Az új generációs Internet alapjai

BENDE ZSÓFIA, CZIGÁNY ÁDÁM, NAGY KRISZTINA, LUKOVSZKI CSABA

Budapesti Műszaki és Gazdaságtudományi Egyetem, Távközlési és Médiainformatikai Tanszék
csaba.lukovszki@tmit.bme.hu

Kulcsszavak: címzés, címtár, mobilitás, biztonság, nemzetközi projektek

Információs társadalmunk egyik alappillére az Internet, melynek működését eddig az Internet Protokoll 4-es verziója szabályozta. Az Internet robbanásszerű elterjedése és az ennek következtében felmerülő új igények azonban szükségessé tették az IPv4 bővítését, fejlesztését. A megoldást egy új verzió jelenti. Cikkünk célja a protokoll 6-os verziójának bemutatása, a megalkotásához vezető igények ismertetése, a létrehozott új szolgáltatások alapjainak felvázolása. Végül, de nem utolsósorban feltárjuk az IPv6 jelenlegi helyzetét, nemzetközi és nemzeti szinten egyaránt.

A következő generációs Internet protokoll, más néven az IPv6 az Internet alapját jelentő 4-es verzió, vagyis az IPv4 (röviden IP) továbbfejlesztése. Az IPv4 1983-ban mutatkozott be és várakozáson felüli sikert tudhat magáénak. Azonban már egy évtizede felmerült az igény az új elvárásoknak is megfelelni képes, továbbfejlesztett verzióra. Néhány évtized múlva valószínűleg már csak internetes múzeumokban találkozhatunk az Internet hőskorát megalapozó 4-es verzióval.

Az első IP megújítását célzó protokollok már a 80-as évek végén megszülettek. Számos javaslat kidolgozása után az IPv6 megalkotásához a protokollokban rejlő újítások egybevetése vezetett. Az IPv6 specifikációk alapjait a 90-es évek elején az Internet számos újítását összehangolva, az Internet Engineering Task Force (IETF) fektette le.

Jelenleg a szakma szerint nincs alternatíva, mely áttörné az Internet fejlődésének gátjait. Az IPv6 térhódítása csupán idő kérdése!

Új igények, változások, újdonságok

Egyre gyakrabban hallunk mutimédia-tartalom továbbításról, biztonságos virtuális magánhálózatokról, mobil irodáról. A felmerült igények kielégítésére az IPv4-et is alkalmassá tették, viszont nagy előny, hogy az IPv6 ezeket szabvány szinten teszi lehetővé. További szempontként említhetjük új szolgáltatások hatékony bevezetésének lehetőségét is. Például többesküldés (lásd később) segítségével hatékonyan küldhet szét egy cég kizárólag az alkalmazottai számára üzeneteket, vagy juttathat el multimédiás csomagokat előfizetői számára.

A meglévő alkalmazások (például videokonferencia, webrádió) elterjedését is elősegítik az IPv6-ban alkalmazott szolgáltatások. Az üzleti területeken kívül a kutatási területeken is előrelépést jelent az IPv6, gondoljunk az elosztott hálózatokra vagy a GRID technológiára.

Az IPv4 évtizedes használata nemcsak új igények megjelenését eredményezte, de megtapasztalhattuk, hogy az egyes IP-ben megvalósított funkciók elhagyhatóak. Így kimaradt az IPv6 fejrészéből az ellenőrző összeg, melynek funkcióját magasabb rétegek veszik át. Ugyanígy kimaradtak a tördeléssel összefüggő mezők, a csomagméretről az IPv6-ot használó végpontoknak kell megegyezniük.

Összességében elmondható, hogy a célok között szerepel a végpontok közötti Internet paradigmájának visszaállítása. Így a peer-to-peer alkalmazások, vagy a végpontok közötti biztonsági megoldások és a címfordítók mellőzése mind az alapkoncepció részét képezik.

A címtér korlátainak ledöntése

Jelenleg a Föld lakosságának körülbelül 10%-a rendelkezik Internet eléréssel. Amennyiben célul tűzzük ki ezen arány növelését és figyelembe vesszük a népesség-növekedést, továbbá az önálló címmel rendelkező eszközök térhódítását, akkor világossá válik, hogy a jelenlegi IP cím mennyiség kevés. Az IPv4-es rendszerben problémát okoz az osztály alapú címzés, mely az egyes címtartományok allokációját csak meghatározott kvantumokban teszi lehetővé. A kiosztás elvi helytelensége miatt ez egy meglehetősen rossz választás volt.

A címtér szűkösségének problémája az Egyesült Államokban kevésbé jelentős, így az IPv6 elterjedése a világ többi részén (pl. Ázsiában, Kínában) hamarabb várható. Ezt könnyen megérthetjük, ha figyelembe vesszük, hogy például Kína 1,3 milliárd lakosa ellenére mindössze 22 millió IPv4-es címmel rendelkezik. A felhasználók száma mára már megközelíti ezt az értéket, viszont 2007-re 62,5 millió előfizetőt jósolnak. Japánban és Koreában is hasonló a helyzet, ezért ezek a kormányok óriási pénzeket költenek az IPv6 bevezetésére. Az IPv4-es címek 70%-a az Egyesült Államokhoz tartozik.

Napjainkban a kevés cím problémáját dinamikus címkiosztással is próbálják orvosolni, vagyis egy hálózatra feljelentkező gép nem minden esetben ugyanazt a cí-

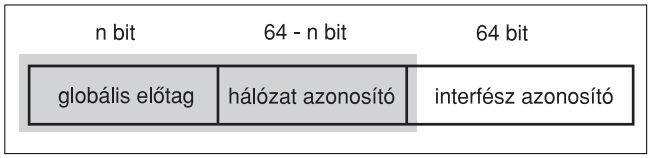
met kapja meg. A címek rendezetlensége miatt egy forgalomirányítónak akár több százezer bejegyzést is tárolni kell, ami nagyobb hardverkövetelményt támaszt az útvonalválasztókkal szemben. Erre nyújt megoldást a hierarchikus címkiosztás.

Az IPv6-os címek

Az IP címek kiosztása delegációs rendszerben történik, melynek legfőbb szerve az IANA (Internet Assigned Numbers Authority). A négy területi regisztrátor szervezet közül Európában a RIPE NCC (Réseaux IP Européens Network Coordination Centre) látja el ezt a feladatot. Ennek a tagjai többnyire Internet-szolgáltatók, illetve a szolgáltatók és regionális szervezet közé beékelődő nemzeti regisztrátorok is. Ezen a láncon keresztül kaphat bármely felhasználó IP címet, vagyis csatlakozási pontot a világ legnagyobb hálózatához. Az IPv6 egyik legjelentősebb újítása a 128 bites címek bevezetése. Ez sok nagyságrendnyi változást jelent az IPv4 által szolgáltatott 32 bites címtartományhoz képest.

Az IPv6 háromféle címzési módot különböztet meg. Egyesküldés (unicast) esetén egyetlen interfész a címzett. Többesküldés (multicast) esetén a címhez tartozó összes interfészhez megérkezik a csomag. Lehetséges, hogy egy címhez tartozó csoport tagjai közül csak valamilyen metrika szerinti legközelebbi interfész kapja meg a csomagot, ekkor használjuk a legközelebbinek való küldést (anycast). Az IPv4-ből jól ismert üzenetszórás az IPv6-ból teljesen kimaradt, helyét a többesküldés veszi át, melyhez számos előre definiált csoportot specifikáltak. [1]

A cím felépítése jól láthatóan hierarchikus *(1. ábra)*.



1. ábra IPv6 címek felépítése

Az *interfész azonosító* feladata, hogy egy IPv6-os kapcsolódási pontot azonosítson az adott hálózatban. Ezt legtöbbször a második rétegbeli hozzáférési közeg címének (pl. Ethernet hálózat esetén a MAC cím) segítségével történik. A MAC cím egyedisége elvileg garantált, gyakorlatilag több gyártó is figyelmen kívül hagyta ezt.

A középső, jelen esetben 16 bitnyi címrész azonosítja az adott hálózatot (SLA, Site Level Aggregation).

A korábbiakban említett címtípusok megkülönböztetésére és a hálózat megadására használjuk a globális előtagot. Ezt a hierarchikus kiosztás és feldolgozás miatt partícionálták. A korábban elfogadott ajánlás szerint az első 3 címtípus bitet (001) követő 13 bit tartozik a legmagasabb szintű szétosztáshoz (TLA, Top-Level Aggregation), melyet globálisan az IANA végez, így minden TLA egy-egy térséget azonosít. Ez a publikus gerinchálózatok szintje. Adott térségben lévő nagy szolgáltatók, vagy nemzeteknek a címek tovább oszthatóak (NLA, Next Level Aggregation), erre a célra a következő 32 bit használható.

Ez a megoldás magában hordozza a strukturált és átlátható címkiosztás lehetőségét, viszont mivel nem látható pontosan előre, hogy a különböző szinteken valójában mekkora tartományokat kell kijelölni a leghatékonyabb lefedéséhez, a kiosztás nagyon pazarlóvá válhat, ám a 128 bitnyi teljes hosszból eredő variációk száma így is igen nagy.

Az egyesküldési címeken belül megkülönböztetünk globálisan, adminisztrációs tartományra értelmezett és linken egyedi címeket. Míg a globálisan értelmezett címek egyedileg azonosítanak egy hosztot az Interneten, addig a adminisztrációs tartományra értelmezett címek egyazon tartományon belüli címzésre használhatóak globális előtag igénye nélkül. A linken egyedi címek csak adott linken belül érvényesek. Elsősorban autokonfigurációs és szomszédság felderítési célokat szolgálnak.

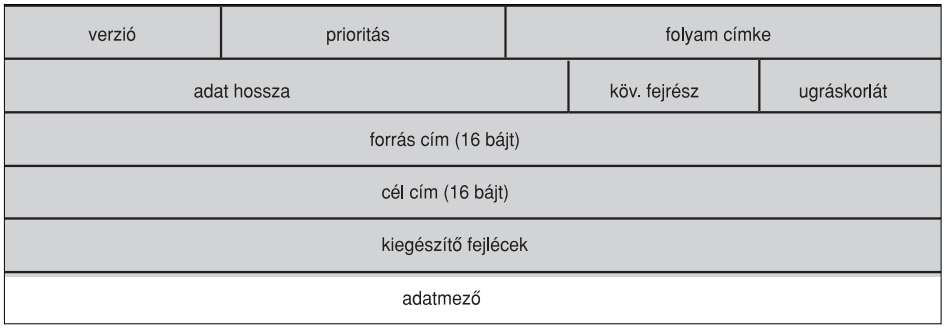
Az IPv6 datagram felépítése

Az IPv6-os címzés ismertetése után térjünk át az IPv6 gyakorlati alkalmazásaira, különös tekintettel az újdonságokra, ezek közül is elsőként az Internet Protokoll egyik alappillérét jelentő szállítási egység vizsgálatára, az IPv6 adatcsomagra.

Az IPv6 alap fejléce fix hosszúságú (ellentétben az IPv4-gyel) és ehhez kapcsolódhatnak még opcionálisan kiegészítő fejrészek. Így az útvonalválasztók számára a feldolgozás egyszerűbbé és gyorsabbá válik.

Minden, az IPv6 alapvető kapcsolatfelépítéshez szükséges adat szerepel *(2. ábra)* a fejlécben úgy, mint a forrás és cél azonosítását szolgáló címmezők, a folyamot meghatározó mező, az adatmező hossza és az ugráskorlát, mellyel a csomag élettartamát lehet szabályozni. Az ezeken felüli opcionális funkciókat a kiegészítő fejlécekben tárolták.

2. ábra
Az IPv6 datagram felépítése



Mobilitás

A 21. század informatikai igényeiben az elsők között szerepel a mobilitás. Ezt a tendenciát az IP világnak is figyelembe kell venni és a most létrejövő piacképes rendszereknek mindenképpen illeszkedniük kell ehhez. Nem meglepő tehát, hogy már az IP 4-es verziójánál is foglalkoztak a témával. Felmerült azonban egy jelentős probléma, amely alapjában véget vethetett volna a mobil IP történetének. Ugyanis ha egy hoszt IP címe megváltozik, akkor ez együtt jár azzal, hogy a felsőbb rétegbeli alkalmazások, melyek eddig ezt az címet használták azonosítóként, megszakadnak[8].

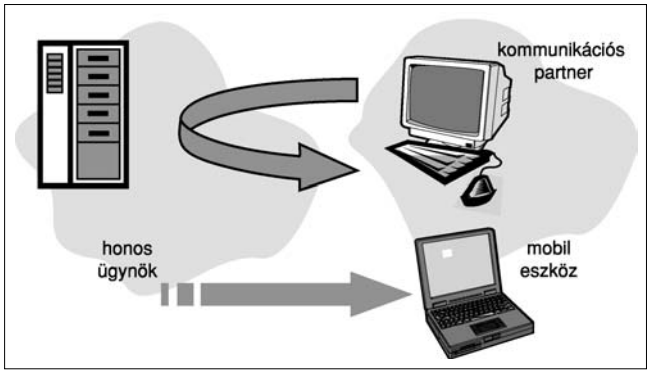
Mindezeket figyelembe véve dolgozták ki a Mobil IPv6-ot [3]. Az eddig kidolgozott protokollok alapján a mobil hoszt számára lehetővé válik az egyes hozzáférési pontok közötti mozgás úgy, hogy közben a hozzá más hozzáférési pontokról érkező csomagokat is megkapja. Ezt a mechanizmust az IP és a rajta működő protokollok az alkalmazások elől elrejtik. Itt már nincs szükség idegen ügynökökre, és nem igényel külön támogatást az aktuális helyi útválasztótól sem. De talán a legjelentősebb eltérés az útvonal optimalizálás bevezetése.

A mobil IP megvalósításának alapötlete igen egyszerű. A hoszt kétféle IPv6-os címmel rendelkezik. Az egyik, az úgynevezett honos cím, amely a honos hálózatbeli állandó cím. Amikor egy másik hozzáférési pontra kapcsolódik, azon egy felügyeleti cím fogja azonosítani. Ez utóbbiból akár több is lehet, de mindig ki kell jelölni az elsődlegest közülük. Ezt a mozgás szerint változó címet a mobil hoszt mindig ismerteti a honos hálózatával, amelyben az aktuális összerendeléseket a honos ügynök tárolja. Ez végzi a távol lévő hoszthoz beérkező csomagok továbbítását is, amennyiben az a honos címre érkezett.

A mobil hoszt természetesen közölheti aktuális IP címét a kommunikációs partnerével. A továbbiakban a kapcsolatfelépítés bemutatása következik, amelynek kétféle módja is van.

Egyik lehetséges megvalósítás, amikor a mobil hoszt nem közli aktuális címét partnerével, így a csomagok először a honos ügynökhöz kerülnek, majd innen jutnak el a másik félhez és vissza *(3. ábra)*. Ez a megoldás, melyet kétirányú alagutazásnak is neveznek, nem igényel külön IPv6 támogatást.

3. ábra Kétirányú alagút használata



Az útvonal optimalizálásnál *(4. ábra)* már szükség van az aktuális címre. Első lépésben a mobil csomópont ismerteti az aktuális cím-összerendelést, így ezután már közvetlenül küldhetők a csomagok a két végpont között, nincs szükség a honos ügynök közreműködésére.

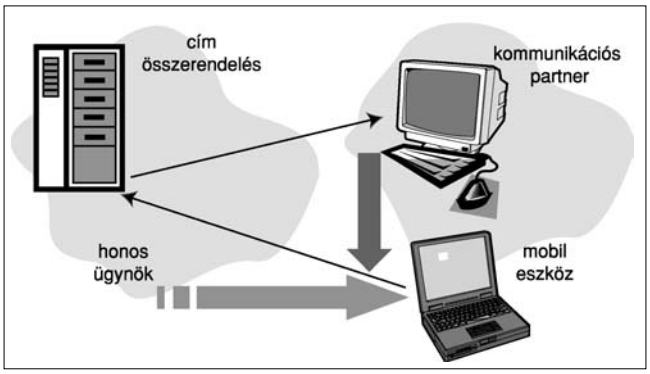
Biztonság

Az Internet gyors növekedésének és elterjedésének eredményeképpen az egyik legfontosabb megoldandó feladattá vált a biztonság problémája. Jelentőségét nem lehet és nem is szabad kétségbe vonni vagy lebecsülni, mára szinte elsődleges kérdéssé vált. A biztonság fogalma alá tartozó szolgáltatások sokfélék lehetnek.

Érdemes néhány szót szentelni a legfontosabb biztonsági követelményeknek. A köztudatban biztonság alatt gyakran a *titkosságot* értik, vagyis annak biztosítását, hogy a címzetten kívül más ne tudja értelmezni az elküldött információt. De természetesen nem ez az egyedüli követelmény és elmondható az is, hogy talán nem is minden esetben a legfontosabb. A titkossághoz talán legközelebb áll az *integritásvédelem*, amely biztosítja, hogy ne változtathassák meg illetéktelenek az elküldött csomag tartalmát. A *hitelesítés*, mely számos internetes biztonsági kérdést megold, célja annak ellenőrzése, hogy az összeköttetésben résztvevő felek valóban azok, akiknek mondják magukat. Végül a *visszajátszás elleni védelem* foglalkozik azzal a problémával, hogy egy csomagot ne lehessen a későbbiekben újra felhasználni.

Az Internet Protokoll 4-es verziója nem volt ezekre megfelelően felkészítve, a biztonsági kérdéseket főként alkalmazás szinten valósították meg, ami azt vonta maga után, hogy egyes funkciókat több alkalmazásba is beépítették. A probléma megoldására alkották meg az IP Security [24] protokollt, ami hálózati rétegbeli biztonságot nyújtott. Az IPv6 újat nyújtott abból a szempontból is, hogy olyan alapszintű biztonsági követelmények, mint a fejléc hitelesítése, a protokoll kötelezően megvalósítandó részei lettek. Ez nem azt jelenti, hogy a kommunikációnak ezután csakis és kizárólag hitelesítve és titkosan kell végbemennie, hanem csupán annyit rögzít, hogy az IPv6-ot megvalósító hosztoknak kötelezően rendelkezésre állnak a hitelesítést és titkosítást végző algoritmusok.

4. ábra Útvonal optimalizálás címösszerendeléssel



A protokoll rugalmas, többféle üzemmóddal is rendelkezik. A kívánt biztonsági szolgáltatások két kiegészítő fejrész segítségével valósíthatók meg [5]. A Hitelesítési fejrész az adatok hitelesítési és integritásvédelmi funkcióit látja el, az elküldött adatok titkosításáért pedig a Beágyazott Biztonsági fejrész felel .

Automatikus konfiguráció

Az Internet Protokoll 6-os verziójának újabb jelentős eredménye az automatikus konfiguráció. Ez képessé teszi a hosztokat arra, hogy saját maguk hozhassanak létre egy lokális címet azon az alhálózaton, amelyre éppen kapcsolódtak. Ezzel érthető módon a hálózati adminisztrációs feladatok is jelentősen lecsökkenthetők. Szolgáltatói oldalról lehetővé válik a hálózathoz tartozó hosztok címeinek egyszerű és gyors cseréje. Az automatikus konfigurációnak két változata van .

Az *állapotmentes automatikus konfiguráció* esetén a hoszt saját maga allokál egy címet [9]. Ennek egy lehetséges módját az IPv6-os cím ismertetése során már bemutattuk. Mielőtt azonban a címet használhatná, szükség van annak ellenőrzésére, hogy egyedi-e. Ezt a metódust nevezik duplikált címdetektálásnak (DAD).

A másik megoldásban rendelkezésre áll egy kitüntetett szerver, például a DHCP (Dinamikus Hoszt Konfigurációs Protokoll) szerver, amely közreműködik a hoszt konfigurációjában, így biztosítva, hogy ugyanaz a hoszt minden esetben ugyanazt a címet kapja a hálózattól. Ekkor *állapot alapú automatikus konfigurációról* beszélünk [10].

Nem lehet azonban figyelmen kívül hagyni, hogy az autokonfiguráció összességében időigényes művelet. Így mobil környezetben nem előnyös a címek duplikálásának vizsgálata. Ennek gyors és egyszerű megoldása, majd annak szabványosítása még várat magára.

Nemzetközi és nemzeti törekvések

Az Internet Protokoll 6-os verziója mára már szinte az egész világon elfogadottá vált és nem egy térségben figyelhetjük meg, hogy az Interneten kialakuló mind nagyobb verseny miként mozdítja elő az IPv6 regionális telepítését, a szolgáltatások alkalmazásának vizsgálatát, valamint a protokoll felhasználási lehetőségeinek folyamatos kutatását. Számos különböző projektet hoztak létre más és más célkitűzésekkel, azonban mégis elmondhatjuk mindegyik egy cél köré csoportosult: elősegíteni az IPv6 széleskörű alkalmazását.

Az *IPv6 Task Force* legfőbb feladata az IPv6 továbbfejlesztése. Ez egy világméretű összefogás, több regionális központtal, melyek Európában, Észak-Amerikában, Brazíliában, Kínában, Japánban, Dél-Koreában, Indiában és Iránban találhatóak. Tényleges eredményként könyvelhetjük el a *6BONE*-t [13], amely egy nemzetközi, kísérleti, virtuális számítógép hálózat. A 6BONE nem egy külön, e célra létrehozott infrastruktúrán üzemel, hanem egy IPv4 alapú Internet hálózaton alakították ki az adatátviteli csatornáit. A 6BONE kitűnő eszköznek bizonyult az IPv6 új útvonal választási stratégiáinak és algoritmusainak kipróbálására és az IPv6 szoftverek és berendezések ellenőrzésére. Mivel mára az IPv6 megérett a használatra, a 6BONE teszthálózatot és az összerendelt cím allokációkat fokozatosan megszüntetik.

Az 1990-es évek vége felé, és az új évezred elején számos kezdeményezés, projekt indult útjára, melyek közül már több be is fejeződött. Ilyen például a *6WINIT* projekt [14], melynek segítségével bevezetésre került az új vezeték nélküli mobil Internet Európában. Egy másik projekt, a *6INIT* [15] olyan technológiákat valósított meg, mellyel felügyelni lehet az információ feldolgozást, továbbá olyan technológiákat, melyek segítik a kommunikációt, a szélessávú hozzáférést, ezek együttműködését is beleértve.

Európa

Európa egyre inkább arra törekszik, hogy egységet alkosson nemcsak az államigazgatás és a gazdaság, hanem a technológiai fejlődés területén is. Az európai országok számára az IPv6 használatának egységes kidolgozása, az Internet piaci verseny mellett, a felzárkózást is biztosítja az információs sztráda alkalmazásában élen járó Amerikához és Ázsiához. Az Európai Unió ennek támogatására hozta létre az európai IST (Information Society Technologies) szervezetet. Mindezek előkövetelménye az egységes szolgáltatási alap megteremtése, melyet napjainkban is számos pilot projekt támogat.

Az egyik legismertebb a *6NET* [16], amely egy három éves EU projekt. Feladatai többek között egy nemzetközi IPv6 pilot hálózat telepítése és működtetése fix és mobil komponensekkel annak érdekében, hogy elfogadtassa az IPv6 fejlesztés eredményeit; migrációs stratégiák tesztelése; új IPv6 szolgáltatások, alkalmazások bevezetése, vizsgálata; címkiosztás értékelése stb. Magyar vonatkozása a dolognak, hogy 2002 óta a 6NET partnere a később bemutatatott HUNGARNET is.

Az *Euro6IX* [17] a mai napig a legnagyobb kutatás, melyet az európai IST indított el. Célja, hogy megtervezze és telepítse az első pán-európai nem kereskedelmi IPv6 hálózatot; ezen az infrastruktúrán IPv6-alapú alkalmazásokat, szolgáltatásokat fejlesszen és teszteljen; elérhetővé tegye a hálózatot egy speciális felhasználói csoport számára tesztelés céljából; elterjessze, összeköttetést és koordinációt biztosítson standard szervezetek (például IETF, RIPE) számára. Nagy jelentőségű egy hálózati szigetek összeköttetésére szolgáló gerinchálózati IPv6 létrehozása, melyet a *GÉANT* [18] projekt valósít meg, amely ezen felül még útvonalválasztással is foglalkozik.

Magyarország

Ugyanezen trendeket figyelhetjük meg hazánkban is. A NIIF [19] (Nemzeti Információs Infrastruktúra Fejlesztési Program) a magyarországi kutatói hálózat fejlesztésének és működésének programja. A program a teljes magyarországi kutatási, felsőoktatási és közgyűj-

teményi közösség számára biztosít integrált országos számítógép-hálózati infrastruktúrát, valamint erre épülő szolgáltatásokat, élvonalbeli alkalmazási környezetet, valamint tartalom-generálási, és tartalom-elérési hátteret. A NIIF IP gerinchálózatát HBONE-nak nevezzük. A HBONE a hazai akadémiai közösség számítógép hálózata. Az IPv6 elterjedéséből származó változások Magyarországot sem kerülték el.

A NIIF IPv6 törekvéseinek mérföldköveiből:
– az NIIF 6NET partnerré vált (2002. szeptember),
– IPv6 hálózat működik (2002. decembere óta),
– HUNGARNET IPv6 címkiosztás elindulása (2002. szeptember),
– natív IPv6 kapcsolat épült ki Bécsbe,
– GÉANT IPv6 pilot szolgáltatáshoz kapcsolódtunk.

A hazai eredmények közé tartozik többek között a hálózat menedzsment létrehozása, a teljesítmény mérése és az alkalmazási kísérletek.

A jelenlegi szolgáltatások közül említésre méltó a NIIF IPv6 címallokációs és regisztrációs szolgáltatása. Az NIIF IPv6 cím allokációs és regisztrálási jogokkal rendelkezik az NIIF/HUNGARNET tagintézmények számára. Ennek keretében vállalja, hogy azon tagintézményei számára, akiknek ilyen szolgáltatásra szükségük van, másodlagos, vagy akár elsődleges és másodlagos reverse IPv6 DNS szervert üzemeltet.

A jövő

Végezetül nézzük meg, milyen események, előrelépések várhatóak a közeljövőben. 2004. októberében Mandelieu-ben, Franciaországban rendezik meg az ötödik ETSI IPv6 „Plugtest” találkozót. Szintén a 2004-es évben kerültek, illetve kerülnek sorra Malajziában, Kínában, Németországban, Svájcban, Észak-Amerikában és Koreában az IPv6-os események folytatását alakító csúcstalálkozók.

Összefoglalva a leírtakat kijelenthetjük, hogy az Internet hatos számot viselő protokollja nem csupán egy újabb ígéretes, de a várakozásokat soha be nem váltó kutatási terv, hanem az elkövetkező évtizedek Információs Szupersztrádáját alapvetően meghatározó fejlesztés. Beszéljünk akár Információs Társadalomról vagy a fejlődő térségek felzárkóztatásáról, a mobilitás térhódításáról vagy új generációs hálózatbiztonsági megoldásokról, mindezek mögött az IPv6-ot fogjuk találni.

Irodalom

[1] IPv6 Cluster, „Moving IPv6 in Europe”, Edition of the 6Link European IPv6 Research and Develpoment Series, May 2003, www.ist-ipv6.org/pdf/ISTClusterBooklet2003.pdf

[2] „IP Address Services”, Internet Assigned Numbers Authority, www.iana.org/ipaddress/ip-addresses.htm

[3] R. Hinden, S. Deering, “IP Version 6 Addressing Architecture”. Request For Comments: 3513, IETF Network Working Group, April 2003

[4] R. Hinden, S. Deering, „Internet Protocol, Version 6 (IPv6) Specification”, Request For Comments: 2460, IETF Network Working Group, December 1998

[5] S. Kent, R. Atkinson, „Security Architecture for the Internet Protocol”, Request For Comments 2401, IETF Network Working Group, November 1998

[6] T. Aura, J. Arkko, “MIPv6 BU Attacks and Defenses” Internet Draft, IETF Mobile IP Working Group, February 2002

[7] D. Johnson, C. Perkins, J. Arkko, „Mobility Support in IPv6” Internet Draft, IETF Mobile IP Working Group, June 30,2003

[8] „IPv6 Stateless Address Autoconfiguration”, Request For Comments 2462, Network Working Group, December 1998

[9] R. Droms, J. Bound, B. Volz, B. Volz, T. Lemon, C. Perkins, M. Carney, „Dynamic Host Configuration Protocol for IPv6 (DHCPv6)”, Request For Comments 3315, IETF Network Working Group, July 2003

[10] Silvano Gai, “Internetworking IPv6 with CISCO routers”, McGraw Hill Text, March 27, 1998

[11] Information Society Technologies honlapja: www.cordis.lu/ist/

[12] IPv6 Task Force honlapja: www.ipv6tf.org/europe.php

[13] 6BONE honlapja: www.6bone.net/

[14] 6WINIT honlapja: www.6winit.org/

[15] 6INIT honlapja: www.6init.org

[16] 6NET honlapja: www.6net.org/

[17] Euro6IX honlapja: www.euro6ix.org/

[18] GÉANT honlapja: www.join.uni-muenster.de/geantv6/

[19] NIIF honlapja: www.iif.hu/

[20] 6LINK honlapja: www.6link.org/

[21] 6POWER honlapja: www.6power.org/

[22] IPv6 Forum: www.ipv6forum.com/

[23] Mohácsi János, Szigeti Szabolcs, Máray Tamás, “Az IPv6 hálózati protokollok”, http://tracy.ipv6.fsz.bme.hu/mydocs/networkshop97/

[24] J. Arkko, V. Devarapalli, F. Dupont, “Using IPsec to Protect Mobile IPv6 Signaling between Mobile Nodes and Home Agents”, IETF Network Working Group, June 2003