IPv6 a szolgáltatói hálózatokban: szélessávú elérés

VARGA BALÁZS, BARTA PÉTER, GAÁL GÉZA, HONVÁRI ISTVÁN

Magyar Telekom – PKI
varga.balazs@telekom.hu

Kulcsszavak: IPv6, IPv4, dual-stack, PPP, szolgáltatói hálózat

A távközlésben világszerte terjed az „all-IP" koncepció, miszerint a különböző hozzáféréseken (például hagyományos vezetékes, kábeltévés, mobil) nyújtott különböző szolgáltatásokat (telefon-, internet- és műsorszolgáltatás) egy „közös" IP-hálózat segítségével kívánják biztosítani a szolgáltatók. Ennek következtében az IP-hálózatok napjainkban minden szolgáltatónál folyamatos fejlesztés alatt állnak, hogy a megnövekedett funkcionális és mennyiségi igényeket hatékonyan és megbízhatóan tudják kielégíteni. Az új szolgáltatások és funkciók az Internet Protokoll jelenleg használt 4-es verziójának (IPv4) eddig is ismert, de manapság még határozottabban jelentkező korlátaival szembesítik világszerte az internet és telekommunikációs szolgáltatókat, illetve a hálózati berendezések gyártóit. Ezen limitációkra, illetve a jövőben felmerülő újabb hálózati igényekre a protokoll legújabb, 6-os verziója (IPv6) kínálhat megoldásokat. Jelen cikk a szélessávú elérések IPv6-képessé tételével foglalkozik, melyek PPP-alapú enkapszulációt alkalmaznak.

1. Bevezetés

Az Internet Protokoll 6-os verzió (IPv6) kifejlesztésének fő mozgatórugója az interneten jelenleg használt 4-es verziójú (IPv4) címek várható „elfogyása" volt. Noha számos igen hatékony hálózati megoldás született a múltban (CIDR: Classless Interdomain Routing, NAT: Network Address and Port Translation stb.) annak érdekében, hogy az IPv4-címek fogyásának ütemét csökkentsék, az internet megállíthatatlan terjedésének köszönhetően ma már nyilvánvalóvá vált, hogy a rendelkezésre álló szabad IPv4-tartomány belátható időn belül elfogy. Jelen cikk írásakor nemzetközileg általánosan elfogadott előrejelzés, hogy az IPv4-címek elfogyása várhatóan 2011 környékén következik be [1]. Noha az IPv6-tal foglalkozó első szabványok a 90-es évek közepén láttak napvilágot, számos kérdés nyitott a szolgáltatói hálózatokban történő alkalmazása tekintetében. Jelenleg a szolgáltatók elsősorban az IPv6 internetelérésére koncentrálnak, így a továbbiakban csak ezen szolgáltatás nyújtásával kapcsolatos lehetséges műszaki megoldások/alternatívák kerülnek bemutatásra.

A következőkben röviden áttekintésre kerülnek az IPv6 főbb jellemzői, majd az IPv6-vonatkozású szabványok. Az ezt követő szakaszok a PPP-alapú szélessávú elérés IPv6-képessé tételéhez szükséges megoldásokat tárgyalja.

2. Az IPv6 főbb jellemzői

Az IPv6 a jelenlegi interneten használatos csomagtovábbítás továbbfejlesztett verziója, mely nagyságrendekkel nagyobb címtartományával közvetlenül címezhetővé teszi az internethez kapcsolódó berendezéseket. Az IPv6 öt legfontosabb jellemzője:

(i) nagyobb címtartomány,
(ii) közvetlen végponti címezhetőség,
(iii) automatikus konfiguráció,
(iv) többszörös címezhetőség és
(v) hálózati mobilitás.

Ugyanakkor számos tévhit kering az IPv6-tal kapcsolatosan a köztudatban. Nem fogja megoldani (sajnos) a szolgáltatók összes műszaki hálózati problémáját, de segít majd biztosítani a távközlési szolgáltatások nyújtását az IPv4-címek elfogyása után is. Sajnálatos módon az IPv6 számos tekintetben inkompatibilis a jelenlegi IPv4-protokollal, így nincs szó az IPv4 teljes lecseréléséről. Nagyon sokáig a két protokoll együttélésére kell felkészülni, azaz a távközlési rendszerekben mindkettőt támogatni kell.

Az IPv6 bevezetése elsősorban az IPv4-gyel való inkompatibilitása, valamint teljes hálózati érintettsége miatt nem egyszerű feladat, nem hajtható végre egyik pillanatról a másikra. Ez egy új technológia, mind a szolgáltatóknak, mind az ügyfeleknek meg kell tanulni bánni vele.

3. IPv6-vonatkozású szabványok és migrációs stratégiák

Az IPv6-vonatkozású, annak alapvető működését rögzítő szabványok az IETF szervezetében születnek és azok tanulmányozása elengedhetetlen a távközlésben dolgozó szakemberek számára. Ugyanakkor a szélessávú szolgáltatók szakemberei számára fontos irányelveket fogalmaznak meg például a Broadband Forum (BBF) munkacsoportjai, melyek a meglévő szabványokon alapuló szolgáltatói környezet tekintetében rögzítenek ajánlásokat.

Jelen írásunkban a BBF TR-101 szabvány [2] szerinti – a szélessávú szolgáltatók által általánosan elfogadott és használt – környezetben kerülnek bemutatásra az IPv6 használatával kapcsolatosan felmerülő műszaki kérdések. Cikkünk terjedelmi okokból nem foglalkozik a CATV-alapú (DOCSIS 3.0) és a mobil elérésen keresztüli IPv6-kapcsolódással.

Az IPv6 bevezetési megoldások tekintetében számos eltérő, a szabványosítás különböző fázisában lévő metódus látott napvilágot (pl. 6to4, 6rd, DS-lite, Softwire, Carrier Grade NAT stb.). Az egyes megoldások természetesen eltérő előnyökkel, illetve hátrányokkal bírnak, és folyamatos vitatémát biztosítanak a szakértők számára. Egyetértés van azonban a tekintetében, hogy a felhasználók számára egyidejűleg kell mind IPv4-, mind IPv6-kapcsolódást biztosítani. Az ilyen megoldást nevezik dual-stack-elérésnek – cikkünk a továbbiakban ezen megoldással foglalkozik PPP-alapú DSL-szolgáltatói környezetet feltételezve. A bemutatott rendszertechnikai kérdések azonban többnyire nem DSL-specifikusak, ennek megfelelően általánosíthatóak és a konklúziók más technológián alapuló elérések esetén is alkalmazhatóak (pl. GPON, P2P Ethernet).

A dual-stack-megoldás egyik fő előnye, hogy nincs szükség IPv4 és IPv6 hálózati átjárók létrehozása, melyek segítségével a csak egyik vagy másik verziót támogató végpontok kommunikálni tudnának egymással.

4. Dual-stack elérés DSL környezetben

4.1. IPv6-címzés

Az IPv6 esetében a címzésre 128 bit áll rendelkezésre. Ugyanakkor, ellentétben az IPv4-hálózatokkal, ahol a hálózati maszk változó méretű, az IPv6 esetében a hálózatok fixen 64 bites (/64) prefixeket használnak. Háromféle egyedi (unicast) címtípust lehet megkülönböztetni:

– link-lokális cím
(link local address, FE80::/10),
– globális unicast cím
(GUA: global unicast address),
– egyedi lokális cím
(ULA: unique local address, FC00::/7).

Minden végberendezésnek (hostnak) rendelkeznie kell link-lokális címmel és legalább egy GUA-címmel az IPv6 internetéréséhez.

A végpontok számára az IPv6 globális cím, illetve prefix biztosítására többféle dinamikus megoldás létezik:

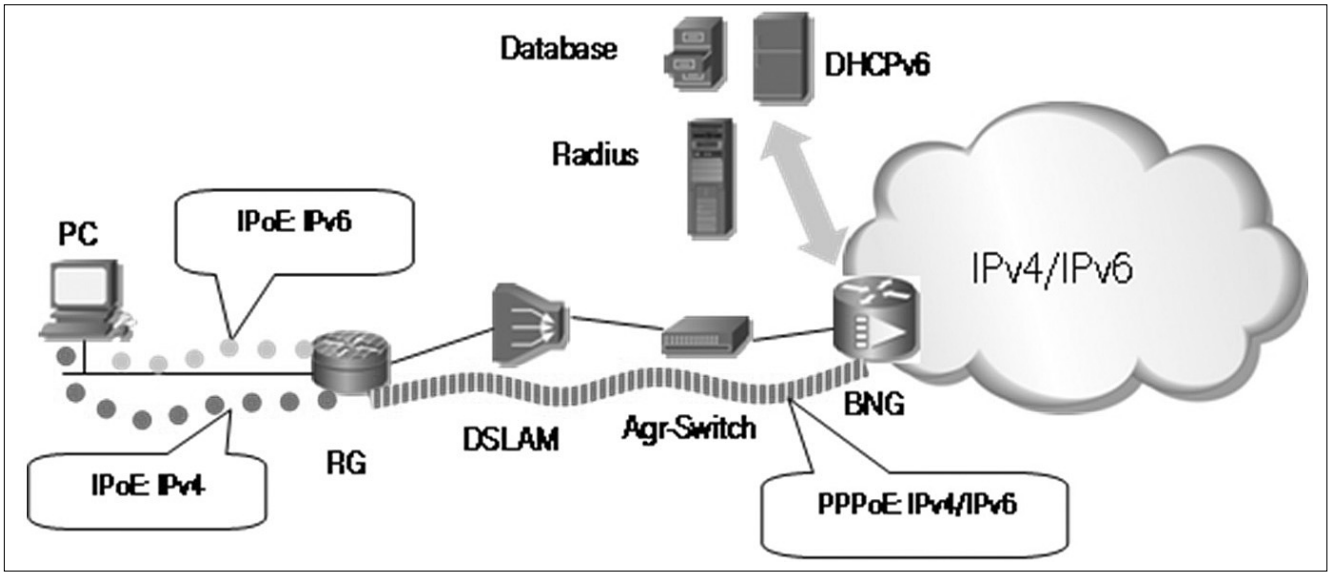
– SLAAC:
StateLess Address AutoConfiguration [3]
– DHCPv6:
Dynamic Host Configuration Protocol for IPv6 [4]
– DHCPv6-PD:
Prefix Delegation options [5]

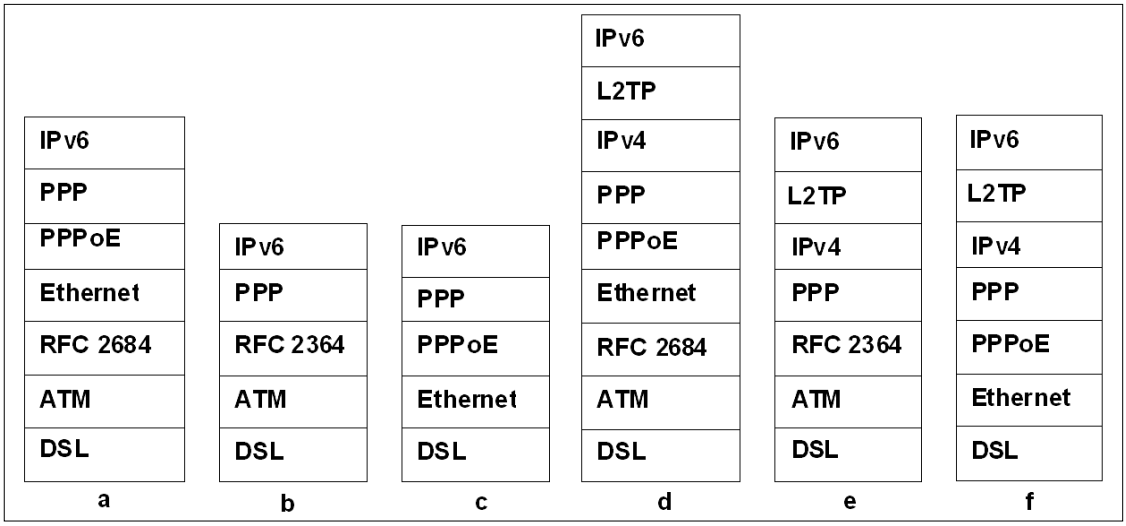
A SLAAC-módszer használatával a végpont a használandó IPv6-os címeit a lokálisan rendelkezésre álló és az adott hálózati szegmensre kapcsolódó router által hirdetett információkból generálja. A router az adott linkhez tartozó subnet prefix-et hirdeti, míg a végpont egy, az adott linken egyedi interface azonosítót generál. Az IPv6-os cím a két rész összeillesztéséből áll elő. Router hiányában a végpontok csak link-lokális címeket tudnak generálni és csak az adott linkre kapcsolódó végpontok tudnak egymással kommunikálni.

A DHCPv6 módszer a GUA-cím biztosítása mellett egyéb konfigurációs információk biztosítására is képes, melyeket speciális DHCPv6-opciók hordozhatnak.

A Prefix Delegation révén egy végpont egy teljes IPv6-tartományt tud kérni a hálózattól DHCPv6-üzenetek segítségével. Az IPv6 esetében az IPv4-gyel ellentétben nincs NAT-olás az otthoni hálózat és a szolgáltatói hálózat között. Ennek megfelelően az ügyfelek – a szolgáltatói hálózathoz egy otthoni routeren (RG – Residential Gateway) keresztül kapcsolódó – eszközei szempontjából gyakorlatilag elengedhetetlen a DHCPv6-PD használata a hatékony és automatikus címzéshez. A delegált prefix mérete az ügyfél hálózatától függően lehet: /60-/56, illetve /48.

1. ábra Szélessávú IPv6-kapcsolódás egyetlen PPP-session révén





2. ábra TR-101 U-referenciapont-protokollstack IPv6 esetében

Az előfizetői forgalom enkapszulációja tekintetében alapvetően két esetet lehet megkülönböztetni: a PPP-alapú elérést és natív IP-elérést. A DSL-, valamint az optikai elérésű szélessávú hálózatokban a szolgáltatók túlnyomó többsége PPPoE-alapú hálózati kapcsolódást biztosít az ügyfelek számára. Ez ugyancsak kapóra jön a szolgáltatóknak az IPv6 bevezetésekor, hiszen a PPP-enkapszuláció mintegy „elrejti" az IPv6-forgalmat az elérési és az aggregációs hálózat elől. Ennek megfelelően ezen hálózatrészekben nincs szükség IPv6-képesség implementálására.

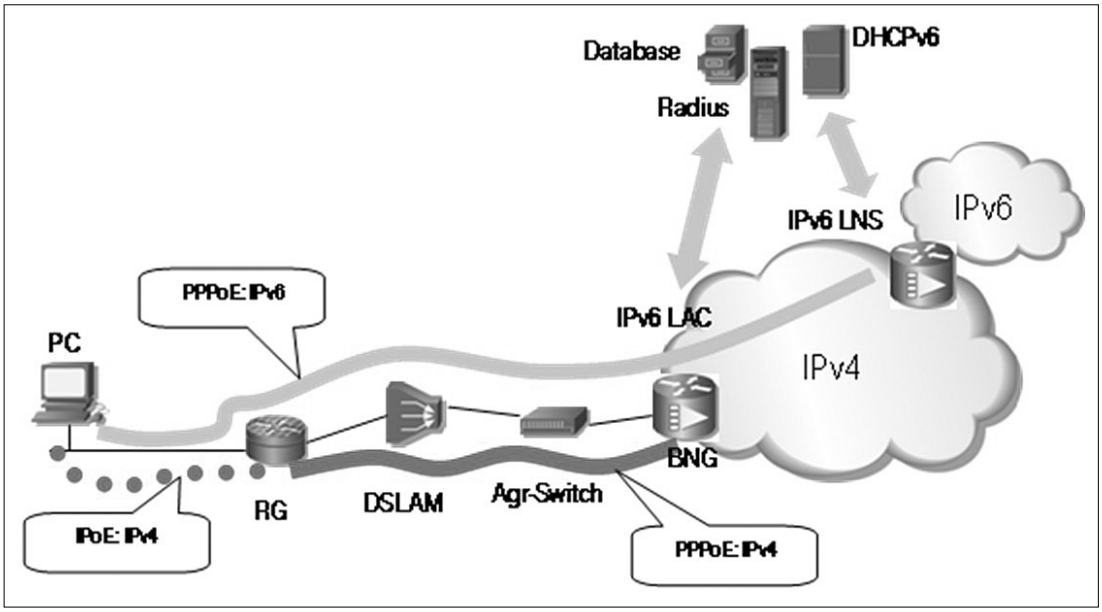
Az *1. ábrán* látható rendszertechnikában IPv6-képességekkel csupán az RG és a BNG kell rendelkezzen.

4.2. PPP-alapú szélessávú elérés

PPP-alapú elérés esetén az IPv6 megjelenésével a TR-101 ajánlás szerinti U referencia ponton a protokoll stack a *2. ábra* szerinti. A natív IPv6-megoldások mellett (a, b, c) az ábra megjeleníti a tunneling/softwire alapú megoldásokat is (d, e, f,).

A PPP-session használata mellett a dual-stack kapcsolat megvalósulhat egyetlen közös PPP-session-ön belül vagy külön IPv6, illetve IPv4 számára dedikált PPP-session-ök révén. Az előbbi esetében a PPP-kapcsolatot indító berendezés mind IPv4, mind IPv6 prefix-szel rendelkezik és az adott PPP-kapcsolaton keresztül továbbítja mindkét IP verzió csomagjait [6]. Utóbbi esetében az IPv4- és IPv6-forgalmat szállító PPP-kapcsolatok elkülönülnek, azokat akár különböző berendezések is indíthatják/végződtethetik. Míg az előbbi esetében a v4 és v6 rendszertechnika azonos, az utóbbi esetében két rendszertechnika akár el is térhet egymástól, ami különösen az IPv6 bevezetése során lehet előnyös.

Jelentős különbségek vannak a PPP használata szempontjából az IPv4- és az IPv6-protokoll tekintetében. Az LCP természetesen független a network layer-beli protokolltól, azonban az NCP már eltérő (IPCP, illetve IPV6CP). Míg az IPv4 esetében számos konfigurációs paraméter is eljut a végpontra, addig az IPV6CP csupán a link-local megkonstruálásához szükséges „inteface ID"-t egyezteti. Az IPv6-világban szükséges DAD (dupplicate address detection) szükségtelen PPP-kapcsolat esetében. GUA-cím konfigurálásához – a manuális konfigurációt elkerülendő – további automatikus mechanizmusokra



3. ábra Szélessávú IPv6-kapcsolódás külön PPP-session révén

van szükség: SLAAC, DHCPv6 vagy DHCPv6-PD. Közös PPP-kapcsolat esetében az IPv4- és IPv6-forgalom megkülönböztetése a PPP-fejrészbeli protokoll azonosítóval történik (IPv4: 0x0021, IPv6: 0x0057).

A PPP-kapcsolatot végződtető BNG berendezésnek ICMPv6 RA (Router Advertisement) üzeneteket kell továbbítani a PPP-peer számára, hogy a végpont beilleszsze a Default Router listájába [7]. Az RA üzenetek felhasználhatók arra is, hogy a végpont WAN kapcsolata számára SLAAC segítségével IPv6 címet biztosítson. Amennyiben a PPP kapcsolat felépülése során a BNG a RADIUS szervertől Framed-IPv6-Prefix attribútumot [8] is visszakap, akkor azt elhelyezi az RA-üzenet PIO-mezőjébe és beállítja az A-bitet (autonomous), valamint az O-bit-et (On-link). On-link prefix hiányában a végpont minden IPv6-os forgalmat a BNG-hez kell továbbítson, azaz nincs szükség az IPv4 világban megszokott Proxy-ARP funkcionalitásra. Az otthoni hálózaton használni kívánt prefix automatikus delegálására DHCPv6-PD-alapon van csak lehetőség. A DHCPv6 természetesen használható a WAN-kapcsolat GUA-címének biztosítására is. A delegálás számára az RG-nek kiosztandó prefixet – RADIUS alapú megoldás esetén – a BNG a Delegated-IPv6-Prefix attribútumban [9] kapja meg a felhasználó authentikálása során. Érdemes megjegyezni, hogy a PPP-interfészeken nincs szükség ND-mechanizmus (Neighbour Discovery) implementálására, így NS (Neighbour Solicitation) üzenetekre sem. Ugyanakkor a fentiekkel összhangban az RA-, illetve RS- (Router Solicitation) üzenetek elengedhetetlenek.

4.3. Routing – vonatkozó kérdések

Érdekes problémát vet fel routing szempontból a „prefix delegation” módszer használata. A BNG-routing táblájába ugyanis be kell jegyezni, mely PPP-kapcsolaton keresztül mely LAN prefix-ek érhetőek el a PPP-kapcsolatot indító berendezés mögött. A routing bejegyzés generálása történhet RADIUS-alapon a framed-ipv6-route [8] attribútum segítségével. Amennyiben a prefixdelegálás egy külső DHCPv6-szerver által történik akkor például a DHCPv6-relay-reply snooping szolgáltathatja a megoldást. Ha a DHCPv6-szerver implementálása a BNG-ben valósul meg és a címkiosztás a BNG-ben definiált pool-ból történik, akkor a BNG belső processzei közötti kommunikáció révén is aktualizálható a routing tábla.

Szolgáltatói környezetben az IPv6-címek kiosztásakor célszerű úgynevezett kvázi-fix címkiosztási módszert követni, azaz a felhasználóknak kiosztott cím mindaddig nem változik, amíg a szélessávú elérés hálózati kapcsolódási pontja változatlan. Ugyanakkor a cím változatlansága nem garantált, azaz adott esetben a szolgáltató egy hálózati rekonstrukció során megváltoztathatja a kiosztott címeket. A kvázi-fix címkiosztás egyik kulcseleme a fizikiai végpont („vonal”) azonosításra szolgáló információs átvitele és felhasználása.

4.4. Otthoni IPv6-hálózat

A szélessávú IPv6-elérés egyik legkritikusabb eleme az RG (Residential Gateway), melyek komoly hátráltatói az IPv6 elterjesztésének. A szabványok kialakításával még csak most kezdenek intenzívebben foglalkozni a szabványosító szervezetek (például Broadband Forum PD-192 dokumentum), így nem meglepő, hogy az implementációk ma még gyerekcipőben járnak. Az IPv6-szolgáltatók többsége önálló fejlesztés keretében biztosítja ezen berendezést előfizetői számára.

A RG IPv6-szempontból egy „tudathasadásos” berendezésnek tekinthető, hiszen a szolgáltatói hálózat felé végpontként (host) viselkedik, míg az otthoni hálózat felé mint router lép fel. Az RG a hálózattól megszerzett prefix révén, biztosítja az otthoni hálózathoz kapcsolódó berendezések számára szükséges konfigurációs információkat (GUA-cím, DNS-szerver stb.).

Mivel az IPv6-szabvány nem írja elő kötelezően a végpontok számára a stateful DHCPv6 [4] implementálását, az otthoni hálózatban a javasolt alapértelmezett címkiosztási módszer a SLAAC. A delegált címtartomány felhasználásával az RG /64 prefixeket használ a hozzá kapcsolódó otthoni hálózati szegmensek címzésére. A RG-re hárul az a feladat is, hogy hálózati rekonstrukció esetén a rá csatlakozó otthoni hálózati végpontokhoz tartozó címeket frissítse. Ezzel kapcsolatosan fontos szerepet játszik a címekhez tartozó élettartam-értékek (valid lifetime, preferred lifetime) propagálásának módja.

A DNS használata a mai hálózatokban gyakorlatilag nélkülözhetetlen, azonban az IPv6-környezet a kiterjesztett címek révén kritikus fontosságú. A DNS-feloldás történhet akár IPv4-, akár IPv6-alapon függetlenül a hordozott információtól (A és AAAA record). IPv6 feletti DNS-feloldáshoz a szerver címét stateless DHCPv6 [10] révén célszerű eljutatni a végberendezésekhez. Elvileg lehetőség van a DNS-információ RA-üzenetekben történő átadására is [11], azonban ez a megoldás a gyakorlatban nem igazán terjedt el. Elméleti lehetőségként fennáll még a manuális konfiguráció, de ennek használata erősen nem javallott.

5. Kitekintés

Az elérési sebesség növelésével mind több szolgáltató kacérkodik a PPPoE-enkapszuláció helyett a natív IP-alapú (IPoE) rendszertechnikára átállás gondolatával. Az IPv6 szempontjából ez számos addicionális – e cikkben nem tárgyalt – követelményt támaszt a hálózati berendezésekkel (access node, aggregation switch) szemben, különösen a szolgáltatók által kedvelt TR-101 szerinti N:1 VLAN-modell alkalmazása esetén. Ennek megfelelően egy-egy ilyen architektúrális változás során célszerű számolni azzal a sajnálatos ténnyel, hogy az alapjaiban érintheti az IPv6-os internetszolgáltatást.

6. Összefoglaló

Jelen cikk a PPP-alapú szélessávú elérések IPv6-képessé tételével kapcsolatos problémákat és megoldásaikat szándékozott bemutatni. Sokan magát az IPv6-ot

tekintik „killer application”-nek, mint ami megteremti a hálózatcentrikus világ létrehozásának lehetőségét. Ha a távközlési szakértők jól dolgoznak, akkor az IPv6 használata a végfelhasználó számára láthatatlan marad. Az egyetlen változás, hogy az internetezés élménye egyes esetekben egyszerűbbé válhat, valamint megjelennek majd olyan szolgáltatások/alkalmazások, melyek IPv4-alapon csak igen komplexen lennének nyújthatóak.

Az IPv6 a végfelhasználó szempontjából egy ajtó, mely megteremti a lehetőséget a változásra. Éppen úgy, mint ahogyan annak idején a vezetékes világban a DSL, vagy a mobil világban a 3G megjelenése indított el egy-egy kommunikációs forradalmat.

A szerzőkről

VARGA BALÁZS a Budapesti Műszaki Egyetemen szerzett villamosmérnöki diplomát 1993-ban, majd doktori fokozatot 1996-ban. Jelenleg a Magyar Telekom Fejlesztési Igazgatóság IP Funkcionális Fejlesztési Osztályának szakmai vezetője. Szakmai irányítása alatt került kifejlesztésre a Magyar Telekom szélessávú termék portfóliója mind az üzleti, mind a lakossági területen (IP VPN, L2 VPN, 3play stb.) valamint az új szélessávú technológiák bevezetése (xDSL, GPON, Ethernet) a Telekom hálózatába. Ezt megelőzően a Magyar Telekom IP Kompetencia Központjának szakmai munkáját irányította. Meghatározó szerepe volt az MPLS technológia hálózati implementációjában valamint az MPLS-alapú szolgáltatások kifejlesztésében. A Telekom képviselőjeként – az IPv6-os vonatkozású szabványok editoraként – részt vesz a Broadband Forum munkájában. Számos nemzetközi konferencia meghívott előadója.

BARTA PÉTER a Kandó Kálmán Műszaki Főiskolán szerezte villamos üzemmérnök diplomáját 1993-ban. Több magas szintű ICT iparági bizonyítvánnyal rendelkezik. Jelenleg senior fejlesztési menedzser a Magyar Telekom Fejlesztési Igazgatóságának IP Funkcionális Fejlesztési Osztályán. Fő területe az IPv6 alapú internet szolgáltatás kifejlesztése és megtervezése, illetve az IPv6 hálózati architektúrát és megoldásokat fejlesztő csoport munkájának összefogása. Munkájához tartozik az IP hálózati protokollok és MPLS-alapú szolgáltatások vizsgálata, illetve a Magyar Telekom hálózatának optimalizálása és fejlesztése, valamint a bevezetésre kerülő eszközök és technológiák elemzése.

GAÁL GÉZA a Budapesti Műszaki Egyetem Gépészmérnöki karán szerzett diplomát 1998-ban, majd 2008-ban a Budapesti Műszaki Főiskolán Mérnök-Informatikus diplomát. Több magas szintű ICT iparági bizonyítvánnyal rendelkezik. 1998 óta a Magyar Telekom PKI Távközlési Igazgatóságánál dolgozik. Szakterülete az Ethernet, IP-alapú hálózatok és az AAA rendszerek, valamint az ezeken alapuló termékek fejlesztése. Műszaki szakértőként meghatározó szerepe volt a Magyar Telekom AAA rendszerének kialakításában, illetve a hálózati biztonságot érintő fejlesztésekben.

HONVÁRI ISTVÁN a Nagy-Britanniai Edinburgh-ban kezdte felsőfokú tanulmányait, majd a Budapesti Műszaki Egyetemen szerzett villamosmérnöki diplomát távközlés szakirányon. Jelenleg a Magyar Telekom PKI Fejlesztési igazgatóságán fejlesztési menedzserként dolgozik. Fő feladata az IP funkcionális fejlesztési feladatok koordinálása és a műszaki megoldások kidolgozása. Szakterülete az AAA rendszer fejlesztése, az IP-hálózat biztonságának növelése és az IPv6 bevezetésének előkészítése. Ezt megelőzően hozzájárult többek között a Magyar Telekom L2 VPN üzleti szolgáltatásának, valamint az xDSL technológiákon alapuló lakossági internet termékek bevezetéséhez.

Irodalom

[1] http://www.inetcore.com/project/ipv4ec/index_en.html
[2] TR-101 Migration to Ethernet-Based DSL Aggregation, Broadband Forum, 2006-04-19
[3] RFC4862: IPv6 Stateless Address Autoconfiguration
[4] RFC3315: Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
[5] RFC3633: IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) v.6
[6] RFC4241: A Model of IPv6/IPv4 Dual Stack Internet Access Service
[7] RFC4861: Neighbor Discovery for IP version 6 (IPv6)
[8] RFC3162: RADIUS and IPv6
[9] RFC4818: RADIUS Delegated-IPv6-Prefix Attribute
[10] RFC3736: Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6
[11] RFC5006: Pv6 Router Advertisement Option for DNS Configuration
[12] RFC4193: Unique Local IPv6 Unicast Addresses
[13] RFC4291: IP Version 6 Addressing Architecture