IPv6 – A jövő Internet-protokollja?

FARKAS KÁROLY

Computer Engineering and Networks Laboratory (TIK)
Swiss Federal Institute of Technology Zurich (ETH Zurich)
farkas@tik.ee.ethz.ch

Kulcsszavak: Internet, IP, IPv4, IPv6

A kapocs, amely a globális Internetet összefűzi az Internet Protokoll vagy röviden IP. Ellentétben számos más hálózati rétegbeli protokollal, az IP-t a kezdetektől fogva arra tervezték, hogy alkalmas legyen különböző számítógép hálózatok közötti kommunikáció megvalósítására. Az IP elsődleges feladata datagramok[1] továbbítása a forrás- és célállomás között a lehetőségekhez képest legoptimálisabb (best effort) módon. A jelenleg használatban lévő az IPv4-es, amely egy régi[2] és világszerte elterjedt protokoll az Internet hálózatban, azonban úgy tűnik, hogy nem képes lépést tartani az óriási arányban növekvő, az Internethez csatlakozó eszközök számával és az egyre bonyolultabb útvonalválasztási megoldásokkal, még a folyamatosan kifejlesztett kiterjesztések ellenére sem. Mi lesz hát az Internettel, ha majd egy szép napon az IPv4 már nem lesz képes többé betölteni eredeti funkcióját? A javasolt megoldás egy új és sokkal hatékonyabb, az úgynevezett 6-os verzió (IPv6) bevezetése. De vajon valóban reális ez az elképzelés? Ha igen, mikor fog ez az átállás bekövetkezni?

1. Bevezetés

Az Internet napjainkban összeköttetést biztosít világszerte számos hoszt és számítógép hálózat között. Ez a világméretű kommunikációs hálózat az ARPANET nevezetű, az amerikai védelmi minisztérium által az 1960-as évek elején létrehozott hálózatból fejlődött ki. Miután 1983. január 1-től az ARPANET hivatalos protokollmodellje a TCP/IP (Transmission Control Protocol/Internet Protocol – átvitelt vezérlő protokoll/Internet protokoll)[3] lett, az ARPANET-hez kapcsolódó hálózatok, gépek és felhasználók száma ugrásszerűen megnőtt. Ez az időpont tekinthető a mai Internet 'születésnapjának'.

Az Internet sikere a nagyszámú, különféle alkalmazás – mint például az e-mail, fájl transzfer, World Wide Web vagy többfelhasználós játékok –, illetve számos, különböző számítógép hálózat IP támogatásának az eredménye. Ezen alkalmazásoknak köszönhetően látványos multimédia tartalom válik elérhetővé akár egy egérkattintás hatására, mely nagymértékben hozzájárul az Internet gyors növekedéséhez. Az elmúlt évtized folyamán ez a növekedés exponenciális méretet öltött, és az iram várhatóan az elkövetkezendő években sem fog alábbhagyni, ami azt jelenti, hogy az Internethez kapcsolódó gépek száma évente mintegy megduplázódik.

Ennek az óriási sikernek a következménye ugyanakkor az Internet jelenlegi legnagyobb dilemmája: meddig lesz még alkalmas az aktuális IP verzió lépést tartani az Internet növekedési ütemével és mi fog történni, amikor már az IPv4 nem lesz tovább képes elvégezni feladatát? A probléma az Internet természetéből és működési módjából fakad. Minden gépnek, amely az Internethez csatlakozik, egy IP cím nevezetű, egyedi azonosítóval kell rendelkeznie. Ezen cím segítségével lehet az egyes gépeket megkülönböztetni egymástól és a logikai kommunikációs kapcsolatok végpontjait azonosítani. Ez azért fontos, mert a továbbítandó adat a küldő és fogadó hoszt között, ahogy az általában adathálózatokban lenni szokott, kis csomagokra van bontva és minden egyes csomagot a közbülső állomások a forrás- és célállomás közötti logikai útvonal mentén egyedileg kezelnek. Így minden egyes adatcsomagnak tartalmaznia kell információt a csomag feladójáról és a célállomásról, ahová a csomagnak el kell jutnia, ezáltal lehetővé téve a közbülső állomások számára a csomagok helyes irányba történő továbbítását.

Az eljárást lépésről lépésre történő útvonalválasztásnak (hop-by-hop routing) nevezzük. Minden közbülső állomás – amelyeket gyakran útvonalválasztóknak (router) hívunk – a beérkező adatcsomagban található, a célállomásra vonatkozó IP címet összehasonlítja a saját útvonalválasztási táblájában (routing table) szereplő bejegyzésekkel. Egy ilyen bejegyzéshez egy IP címtartomány és egy szomszédos csomópont azonosítója tartozik. Amennyiben a cél IP cím beleesik valamelyik bejegyzéshez tartozó IP címtartományba, az állomás továbbítja a csomagot a bejegyzéshez tartozó szomszédos csomópontjának. Ha nincs egyezés, a csomag az alapértelmezett útvonal (default route) mentén továbbítódik, amely útirány tartalmaz olyan útvonalválasztót, amelyik várhatóan ismeri a célállomáshoz vezető utat.

Az IPv4 32 bit hosszúságú bináris számokat használ IP címként, amely 'csak' $2^{32} \approx 4{,}3$ milliárd ($4{,}3 \times 10^9$) számítógép azonosítását és címzését teszi lehetővé[4].

1 Különálló adatcsomagok, melyeket a hálózat egyedileg kezel
2 Az első IPv4 implementáció 1981-ben született
3 A TCP/IP tulajdonképpen az Internet esetén használt protokoll rétegmodell elnevezése, amely számos különböző Internet protokoll gyűjtőneveként használatos
4 A gyakorlatban ez a limit egy kicsivel alacsonyabb, mert ebből a tartományból nem minden szám használható fel egyedi hoszt IP címeként

Jelenleg e címtartomány közel 70%-a van használatban vagy lefoglalva, míg a maradék, hozzávetőleg 1,3 milliárd cím még felhasználható. Mondhatnánk, hogy ez még mindig egy óriási szám! Igen ám, de annak fényében, hogy Kína egymaga fel tudná használni a maradék IPv4 címtartományt egy év leforgása alatt, a helyzet sokkal válságosabbnak tűnik és könnyen vezethet az IPv4 címtartomány kimerüléséhez (address space depletion).

Ezen felül további problémái az IPv4-nek a komplex protokoll fejrész, az új opciók és kiterjesztések hozzáadásának bonyolult folyamata, a különböző szolgáltatások korlátozott száma, az útvonalválasztási táblák folyamatosan növekvő mérete és komplexitása, valamint a korlátozott biztonság. Ezek áthidalása érdekében 1990-ben az IETF (Internet Engineering Task Force)[5] [1] elkezdte a kidolgozását egy új IP verziónak, amely manapság IPv6 néven ismert. Noha az új protokoll lényegi részeinek a szabványosítása már befejeződött, a világméretű áttérés az IPv6-ra még várat magára.

A továbbiakban áttekintjük az IPv6 fontosabb tulajdonságait és ismertetjük a főbb érveket, melyek az IPv4 teljes, IPv6 általi leváltása mellett és ellen szólnak, valamint kitérünk arra is, hogy ez az átállás várhatóan mikor fog bekövetkezni, ha egyáltalán bekövetkezik...

2. Az IPv6 protokoll

Előre látva az IPv4 problémáit, 1990-ben az IETF elkezdett munkálkodni egy új IP verzión, amely soha nem fogyna ki a címekből, megoldást nyújtana az említett problémákra és sokkal hatékonyabb és rugalmasabb lenne elődjénél [2]. A fő célkitűzések a következők voltak:

- Hosztok milliárdjainak támogatása, még tetszőleges címtartomány-hozzárendelés esetén is;
- Az útvonalválasztási táblák méretének csökkentése;
- A protokoll egyszerűsítése, lehetővé téve ezzel az útvonalválasztóknak a csomagok gyorsabb feldolgozását;
- Az IPv4-nél jobb biztonság (hitelesítés és titkosság) biztosítása;
- Lehetővé tenni, hogy egy számítógép a címének megváltoztatása nélkül barangolhasson a különböző hálózatok között;
- A protokoll fejlődésének biztosítása;
- Az új és a régi protokoll még évekig való egymás mellett létezésének lehetővé tétele.

Hosszú megbeszélések és viták után az IETF kiválasztott egyet a számos, következő IP verzióra vonatkozó javaslat közül, és az IPv6 elnevezést adta neki (az IPv5 már használatban volt egy kísérleti kutatási folyamprotokoll megnevezésére).

Az IPv6 egészen jól megfelel a kitűzött céloknak. Megtartja az IPv4 jó tulajdonságait, elveti vagy kevésbé hangsúlyossá teszi a rosszakat, és újakat is hozzáad, ahol szükség van rá. Azonban fontos megemlítenünk, hogy az IPv6 nem kompatíbilis az IPv4-gyel.

A legfontosabb előrelépés, hogy az IPv6 hosszabb címeket használ, mint az IPv4, és ezáltal a címtartomány kiterjedése is lényegesen nagyobb. A címek mérete 128 bit, amely megoldást nyújt az IPv4 címtartomány kimerülésének problémájára egy gyakorlatilag végtelen méretű Internet címtartománnyal. 128 bittel 2^{128} hosztot címezhetünk meg a hálózatban, ami hozzávetőleg $3x10^{38}$. Ez egy igen nagy szám! Ha az egész Föld felülete, beleértve a szárazföldet és a vízfelszínt is, számítógépekkel lenne befedve, az IPv6 $7x10^{23}$ IP címet tenne lehetővé négyzetméterenként.

Azonban a hosszú IP címek használatának van egy hátulütője: Hogyan tudják a rendszeradminisztrátorok ezeket a címeket hatékonyan ábrázolni és kezelni? Ezen probléma megoldására a következő jelölésrendszer lett bevezetve: a 16 bájtos címeket nyolc, egyenként négy hexadecimális számjegyből álló csoportként írjuk le a csoportok között kettősponttal, mint például

0000:0000:0000:0000:1234:5678:9ABC:DEFF.

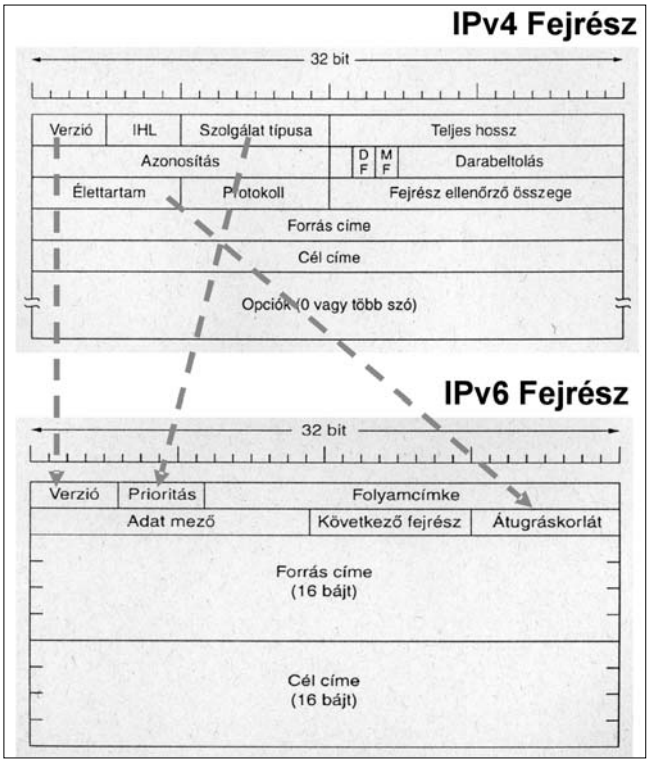
Mivel számos cím sok nullát fog tartalmazni, ezért három egyszerűsítés alkalmazható. Először is, egy csoporton belül a bevezető nullák elhagyhatók, így a 0345 345-nek írható. Másodszor, egy vagy több 16 nullából álló csoport két kettősponttal helyettesíthető. Így az előző példa a következő rövidebb formában írható:

::1234:5678:9ABC:DEFF.

És végül, az IPv4 címek két kettőspont, és a régi, pontokkal elválasztott decimális szám formájában írhatók le, például:

::129.132.66.157.

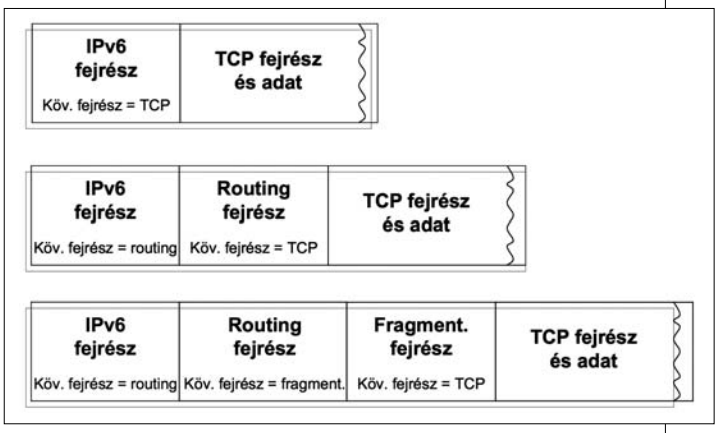
1. ábra Az IPv4 és IPv6 fejrész összehasonlítása



5 Az IETF egy nemzetközi szervezet, amely az Internettel kapcsolatos technológiák szabványosításáért felelős

Egy másik határozott előrelépés IPv6 használata esetén az IP fejrész jelentős egyszerűsödése. Ahogy azt már korábban említettük, minden egyes adatcsomagnak tartalmaznia kell bizonyos információt, hogy az útvonalválasztó csomópontok képesek legyenek a csomagok helyes irányba történő továbbítására. Ez az információ az IP fejrészben található. IPv6 esetén az IP fejrész mindössze 8 mezőből áll, ellentétben az IPv4 14 mezőjével. Ez az egyszerűsítés lehetővé teszi az útvonalválasztó csomópontok számára a beérkező adatcsomagok gyorsabb feldolgozását, így több adat átbocsátását, ezáltal növelve az útvonalválasztó kapacitását és hatékonyságát.

Az előző oldali *1. ábrán* látható a két különböző IP verzió által használt protokoll fejrész, és a kapcsolat bizonyos mezők között, amelyeket többé-kevésbé átvett az IPv6 az IPv4-től. Egy érdekes dolog az úgynevezett *következő fejrész (next header)* mező használata. Ez az oka annak, amiért az IPv6 fejrész egyszerűsödhetett, hiszen ennek segítségével az IP fejrész szükség esetén kiterjeszthető további (opcionális) mezőkkel. A 'következő fejrész' mező határozza meg, hogy melyik fejrész következik a (jelenleg) 6 kiegészítő fejrész közül. Az utolsó fejrész esetén pedig ez a mező azt mondja meg, melyik transzport protokoll kezelőjének, például TCP, kell a csomagot továbbítani. A *2. ábra* szemlélteti eme mechanizmus működését egy példával illusztrálva a fejrész kiterjesztések láncolt használatát.



2. ábra Láncolt fejrész kiterjesztések

Az IPv6 előrelépést jelent biztonság tekintetében is. A biztonságos adatátvitel szerves része az IPv6-nak, ellentétben az IPv4 esetén használt utólagos kiterjesztésekkel. A biztonságos adatátvitel magában foglalja az IP szinten történő adathitelesítést és adattitkosítást. A hitelesítés segítségével az adatcsomag címzettje biztos lehet abban, hogy a csomagot valóban a feladója küldte, és a csomag nem változott meg a továbbítás során. A titkosítás biztosítja, hogy csak az a vevő tudja elolvasni a csomagot, akinek azt valójában szántuk. Azonban még az IPv6 sem kínál megoldást hozzáférési jogosultságok kezelésére, azaz annak eldöntésére, hogy a felhasználónak a sikeres azonosítás után vajon van-e jogosultsága az erőforrások használatához. Ez továbbra is alkalmazás-szintű törődést igényel. Az említett biztonsági megoldások implementálása egy titkos kulcsrendszer segítségével történik az IPv6-ban, azaz a küldő és fogadó állomásnak meg kell állapodnia egy vagy több titkos kulcsban – ami tulajdonképpen egy kód –, melye(ke)t csak ők ismernek, és ezen kulcs(ok) használatával történik később az adatcsomagok hitelesítése és titkosítása. Továbbá, a küldő és fogadó állomásnak egy biztonsági viszonyt kell kialakítania egymással. Ez a viszony tartalmazza a kulcsot, a hitelesítés és/vagy titkosítás algoritmusát, illetve egyéb paramétereket, mint például a kulcs érvényességi idejét.

A gyakorlatban a hitelesítés a *hitelesítő fejrész (authentication header)* – amely egy IPv6 kiegészítő fejrész – segítségével történik. A hitelesített adat – az adatcsomag feladójának címét és néhány más IP fejrész mezőt, mint bemeneti információt felhasználva – egy matematikai algoritmus alkalmazásával kerül előállításra, és az eredeti adatcsomaghoz csatolva kerül továbbításra. Az alkalmazott algoritmus az úgynevezett *kulcsolt MD5 (keyed MD5 – Message Digest 5)*, amelyet rendkívül nehéz visszafejteni és amely ezáltal biztosítja, hogy az adatcsomag sértetlen és a valódi feladójától ered. A hitelesítő fejrész azonban nem titkosítja magát az adatcsomagot. Erre a *titkosított biztonsági adatmező fejrész (encrypted security payload header)* használandó. Titkosítás használata esetén ennek a kiegészítő fejrésznek kell következnie rögtön az alapvető IPv6 fejrész után, hiszen csak így lehet biztosítani mind a hitelesítési információ, mind pedig az adatmező titkosítását. A titkosításhoz használt alapértelmezés szerinti eljárás a *CBC (Cipher Block Chaining – titkosított blokkok láncolata)*, amely a DES (Data Encryption Standard) titkosítási szabványra épül.

A szolgáltatás minőségére (Quality of Service) vonatkozó kérdések tekintetében is előrelépést jelent az IPv6. Az IPv6 fejrész *prioritás (priority)* mezője (1. ábra) használatos azon csomagok közötti különbségtételre, amelyeknek a feladója képes forgalomszabályozásra, és amelyeknek nem. A 0-7-ig terjedő értékek azon adatkapcsolatokat jelölik – mint például honlapletöltés –, amelyek képesek torlódás esetén az átviteli sebesség csökkentésére. A 8-15-ig terjedő értékek az olyan valós idejű kapcsolatokhoz tartoznak, amelyeknek a küldési sebessége állandó és kicsi a késleltetés és késleltetés ingadozás az egyes csomagok között. Például hang és mozgókép átvitel tartozik ebbe a kategóriába. Ez a megkülönböztetés lehetővé teszi az útvonalválasztók számára, hogy a csomagokat hatékonyabban tudják kezelni torlódás esetén.

A *folyamcímke (flow label)* mező (1. ábra) még mindig kísérleti stádiumban van, de arra lehet majd használni, hogy a forrás- és célállomás létrehozhasson egy virtuális összeköttetést bizonyos igényekkel és tulajdonságokkal. Az így létrehozott adatfolyamot előre fel lehet állítani a hálózatban. Minden folyamot egyedileg lehet azonosítani a forrás-, célcím és a folyamcímke által, így több folyam is lehet aktív egyidejűleg két csomópont között.

Amikor egy nem nulla folyamcímkéjű csomag jelenik meg egy útvonalválasztónál, az útvonalválasztó ki tudja keresni a belső táblázataiból, hogy a csomag milyen különleges bánásmódot igényel. Azonban a folyam szintű szolgáltatás minőségre vonatkozó eljárásoknak közismert skálázhatósági problémái vannak nagy hálózatokban, amely gondot okozhat az IPv6 folyamkezelés esetében is.

És végül, az IPv6 alapvető mobilitás támogatása – azaz annak lehetővé tétele, hogy a mozgó hosztok helyváltoztatásuk ellenére is az Internethez kapcsolódva maradhassanak – is egy újabb, jelentős előrelépés. Az IPv6 támogatja az IP címek automatikus konfigurációját mind állapot-követéses, mind állapotmentes módon.

Az állapot-követéses automatikus konfiguráció a DHCP (Dynamic Host Configuration Protocol – dinamikus hoszt konfigurációs protokoll) használatán alapul, akárcsak az IPv4 esetén, amely megköveteli DHCP szerverek telepítését és menedzselését a hálózatban. Az állapotmentes automatikus konfiguráció esetén nincs szükség ilyen szerverekre. Ebben az esetben a hoszt saját maga állítja elő az IPv6 címét a MAC (Medium Access Control – közeg hozzáférési kontroll)[6] címének és az úgynevezett *alhálózati prefixnek (subnet prefix)*[7] a felhasználásával. A *szomszéd felderítési (neighbor discovery)* eljárások is tovább lettek fejlesztve az IPv6-ban.

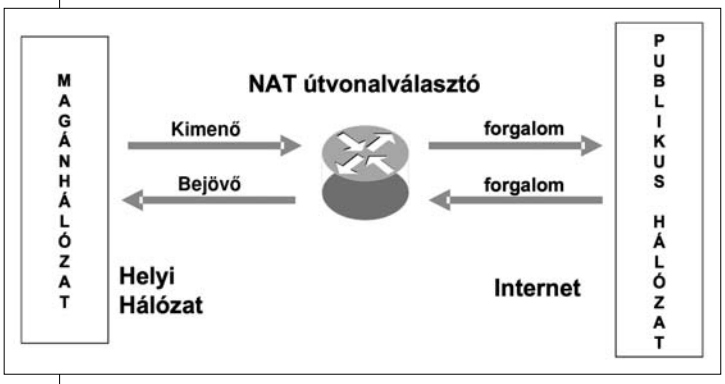
Az összes olyan mechanizmus, amely az azonos hálózati szegmenshez csatlakozó hosztok és útvonalválasztók közötti interakcióval kapcsolatos, az IPv6 esetén egyetlen protokollba, mégpedig az ND (Neighbor Discovery – szomszéd felderítés) protokollba lett összevonva. Az ND felváltja az IPv4 által használt ARP (Address Resolution Protocol – cím feloldási protokoll), ICMP (Internet Control Message Protocol – Internet kontroll üzenet protokoll), RD (Router Discovery – útvonalválasztó felderítés) protokollokat, valamint további fejlesztéseket is tartalmaz. Ezen tulajdonságok elősegítik a mobil IP[8] használatát IPv6 esetén is.

3. Az IPv6 a megoldás?

Most, hogy áttekintettük az IPv6 által bevezetett újdonságokat, feltehetjük a kérdést: Miért nem terjedt már el világszerte az IPv6, mikor számos előnnyel rendelkezik az IPv4-gyel szemben? Ráadásul az IPv6 lényegi részeinek a szabványosítása már befejeződött és az IPv6 Fórum[9] [3] már évek óta támogatja és propagálja az IPv6 rendszeresített használatát.

Nem egyszerű válaszolni erre a kérdésre. Ehhez közelebbről meg kell vizsgálnunk, vajon az IPv6 által bevezetett újdonságok [4,5] valóban lényegi előrelépést jelentenek-e?

A gyakorlatilag kimeríthetetlen IPv6 címtartomány egy lényeges előrelépés. De valóban szükség van erre már manapság illetve a közeljövőben? Úgy tűnik, nem, mert a jelenleg használatban lévő, az IPv4 esetén alkalmazott IP cím-kímélő kiterjesztésekkel, mint például a NAT (Network Address Translation – hálózati címfordítás), és előrelátó címfoglalási stratégiákkal az IPv4 címtartomány még biztosan kitarthat az elkövetkezendő pár év folyamán.



3. ábra NAT

Például, a nyilvános Internet és egy magánhálózat határán elhelyezkedő NAT útvonalválasztó használata estén *(3. ábra)* mindössze pár nyilvános IP címre van szükség (gyakran csak egyre) ahelyett, hogy minden egyes hoszt a magánhálózatban egy külön nyilvános IP címmel rendelkezne. Ebben az esetben a NAT útvonalválasztó lefordítja, azaz kicseréli, a forrás IP címét minden olyan csomagnak, amely elhagyja a magánhálózatot egy, az útvonalválasztó által használható nyilvános IP címtartományból kiválasztott nyilvános IP címre. Ezen felül a NAT útvonalválasztó visszacseréli az Internet felől érkező csomagok cél IP címét a magánhálózatban lévő célállomás által használt magán IP címre. Ezzel a megoldással számos különböző magánhálózat használhatja ugyanazt a magán IP címtartományt a hálózaton belül – mert ezek a címek nem érhetők el a magánhálózaton kívülről, így nem okoznak címütközést –, ami növeli a kioszthatő IP címek számát.

Azonban a NAT használatának is vannak korlátai. Például az olyan alkalmazásoknak, melyeknek egy NAT útvonalválasztón kell áthaladniuk, a magánhálózatból kell kezdeményezniük a logikai adatkapcsolat létrehozását, mivel az Internet felől csak bonyolult eljárásokkal – úgymint alkalmazás szintű DNS (Domain Name System – tartománynév rendszer) átjáróval – lehetséges ez, hiszen az Internet felől a NAT útvonalválasztó túloldalán lévő hálózat nem látható. Továbbá, összefüggő végpont-végpont (end-to-end) szintű csomagtovábbítás és biztonságos átvitel biztosítása is csak egyéb el-

6 A MAC cím általában az egyedi azonosítója az adott gép hálózati interfészének
7 Az alhálózati prefix annak a hálózati szegmensnek az azonosítója, amelyhez a hoszt csatlakozik és amelyet az úgynevezett szomszéd felderítési (neighbor discovery) eljárás segítségével kérdez le az adott szegmenshez csatlakozó útvonalválasztótól
8 A mobil IP egy protokoll szabvány mobilitás kezelésére az Internet hálózatban
9 Az IPv6 Fórum egy világméretű, az Internettel kapcsolatban lévő cégek és kutatási/oktatási hálózatok non-profit konzorciuma, amelynek célja az IPv6 népszerűsítése

járások segítségével lehetséges – mint például úgynevezett *alagút (tunnel)* használatával –, mivel alapesetben a logikai kapcsolatok végpontjai a NAT útvonalválasztóval, és nem közvetlenül egymással kommunikálnak.

Az IPv4 címtartomány kimerülésének tempóját vizsgálva a következőket figyelhetjük meg: 1994 előtt megközelítőleg 36%-a volt a rendelkezésre álló IPv4 címtartománynak kiosztva. Azóta további 20% lett felhasználva [4], és ez az időszak magába foglalja a teljes Internet robbanás időtartamát is! Amennyiben ez a tendencia folytatódik, akkor úgy tűnik, hogy még évekig ki fog tartani az IPv4 címtartomány.

A biztonságos kommunikáció is egyre nagyobb figyelmet igényel manapság. Míg az IPv6 esetén a biztonságos kommunikáció lehetőségét már a protokoll tervezésétől kezdve figyelembe vették, addig ez az IPv4 esetén csak különböző kiegészítésekkel oldható meg, mint például az IPsec használatával, amely egy protokoll gyűjtemény a biztonságos adatcsere lehetővé tételére. De valójában mennyire fontos az, hogy a biztonságos kommunikációt a hálózat implementálja? Egy komoly alkalmazás, amely biztonságos adatátvitelt igényel, saját maga implementálja azt, és nem hagyatkozik a hálózatra, legalábbis manapság még nem.

A szolgáltatás minőség vagy QoS támogatás tekintetében még mindig az úgynevezett *túlkínálat (overprovisioning)* a legegyszerűbb és legolcsóbb megoldás az Internet hálózatban. Ez leegyszerűsítve azt jelenti, hogyha valahol a hálózatban több kapacitásra lenne szükségünk, akkor egy újabb kábel hozzáadása vagy az optikai szálak számának növelése egy összeköttetés mentén gyors és egyszerű megoldást kínál ellentétben bonyolult QoS irányelvek és technikák alkalmazásánál. Továbbá, a korábban említett, IPv6 által támogatott folyamszintű QoS skálázhatósági korlátai még gondot jelenthetnek a jövőben.

És végül, a rohamosan növekvő, az Internethez csatlakozó mobil eszközök számával a mobilitást támogató megoldások egyre jobban előtérbe kerülnek. Az állapotmentes automatikus konfiguráció és a továbbfejlesztett szomszéd felderítési eljárások jelentős segítséget nyújthatnak IPv6 használata esetén. Azonban az IPv6 önmagában nem szolgál teljes megoldással erre a problémára, így néhány további protokoll használatára is szükség van (mint például a mobil IP-re, ellenben a mobil IP képes IPv4-gyel is együttműködni).

4. Áttérés az IPv6-ra?

Ezután a rövid elemzés után úgy tűnik, hogy a fő motivációt az IPv6 világméretű elterjedésére és használatára az a szituáció fogja jelenteni, amikor majdnem minden eszköz a hűtőgéptől a mikrohullámú sütőig az összes mobil eszközünkkel egyetemben az Internethez fog kapcsolódni, és egyedi IP címet fog igényelni. Azonban most még nehéz megjósolni, hogy ez mikor fog bekövetkezni. Természetesen ez nem egyik napról a másikra fog végbemenni az átállás hatalmas terhei (idő, munka, pénz stb.), a szükséges működtetési tapasztalat hiánya és azon rizikó miatt, amelyet egy évtizedek óta működő rendszernek egy olyan rendszerrel való felváltása jelent, amellyel kapcsolatban vajmi kevés tapasztalattal rendelkezünk.

Mindamellett egy idő óta jó néhány kísérleti, sőt már kereskedelmi IPv6 hálózat is működik világszerte. Ebben a tekintetben Ázsia, különösen Japán és Dél-Korea viszi a vezető szerepet, de Európában is jelentős számú, IPv6-tal kapcsolatos kutatási projekt fut.

Svájcban például a SWITCH, a svájci oktatási és kutatási hálózat [6] nyújt IPv6 használata által való kapcsolódási lehetőséget az Internethez, már 1996 novembere óta. 2004 júniusától a SWITCH „SWITCHlambda" nevezetű gerinchálózata IPv4 és IPv6 támogatást nyújt egyidejűleg ugyanazon hálózati elemek használatával. A Swisscom Innovations, amely a központi innovációs részlege a Swisscom nevezetű svájci telekommunikációs cégnek, már jó ideje futtat IPv6 teszt hálózatot, és jelenleg belső Intranet hálózata is alkalmas IPv6 használatára [7].

Az USA is kezdi komolyan fontolóra venni az IPv6-ot. Az amerikai védelmi minisztérium 2003-ban írásba is fektette azon célját, mely szerint a teljes IP hálózatán IPv6-ra kell átállnia 2008-ra [8]. És végül, Magyarországon is lehet IPv6 címtartományt regisztráltatni az NIIF-nél (Nemzeti Információs Infrastruktúra Fejlesztési Program) [9], illetve működő teszthálózatok is találhatók, például a Budapesti Műszaki és Gazdaságtudományi Egyetemen [10] vagy az NIIF gondozásában [9].

Figyelembe véve a jelenlegi tendenciákat úgy tűnik, hogy az IPv6 világméretű elterjedésére 2008-2010-re lehet számolni. Meglátjuk...

Irodalom

[1] IETF – www.ietf.org
[2] A. S. Tanenbaum: Computer Networks, Prentice-Hall Inc., ISBN: 0-13-394248-1, 1996.
[3] IPv6 Forum – www.ipv6forum.com
[4] G. Huston: Waiting for IPv6, in the ISP Column, January 2003, http://ispcolumn.isoc.org/2003-01/Waiting.html
[5] L. Ladid, J. Bound: Response by IPv6 Forum to ISP Column article entitled 'Waiting for IP version 6', http://www.isoc.org/pubs/isp/ipv6response.shtml
[6] SWITCH IPv6 Pilot – www.switch.ch/network/ipv6/
[7] Swisscom Innovations – IPv6 Labs and Services, http://www.swisscom.com/Innovations/content/Labs/IPv6/
[8] DoD IPv6 General Information – http://ipv6.disa.mil/
[9] NIIF/HUNGARNET IPv6 Projekt – http://6net.iif.hu/
[10] BME – http://portal.bme.hu/