)*** a „hagyományos”, ***IPv4***-es módszer szerint kiosztott címek számára van fenntartva. Az ***IPv6 unicast*** címek ily módon történő felosztásának köszönhetően mindkét fajta címkiosztás lehetséges.
A ***helyi használatú címek (local use addresses)*** a belső hálózatok számára vannak fenntartva, amelyek elszigetelten, tűzfalak árnyékában élik életüket. Az ilyen címek felé menő csomagokat egy útválasztó sem továbbítja a kommunikációs alhálózat felé.
Kétféle helyi használatú cím létezik. Az első a ***kapcsolati lokális cím (Link Local Address)***. Ezt akkor használják, ha a hálózaton lévő összes gép egyetlen ***LAN***-on van. Ilyenkor mind a 118 bit rendelkezésre áll az interfész azonosítására. A másik típus a ***hely lokális cím (Site Local Address)***, amely egy belső intranet kialakítására szolgál. Ilyenkor hálózatunk több különálló ***LAN***-ból áll, amelyeket egymással útválasztókkal kapcsolunk össze. Ebben az esetben a cím első pár bitje szolgál az egyes ***LAN***-ok



3. ábra Az IPv4 csomagok fejléce

azonosítására.
A ***többesküldésű (multicast)*** címek mindig nyolc darab egyessel kezdődnek. Ezek a címek ***unicast*** címek egy csoportját azonosítják. Az erre a címre küldött csomagot a csoport összes tagja megkapja (lásd az előző részt).
Az ***IPv6*** rendelkezik egy új funkcióval, mégpedig a ***bárhova küldéssel (anycasting)***. Ilyenkor szintén interfészek egy csoportjának küldünk egy csomagot, viszont közülük csak az egyik kapja meg (általában az, amelyik a legközelebb helyezkedik el a géphez).
Ha például van több, ugyanazzal a tartalommal ellátott (úgymond tükrözött) fájlszerverünk, és ezekhez rendelünk egy ***anycast*** címet, akkor a gépek ezen a címen mindig kapcsolatba léphetnek valamelyikükkel. Hogy a több szerver közül ki lesz az a kiválasztott, aki a csomagot megkapja, azt az útválasztók döntik el. Az ***anycast*** címek tartományát hiába keressük az 1. ábrán, ugyanis ilyen nem létezik. Az ***anycast*** címek az ***unicast*** címek közül kerülnek kiválasztásra, így elvileg lehetetlen egy címről eldönteni, hogy az ***unicast***, vagy ***anycast*** cím-e.
(Az ***unicast*** és ***anycast*** címek közötti különbség gyakorlatilag annyi, hogy míg az ***unicasthoz*** csak egyetlen interfész van rendelve, addig az ***anycasthoz*** egyszerre több).
Az ***IPv6*** címeket nyolc darab négy hexadecimális számmal jelöljük, amelyeket egymástól kettősponttal választunk el. Például:

0100:0000:0000:0123:4567:89AB:CDEF:
➥1234

Ezt a címet azonban rövidebben is leírhatjuk, például a ***0123***-at ***123***-ként is jelölhetjük. A cím méretét csökkenthetjük azzal is, hogy a ***0***-t nem írjuk ki, sőt, ha több 0 van egymás mellett, akkor az egészet két kettősponttal helyettesítjük. Az előbbi cím tehát így nézne ki rövidebben:

0100::123:4567:89AB:1234.

Az IPv6 csomagok fejléce

A 2. *ábrán* látható az ***IPv6*** csomagok fejlécének felépítése. Most gyorsan áttekintjük, hogy melyik mező mire szolgál.
A prioritás mező segít az útválasztóknak, hogy könnyebben megbirkózzanak a torlódásokkal. A csomagok a prioritás mezőjük szerint két csoportba oszthatók: a 0 és 7, illetve a 8 és 15 közöttiekre. Az első csoportba azok a csomagok tartoznak, amelyek olyan forrásból származnak, amik képesek a forgalomszabályozásra (torlódás esetén visszavehetnek az adás sebességéből). A másik csoport tipikusan valósidejű forgalmat szállít, például hangot vagy mozgóképet. Az ilyen csomagokat kibocsátó alkalmazások sosem változtathatnak az adás tempóján, még akkor sem, ha fennáll a veszély, hogy egyes csomagok útközben elvesznek.
E két csoportot tovább bonthatjuk fontosabb és kevésbé fontosabb csomagok osztályára. Az első csoportot véve példaként, az 1 értékű prioritású mező egy olyan csomagot jelöl, amelyet az útválasztók nyugodtan késleltethetnek, hiszen senki sem fog megbotránkozni, ha pár másodperccel később éri el a célját. Vannak azonban olyan, többnyire interaktív forgalmat szállító csomagok, ahol minden másodperc késlekedés a felhasználókban komoly indulatokat szülhet. Tipikusan ilyen a ***telnet*** vagy az ***ssh***. Az ilyen csomagokhoz legalább 6-os prioritási szintet érdemes rendelni.
A prioritás mező használata lehetőséget ad a beleszólásra, hogy az útválasztók miként kezeljék csomagjainkat, ám van amikor ennél többre van szükségünk. Például két alkalmazás kommunikációjához szükség van valamiféle speciális késleltetésre. Erre nem tudjuk az útválasztókat rávenni kizárólag a prioritás mező használatával.
Erre találták ki az ***IPv6*** folyamcímke (***flow label***) nevű szolgáltatását, amely jelenleg még csak kísérleti jellegű. Segítségével a forrás és a cél között egyfajta álösszeköttetést, úgynevezett folyamot hozhatunk létre, amely különböző tulajdonságokkal rendelkezik (például sávszélesség). A folyamon keresztül haladó csomagok egyedi bánásmódot igényelnek az útválasztóktól. Az útválasztók úgy továbbítják ezeket a csomagokat, hogy ne sértsék meg az adott folyam előírásait. Ha például elő van írva egy meghatározott sávszélesség, akkor az útválasztóknak garantálniuk kell, hogy ez a paraméter ne sérüljön. Ez a szolgáltatás tulajdonképpen nem más, mint hogy virtuális áramkör alapú alhálózat „szimulálása" egy datagram alapú alhálózaton. Ez egyfajta egyesítése a két típusú alhálózatnak úgy, hogy nem sérül a datagram alapú alhálózatok rugalmassága, viszont kiegészül a virtuális áramkör által nyújtott garanciákkal.
Hogy egy csomag melyik folyamba tartozik, azt a folyamcímke mezője határozza meg. Ha egyik folyamhoz sem tartozik, akkor a mező értéke mindig nulla. Az útválasztók a folyamokat egyértelműen azonosítani tudják a forrás és célcím, illetve a folyamcímke mező alapján.
Az ***IPv6*** fejlécét úgy sikerült egyszerűsíteni, hogy azokat a mezőket, amelyekre nincs minden csomagnál szükség, opcionálissá tettek. Az opcionális fejrészeket csak akkor kell a fejléchez csatolni, ha valóban szükség is van rájuk. A 2. ábrán az ***IPv6*** fejlécnek csak a kötelező 40 bájtos részét tüntettük fel. Az opcionális mezők ezután következnek, ezek méretét a ***Payload Length*** nevű mező tartalmazza. Az opcionális részek a 40 bájtos kötelező rész után következnek. Hogy ezek közül melyik az első, azt a ***következő fejléc (next header)*** mező mondja meg. Az utolsó fejléc következő fejléc mezője pedig azt mondja meg, hogy a csomag tartalmát melyik szállítási rétegbeli protokoll (***TCP*** vagy ***UDP***) kezelőjének kell átadni.
Hat típusú opcionális fejrész létezik, ezek nagy részével az útválasztók számára állíthatunk be bizonyos paramétereket. Ezenkívül itt adhatjuk meg a hitelesítésre és a titkosításra vonatkozó paramétereket. Ezek használatához a kommunikáló feleknek először meg kell egyezniük egy vagy több titkos kulcsban

(hogy ezt miként teszik, azzal az *IPv6* nem foglalkozik).
Hitelesítés esetén nincs szükség a csomag tartalmának titkosítására. Ilyenkor csak ki kell nullázni a fejléc azon adatait, amelyek útközben változhatnak (például ugrásszámláló), majd a csomaghoz fűzni a titkos kulcsot, és így elkészíteni a csomag lenyomatát például az *MD5* algoritmussal.
Az *IPv6*-ban a titkosítás is algoritmusfüggetlen, lényegében csak az adón és a vevőn múlik. Mindenesetre, az átjárhatóság érdekében, a *DES-CBC* nevű algoritmus használata a javasolt (a titkosító algoritmusokról sorozatunk egy későbbi részében részletesen is beszélünk).
Az *ugráskorlát (hop limit)* mező akadályozza meg a halhatatlan, az alhálózaton az idők végezetéig bolyongó csomagok létezését. Ez a mező teljesen megegyezik az *IPv4* élettartam nevű mezőjével.
Érdemes egy rövid összehasonlítást végezni az *IPv6* és az *IPv4* csomagok fejléce (3. *ábra*) között. Először is eltűnt az *IHL* és a *Protokoll mező*, mivel az *IPv6* fejlécek rögzített méretűek, másrészt a *Next Header* mezőből kinyerhető, hogy a csomag tartalma milyen szállítási protokollhoz köthető. Eltűntek továbbá az IP csomagok darabolására vonatkozó részek is.
Ez azzal magyarázható, hogy az *IPv6* útválasztók nem darabolják a csomagokat. A szabvány szerint minden útválasztónak kezelnie kell az 576 bájtos csomagokat, viszont az ennél nagyobbakat el kell dobniuk, és hibaüzenetet kell küldeniük a küldő állomás felé. Ha mégis nagyobb méretű csomagokat szeretnénk küldeni, akkor a darabolásról a forrásnak kell gondoskodnia.
Ez a gépek szempontjából visszalépésnek számít, viszont az útválasztók munkája egyszerűsödött, ezáltal gyorsabban dolgozhatják fel a beérkező csomagokat.
Szintén nem találjuk sehol az *ellenőrző összeg (checksum)* mezőt. Ennek oka az, hogy az *IPv6* nem is számol ilyet, mivel a felsőbb rétegbeli protokollok úgyis ellenőrzik az adatok sértetlenségét.

Az áttérés

Az *IPv6* egy rugalmas és gyors protokoll, amely bőséges címtartománnyal rendelkezik. Ezen tulajdonságai alkalmassá teszik, hogy kiváltsa az Interneten jelenleg uralkodó *IPv4* protokollt. Ez az átállás azonban nem egyik pillanatról a másikra fog megtörténni. A már telepített *IPv4*-es gépek nagy száma miatt lehetetlen megoldani, hogy vasárnap éjszaka leállítani az egész Internetet, majd hétfő hajnalban újraindítani úgy, hogy mindenki az *IPv6*-ot használja.
Az átállás folyamatosan, kisebb lépésenként fog történni. Már ma is rengeteg hálózat használja az *IPv6*-ot, egyfajta a „külvilágtól” elzárt szigetet alkotva az Internet hálózatai tengerében. Ezek az *IPv6* hálózatok egymással úgynevezett *alagutakon (tunnel)* keresztül kommunikálnak. Az alagút segítségével egy hálózaton keresztül olyan csomagokat vihetünk át, amely nem kompatibilis az adott hálózattal. Egy *IPv6* csomagot például nem indíthatunk útnak az Internet kommunikációs alhálózatán keresztül, hiszen ezek az útválasztók ma még *IPv4*-et használnak (habár az újabb útválasztók már mindkét protokollt ismerik). Ezért a két *IPv6*-os hálózat között egy alagutat kell létrehozni, amelyen az *IPv6*-os csomagok vándorolnak.
Ez a gyakorlatban úgy működik, hogy az elküldendő *IPv6*-os csomagot berakjuk egy *IPv4*-es csomag belsejébe, és azt indítjuk útnak a célpont hálózat felé. Az alagutak működésére a legjobb szemléltető példa a *Franciaországot Angliával* összekötő *Csalagút*. Ebben az alagútban csak vonatok közlekedhetnek, autók csak úgy, mint a vonatok rakománya. A közúton persze az autók gond nélkül haladhatnak, de az alagútban nem, ott őket vonaton át kell szállítani.
A jövőben ezek a ma még elszigetelt *IPv6* szigetek egyre nagyobb méretűek lesznek, az egyes szigetek egymásba olvadva még nagyobb hálózatokat hoznak létre. Az áttérés utolsó pillanata valószínűleg az lesz, amikor az utolsó két nagy sziget is egymásba olvad.
Hogy ez mikor fog bekövetkezni, nehéz kérdés. Az biztos, hogy még jó pár évre van szükség. Mindenesetre az *IPv6* terjedése ma már sokkal gyorsabb mint régen, mivel az útválasztók és az operációs rendszerek egyre szélesebb körben támogatják az új internet protokollt.
Ezzel be is fejeztük a hálózati réteg bemutatását, a következő résztől a szállítási réteggel és azok protokolljaival, a *TCP*-vel és az *UDP*-vel foglalkozunk.

Garzó András (garzo@interware.hu)
Körülbelül három éve foglalkozik Linux- és más Unix-rendszerekkel. Legjobban az operációs rendszerek lelkivilága érdekli, de nyitott egyéniség. Kedvenc étele a palacsinta, és van egy Richard nevű macskája. Minden észrevételt, megjegyzést, levelet szívesen fogad.