Áttérés az újgenerációs Internet használatára

BENYOVSZKY BALÁZS, MEZŐ BALÁZS, PALLOS B. RICHÁRD, LUKOVSZKI CSABA

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

Kulcsszavak: IPv6, áttérési technikák, protokollfordítók

Az újgenerációs Internet ötletének megszületése és annak megvalósítása között eltelt idő közel sem volt olyan hosszú, mint amennyi idő szükséges lesz a protokoll elterjedéséhez. A legfontosabb feladat az, hogy az IPv6 megjelenése az Internet világában ne okozzon törést a világhálóban. Átjárható legyen mind az IPv4-et és IPv6-ot használó felhasználók számára is. Ez úgy lehetséges, ha minél hatékonyabb áttérési technikák segítik a két protokoll egyidejű működését. Az IPv6 számos előnyös tulajdonsága serkenti az áttérés folyamatát. Azonban vannak olyan tényezők is, amelyek lassítják, és késleltetik az IPv6 világméretű elterjedését.

Az Újgenerációs Internet megszületésének elsődleges és legfontosabb célja az volt, hogy megoldást nyújtson az egyre fogyatkozó IP címek problémájára. Ennek tökéletesen eleget tesz az új 128 bites cím, és a hierarchikus címzési rendszer. Az újabb felhasználók rövid időn belül rákényszerülnek az új címek használatára. Mikor a szolgáltatók már kifogynak a megszokott IPv4-es címekből, kénytelenek lesznek nyitni az IPv6 felé. Vannak azonban olyan előnyei az új protokollnak, ami esetleg arra ösztönzi a szolgáltatókat, felhasználókat, hogy ne várják meg ezt az időt, és hamarabb használják ki e hasznos tulajdonságokat.

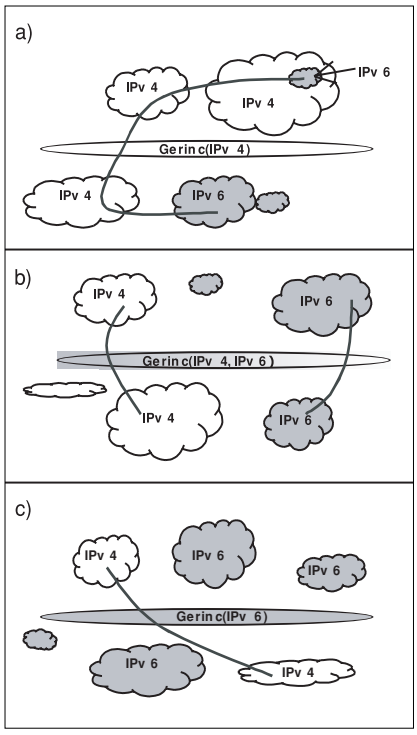
Egy komoly európai ösztönzésnek vehetjük azt a közelmúltban megjelenő hírt, mely szerint az Európai Unió területén 2007-2008-ig az IP 6-os verziójára akarnak áttérni. Ezzel kapcsolatban, már felülről irányuló ösztönzés érzékelhető.

Mindezek ellenére mégis azt tapasztalhatjuk, hogy az áttérés az IPv6 használatára nem olyan viharos sebességű, mint azt korábban sejthettük. Ennek oka lehet számos olyan IPv4-en alkalmazott kényszermegoldás, mely az új protokoll bevezetését nagymértékben késlelteti. Ilyen technika a rohamosan csökkenő IP címek problémájára ideiglenes megoldást nyújtó hálózati címfordító, ismert nevén a NAT (Network Address Translator). Ennek segítségével magánhálózati címeket oszthatunk alhálózati eszközeinknek, melyek csak kevés globális címen osztoznak az Interneten. Kívülről azonban emiatt nem tudjuk megcímezni az egyes eszközöket. A megoldás késlelteti az IP címek kimerülését, és ezáltal lassítja az áttérés folyamatát.

Az IPv6-os protokoll szélesebb körű bevezetése azonban nemcsak ezen okok miatt várat még magára. Számtalan előkészületi feladatot kell még elvégezni a világméretű elterjedése előtt. Létezik már egy IPv6-os gerinchálózat melyet 6Bone névre kereszteltek el, és amelyre a rákapcsolódás lehetősége számunkra is adott.

Azonban az IPv6-os áttérés nem tud azonnal megvalósulni. Számos olyan áttéréssel kapcsolatos vonatkozása van, melyeknek meg kell feleltetni az újonnan kapcsolódó eszközeinket. Az új protokollnak felülről kompatíbilisnek kell lennie a régivel, valamint az áttérés során a hálózat berendezéseinek egyaránt támogatniuk kell mindkét verziójú protokollt.

1. ábra Áttérési tendenciák



Nagyobb probléma viszont, hogy a hozzáférési és gerinchálózati szolgáltatók nincsenek felkészülve az IPv6-os átvitel kezelésére. Másrészt az alkalmazásoknak is támogatniuk kell az IPv6-os forgalom generálását. Mivel az áttérésnek nincs kitűzött időpontja, a fent említett tényezők mind az áttérési időszak elnyújtásához fognak vezetni.

Az áttérés tendenciái

Az IPv6-ra való áttérés menete három nagyobb időszakra bontható *(1. ábra)*, melyekben különböző megoldások használata célszerű az IPv4-es és IPv6-os protokollok egyidejű működtetéséhez.

Az IPv6 elterjedésének kezdeti szakaszában *(1/a. ábra)* jellemzően a mostani technológia által nyújtott infrastruktúrát kell használni. Ebben a szakaszban a meglévő gerinchálóz-

zatot kell úgy felhasználnunk, hogy a kisszámú, IPv6-alapú hálózatot össze tudjuk kapcsolni. Ezen, különálló IPv6 képességekkel rendelkező hálózatokat hívjuk IPv6-os szigeteknek. A szigetek összekapcsolásának megvalósítását tűzte ki célul a 6Bone projekt is. Az átállás e korai fázisában jellemzően az IPv6-ra már átállított hálózati eszközök egymás közötti kommunikációját kell megoldani IPv6 képességekkel nem rendelkező hozzáférési hálózatokon.

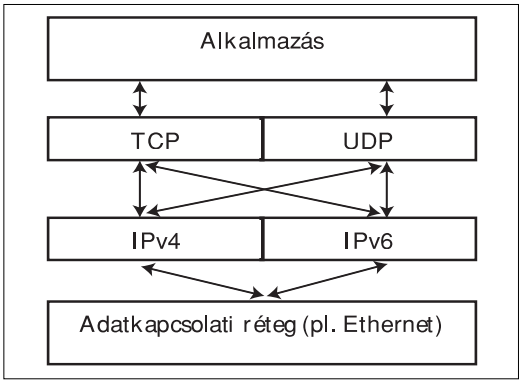
Az IPv6 terjedésével várhatóan egyre többen kapcsolódnak majd be az új protokoll használatába *(1/b. ábra)*. Emiatt a későbbiekben szükségessé válik, hogy a különböző verziójú IP protokollt támogató gépek képesek legyenek egymással kommunikálni. A végpontok számára további követelmény, hogy ez a kapcsolatfelépítés átlátszóan, a hálózat felhasználói számára észrevétlenül menjen végbe. Az IPv6 terjedésének utolsó szakaszában már jellemzően az IPv6 protokoll alapján működő eszközök lesznek túlsúlyban, miközben a gerinchálózatok is már az új protokollt fogják használni *(1/c. ábra)*. A gerinchálózatokon a még megmaradt IPv4-es eszközök üzemeltetése szintén valamilyen megoldást igényel.

Az IPv6-ra való áttérés hosszú folyamatnak ígérkezik. Emiatt szükséges, hogy az átállás közben a már működő IPv4 feletti alkalmazások zökkenőmentesen legyenek képesek illeszkedni az új protokollhoz. Ezen igény miatt születtek az áttérési technikák, melyek a két protokoll együttműködését hivatottak biztosítani.

Áttérési technikák alapjai

Az áttérési technikák alapjainak három nagy csoportját kell megemlítenünk. Ezek kombinálásával alakítható ki az adott lehetőségekhez legjobban illeszkedő megoldás.

Az első és legfontosabb technikája az áttérésnek az IPv6 csomagok átvételének megvalósítása egy IPv4-es eszközön. Ilyenkor a már meglévő IPv4-es protokoll verem „mellé” egy IPv6-ost is létesítünk, így az eszköz *kettős protokoll veremmel* [1] fog rendelkezni. A megoldás lényege, hogy a hálózati eszközök így képesek mind az IPv6-os, mind pedig a IPv4-es protokoll feldolgozására. Az eszköz felismeri a bejövő IP csomagokat, és a megfelelő veremnek továbbítja. Az alkalmazások a két protokollt egyidejűleg használhatják *(2. ábra)*.



2. ábra Kettős protokoll verem

Számítógépek számára ez a megoldás csupán szoftverfrissítést igényel, egyéb beágyazott rendszereket futtató hálózati eszközök esetében viszont sokszor komolyabb költségeket jelenthet. Egy hálózati útválasztó esetén például szükséges az útválasztó protokollok frissítése is. Ilyen frissített protokoll a RIPng, az OSPFv6 vagy a BGP4+.

Figyelembe kell venni azonban a többletterhelést is. Mivel a kettős protokoll veremmel rendelkező eszközöknek IPv4-es és IPv6-os címre is szükségük van, ezért ezen eszközöknek nagyobb többletterheléssel méretezendők a címek karbantartása miatt. Egy hálózati útválasztóban például meg kell oldanunk, hogy az eddigi 32 bites IP címekre méretezett útválasztó táblák mellett képes legyen az eszköz a 128 bites IP címekkel rendelkező IPv6-os hálózatok szerkezetét is tárolni.

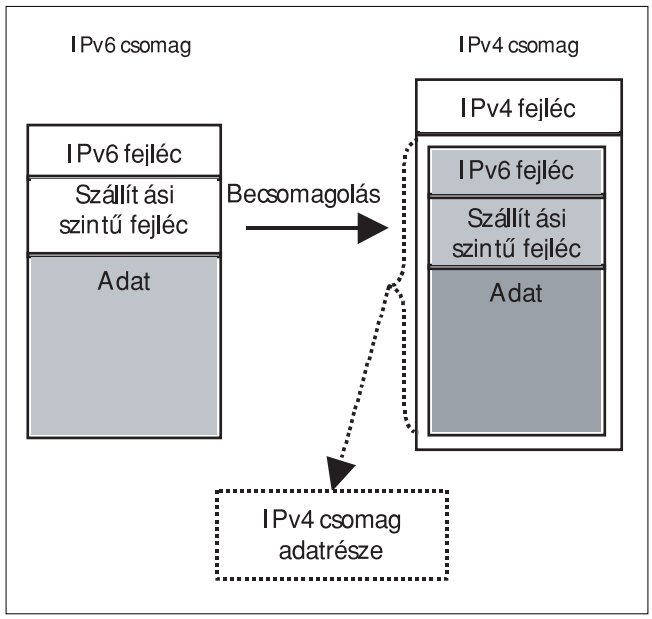
Ugyan az új technológia funkciói ezen esetben kis költséggel kihasználhatóvá válnak, de ez a megoldás semmit sem javít az IPv4-es címek elfogyásán. Szintén nem oldja meg a csak IPv6-ra, illetve csak IPv4-re felkészített csomópontok közötti kommunikációt.

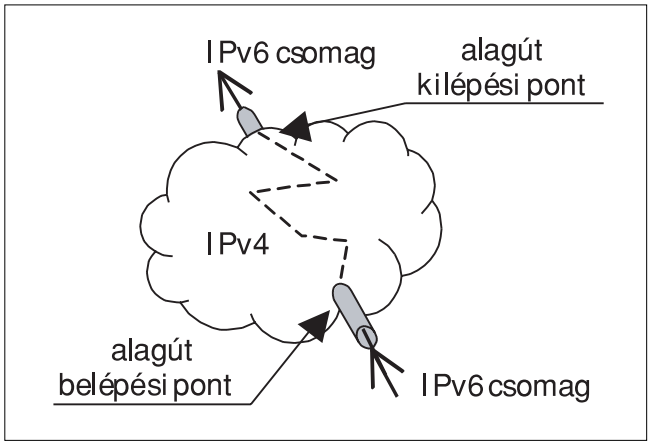
A kettős protokoll verem megvalósítása a legtöbb áttérési megoldás működéséhez alapkövetelmény.

A második áttérési módszer az *alagút technika* [1], amely nagyobb távolságok áthidalására született arra az esetre, ha közöttük nem áll rendelkezésre IPv6-os hálózati összeköttetés. Alkalmazásával lehetséges távoli elszigetelt IPv6-os hálózatok összekapcsolása valamilyen hordozó protokoll felett. A megoldás lényege, hogy az IPv6-os csomagokat egy azonos szintű protokoll csomagjaiba ágyazzuk *(3. ábra)*.

A beágyazás az IPv6 kezelésére alkalmatlan hálózatbelépési ponton történik meg. Ezen hálózatban az útválasztók nem tekintenek bele a csomag tartalmába, melynek hasznos terhében „utazik” a teljes IPv6-os csomag *(4. ábra)*.

3. ábra IPv6-os protokoll IPv4-be ágyazása





4. ábra Az alagút technika

A köztes hálózat a saját útválasztásának megfelelően (az ábrán szaggatott vonallal) továbbítja a csomagokat az alagút végpontja felé, a belső IPv6-os tartalommal nem foglalkozik.

Az alagút kilépési pontja az IPv6-os csomag célhálózatának pereme, mely szükségszerűen egy dupla protokoll veremmel rendelkező hálózati eszköz. A csomópont felismeri a beágyazott IPv6-os csomagot, és elvégzi a kicsomagolást a hordozó protokoll „burkából". Ezután a csomagot már IPv6-os csomagként továbbítjuk. A legelső ilyen megvalósítás a 6over4 technika volt [2].

Az alagút alapú technikáknak két nagy hátránya van. Mivel a meglévő protokollokat egy azonos szintű protokollba kell becsomagolni, ezért ez egy plusz fejlécet jelent minden csomagnak. Ekkor egyrészt növekedik a hálózati terhelés, másrészről a megnövekedett csomagméret miatt az alagútban szükség lehet a csomagok tördelésére.

Az alagút technikát használó megoldások két nagy csoportja a manuálisan beállított, és az automatikusan konfigurálódó alagutak. Az *automatikus alagutak* alkalmazásánál speciális, IPv4 kompatíbilis IPv6 címeket használunk. Itt az IPv6-os cím megegyezik az IPv4-es címmel, megfelelő számú nulla bitet eléírva. Ilyen IPv4 kompatíbilis IPv6-os címet használnak a kapcsolattartó eszközök az alagút belépési pontjának címzésére. Miután az IPv6-os hálózat eljuttatta a küldött csomagot az alagút belépési pontjának, az egy IPv4-es csomagba helyezi az IPv6-os csomagot. Így a belépési pont az IPv4-es protokollon indítja útjára a csomagot. Az útválasztás értelemszerűen az IPv4-es topológia szerint történik. A megoldás előnye a konfiguráció automatizálása, mellyel több távoli hálózatot is elérhetünk külön alagút adminisztráció nélkül. Hátránya, hogy az IPv6 128 bites címtere az IPv4 kompatíbilis címek miatt nem használható ki, ezért ebben az esetben meg kell elégednünk a jelenlegi protokoll 32 bites címeivel.

A *manuálisan beállított alagutak*nál adminisztrálni kell a távoli hálózat felé menő alagút be- és kilépési pontját, valamint az útválasztási táblákat. Kevés külső szigettel való összeköttetés esetén ez egyszerűen használható megoldás.

Az előzőekben tárgyalt módszerek nem teszik lehetővé a csak IPv4-et és a csak IPv6-ot támogató eszközök együttműködését. Az áttérési technikák harmadik típusa, a *protokoll fordítók*, e probléma megoldására születtek. Működésükből és a két protokoll közötti sok különbségből adódóan nem alkalmasak hosszú távon megoldani a csak IPv4 és a csak IPv6 képességű eszközök együttműködését. Sok esetben csak kellő körültekintéssel alkalmazhatóak, ennek ellenére a legtöbb esetben kielégítő megoldást nyújtanak.

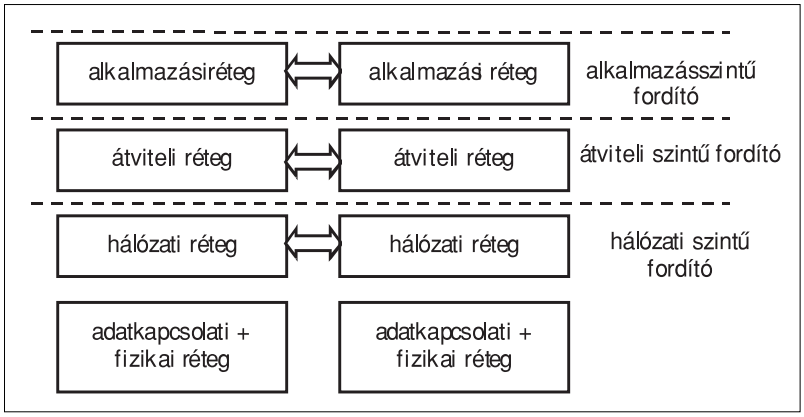
A protokoll fordítás műveletét e technikák a TCP/IP hivatkozási modell különböző rétegeiben végezhetik el. A modell rétegei alapján különböztetjük meg az alkalmazás szintű, az átviteli szintű és a hálózati szintű protokollfordítókat *(5. ábra)*.

Legalacsonyabb szinten a *hálózati rétegbeli protokollfordító* dolgozik. Ezen az absztrakciós szinten a fordítóprogram csupán a régi és az új protokoll fejléceit képes egymásba átfordítani. Működése egyszerű, mivel nem vizsgálja a csomagok tartalmát, csupán a fejlécet. Ebből adódóan a beágyazott IP címet tartalmazó protokollokat (mint például az FTP vagy a DNS) nem képes hibátlanul fordítani. Egyszerű konfigurálhatósága és a fordítás gyorsasága miatt használják.

Az *átviteli rétegben megvalósított fordítókat* kiszolgálókon lehet alkalmazni. Működésük lényeges eleme, hogy két külön kapcsolatot építenek fel a fordítandó kapcsolat esetében, így hasonló koncepcióban működnek, mint a proxy tűzfalak. A kezdeményező fél a szerveren keresztül próbálja elérni a célt. A szerver ekkor felépít egy kapcsolatot a kezdeményezővel az egyik (tegyük fel, IPv6-os) protokollon. Ezután kiépít egy kapcsolatot a cél felé, de ezt már a másik (IPv4-es) protokollon teszi. Ezek után a két fél között továbbítja a csomagokat, és a két protokollt egymásba átfordítja.

Működésének feltétele egy speciális DNS fordítóprogram, mely az IPv4-es címeket fordítja megfelelően az IPv6-os eszközök számára. Emiatt csak olyan IPv6-os végpont képes kapcsolatot létesíteni az IPv4 felé, mely a DNS fordítón keresztül keresi az IPv4-es cél cí-

5. ábra A fordítók típusai



mét. A visszakapott cím egy előtagból és a cél IPv4-es címéből áll. A speciális előtagot a hálózat a fordítást végző kiszolgáló felé irányítja, így halad azon keresztül a két fél közötti adat. A kiszolgáló a megfelelő címkonverziókat elvégezve valósítja meg a fordítást.

Az *alkalmazási rétegben megvalósított fordító*k lényege, hogy a fordító a teljes csomagtartalom alapján végez fordítást. Legtöbbször két inkompatíbilis hálózat közötti átjárónak alkalmazzák, emiatt tartalmaznia kell mindkét hálózat protokolljának implementációját. Mivel a teljes csomagtartalom alapján végez protokollkonverziót, ezért jóval nagyobb a számításigénye, mint az alacsonyabb rétegben működő fordítóknak. A használni kívánt alkalmazások számára külön kell a szükséges protokollokat a fordítóban megvalósítani. Emiatt ez a technika megoldja a beágyazott IP címeket tartalmazó protokollok fordításának nehézségét is.

Magán felhasználók

A kidolgozott áttérési technikáknak köszönhetően az otthoni felhasználók számára lesz a legkönnyebben megvalósítható az áttérés. Jelenleg ha egy magán felhasználó csatlakozni szeretne az IPv6-os hálózathoz, akkor erre a legegyszerűbb lehetősége valamilyen IPv6-os alagút alapú megoldás segítségével van.

A felhasználók szempontjából egyik legkényelmesebb megoldás az *alagút ügynök* [3] használata. Ehhez egy dedikált szervernek kell működnie azon szolgáltatónál, mely az IPv6-os hozzáférést szolgáltatja. Az ügynök feladata, hogy a felhasználó azonosítása után létrehozza az alagutat, szükség esetén módosítsa, használat után pedig lebontsa azt. Bejelentkezéskor elvégzi az alagút szerverekben szükséges beállításokat és elkészíti a DNS bejegyzéseket is az IPv6-hoz csatlakozó felhasználó számára, továbbá beállítja a használt alagút végpontjainak címeit. Működéséhez meglévő IPv4-es infrastruktúra szükséges, előnyeit és hátrányait az alagút alapú megoldásoktól örökli.

Hasonló, ám időben jóval előrébb tekintő megoldás *a kettős protokoll verem alapú áttérési technika* (DSTM) [4]. Erre az áttérés késői szakaszában lesz szükség, amikor a hálózatok jórészt az IPv6-os protokollal működnek.

A DSTM egy szerver-kliens alapú modell, melyben a szervert a hozzáférési szolgáltató biztosítja. A kliens ekkor már főként az IPv6-os protokollt fogja alkalmazni, de szükség lesz rá, hogy kettős protokoll veremmel rendelkezzen. Amennyiben a kliens IPv6-os végponttal szeretne kapcsolatot teremteni, azt gond nélkül megteheti. Ha viszont csak IPv4 támogatással rendelkező címet próbálna elérni, szüksége lesz egy IPv6 feletti IPv4-es alagútra a távoli végpontig. A kliensnek az alagút elkészítéséhez szüksége van IPv4-es címre is, mellyel alapesetben nem rendelkezik. Ekkor jön a képbe a DSTM szerver, mely a kommunikáció időtartamára egy IPv4-es címet szolgáltat az alagút végpontnak és elvégzi annak beállításait.

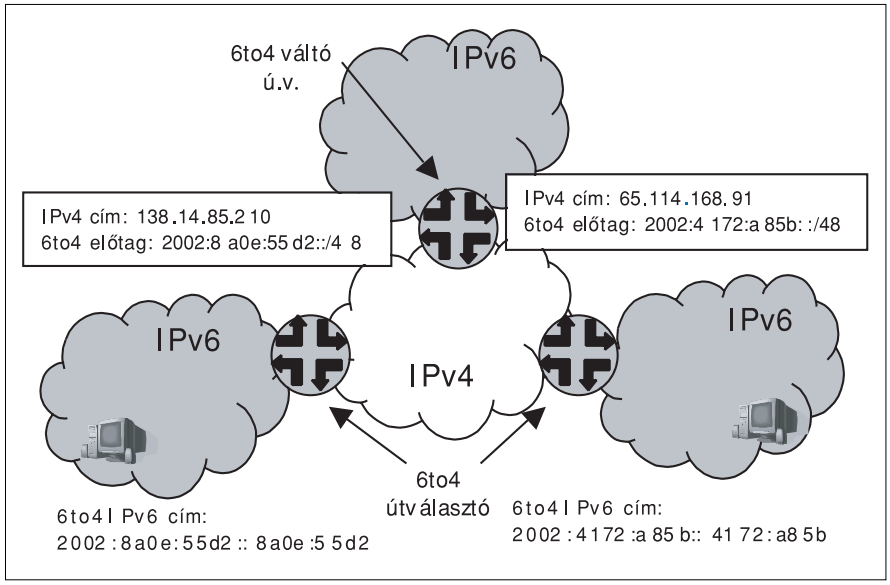
Hozzáférési szolgáltatók

Egy hálózaton belüli elszigetelt IPv6-os alhálózatok összekötésének leggyorsabb módszere a kézzel adminisztrált alagutak alkalmazása. Ezeket egyszeri beállítás után stabilan lehet használni IPv4-es hálózat áthidalására. Több ilyen elszigetelt hálózat esetén viszont a *6to4* [5] alagút megoldás alkalmazása célszerű, mely képes automatikus alagutakat építeni, így elkerülhető a bonyolult alagútmenedzselés. Működésekor az IPv6-os alhálózat egy speciális IP cím előtaggal [6] hirdeti a hálózathoz tartozó, távoli hálózatba vezető alagutak belépési pontjainak címeit *(6. ábra)*. Ezek szükségszerűen dupla protokoll veremmel rendelkező alagút végpontok, melyeknek van IPv4-es címe. Ezen IPv4 címeket az alagút végpontok a közös IPv4-es hálózaton egymás között hirdetik. Így az IPv4-es hálózathoz kapcsolódó IPv6-os alhálózatok határaihoz eljutnak ezen információk.

A meghirdetett címek alapján az IPv6-os szigetek egymás között már képesek alagutakat felépíteni. A megoldás érdekessége, hogy a címek hirdetésére elegendőek lehetnek a már régóta működő IPv4 feletti útválasztó protokollok.

Az eddigi alagút alapú megoldásokhoz szükség volt globális IPv4-es címre, mely az alagút egyik végpontját jelentette. Amennyiben szükségünk lenne privát címtartományból, például hálózati címfordítóval (NAT) védett hálózatból elérni távoli IPv6-os hálózatokat, a *Te-*

6. ábra A 6to4 működése



redo [7] megoldást kell szemügyre vennünk. Ez az egyetlen megoldás mely képes NAT mögül is megfelelően működni.

Az *állapotmentes IP/ICMP fordító* [8] (SIIT) a hálózati rétegben működő protokollfordító. Feladata, hogy a fordítást végző eszköz számára állapotmentesen, azaz belső állapotok tárolása nélkül valósítsa meg a protokollok fejlécei közötti váltást. Megoldja az ICMP csomagok fordítását és tördeli az IPv4-es csomagokat, hogy az IPv6-os hálózat maximális csomagméretének megfeleljenek. Külön IPv6 címeket használ azon IPv4-es eszközök számára, melyek értelmezni tudják az újabb protokollt. Ezen címek az IPv4 lefordított címek. Az IPv6-ot nem támogató eszközöket az IPv4 összerendelt címekkel azonosítja.

Működése során a fordító az IPv4 és IPv6-os fejléceket alakítja át egymásba. Alkalmazása azon esetekben lehetséges, ahol a teljes alhálózat támogatja már az IPv6-ot, és szükséges a külső IPv4-es címek használata. A kapcsolatokhoz az IPv6-os végpontoknak IPv4 lefordított címekre van szükségük, melyeket egy speciális DHCP kiszolgáló oszt ki számukra.

Az SIIT fordítókat az IPv6-os hálózat határán kell elhelyezni. Állapotmentes működésük miatt nem szükséges, hogy egy kiszemelt kapcsolatnak minden csomagja egy eszközön haladjon keresztül, ezért a határoló pontokon párhuzamosan több SIIT eszközt is lehet használni a terhelésmegosztásra.

Szintén hálózati rétegbeli mechanizmus a *hálózati címfordító és protokollfordító* (NAT-PT), mely a NAT megoldás egy kiterjesztése [9]. Működése a felhasználó számára hasonlóan átlátszó protokollfordítást tesz lehetővé, mint az SIIT megoldás. Fontos kiemelni viszont, hogy a NAT-PT szintén az IPv6 sziget határán helyezkedik el, de mivel a NAT-PT állapottartó, ezért szükséges, hogy minden a szigetről kifele kezdeményezett hálózati kapcsolat rajta, vagy vele együttműködő útválasztókon keresztül haladjon. A NAT-PT működésekor minden, az IPv6-os szigetet azonos cél felé elhagyó csomaghoz, dinamikusan rendel egy IPv4 címet az általa használt IPv4 címtérből. Így a NAT-PT az IPv6-os szigetről kapcsolatot kezdeményező fél számára átlátszóan továbbítja a csomagokat az IPv4-es cél felé.

A NAT-PT előnyös tulajdonsága, hogy az IPv6-os szigeten nincs szükség kettős protokollveremre. A kiszolgáló beállítása egyszerű, az IPv6-os alhálózat számára átlátszó.

Az átviteli rétegben működő, szervereken megvalósítható mechanizmus a *Transport Relay Translator* [10] (TRT). A TRT feladata, hogy a rajta keresztülhaladó csomagokat elfogja, és átfordítsa IPv4-ről IPv6-ra és viszsza ugyanígy. Egy kapcsolat felépülése után fontos, hogy a teljes kapcsolat a TRT kiszolgálón haladjon keresztül. Működéséhez szükséges egy speciális DNS kiszolgáló, mely az IPv6-os sziget által megcímzett távoli hálózaton elhelyezkedő IPv4-es cél címét egy megfelelő előtaggal kiegészítve IPv6-os címként oldja fel. Az előtag feladata, hogy a hálózat a TRT kiszolgáló felé továbbítsa a távoli, IPv4-es félnek küldött csomagot, melyet a kiszolgáló lefordít és továbbküld a cél felé.

A TRT megvalósítása a *SOCKS64* [11] technika, mely az átviteli rétegben működik, ehhez kettős protokoll veremmel rendelkező kiszolgáló, valamint a kliensek hálózati programkönyvtárainak módosítása szükséges, mivel a kliens és a szerver egy speciális SOCKS protokollon kommunikálnak. Az eredeti SOCKS implementáció [12] tűzfallal izolált hálózatokon keresztül nyújtott átjárót a belső hálózat IPv4-es és a külső hálózat szintén IPv4-es hálózati eszközei között. A SOCKS64 megvalósítás már lehetővé teszi IPv4-es és IPv6-os csomópontok kommunikációját mind homogén (azonos protokollok között pl. IPv4-IPv4), mind heterogén (különböző protokollok esetén pl. IPv6-IPv4) kapcsolat esetén.

Teljes protokoll konverziót valósítanak meg az *alkalmazás szintű átjáró*k [13] (ALG). Az átjárók két inkompatíbilis hálózat határán helyezkednek el, és szükségszerűen rendelkeznek mindkét hálózat protokollvermével. A két hálózat közötti kommunikáció teljes protokoll konverzióját elvégzik. Mivel ehhez szükséges a teljes csomagtartalom vizsgálata, ezért az alkalmazás szintű átjárók működése jelentősen nagyobb terheléssel jár, mint az alacsonyabb szinten megvalósított áttérési megoldásoké.

Az IPv4 és IPv6 közötti különbségek miatt a fordítás során bizonyos funkciók elveszhetnek, de ezektől eltekintve az ALG megoldja az összes problémát, mely a többi technikánál jelentkezhet.

Összefoglalás

A szolgáltatóknak a fent említett technikák kiválasztásánál figyelembe kell venni a korábban alkalmazott átviteli technológiákat. Munkájukat nagyban megkönnyíti, hogy az Internetes társadalom már eddig is nagy erőfeszítéseket tett arra, hogy megvizsgálja az IPv6 ATM-mel és MPLS technológiával való együttműködését.

Az áttérési technikák hivatottak tehát az IPv4 és IPv6-os protokollok együttműködését megvalósítani. De mint érzékelhető, az áttérés komplex feladat, melyre nincs egyértelmű megoldás. Minden esetben az adott környezethez és infrastruktúrához legjobban megfelelő technikát érdemes alkalmazni.

Irodalom

[1] R. Gilligan, E. Nordmark,
"Transition Mechanisms for IPv6 Hosts and Routers",
Request for Comments 1933,
Network Working Group, April 1996
[2] B. Carpenter, C. Jung,
"Transmission of IPv6 over IPv4 Domains
without Explicit Tunnels",

Request for Comments 2529,
Network Working Group, March 1999
[3] A. Durand, P. Fasano, I. Guardini, D. Lento,
"IPv6 Tunnel Broker",
Request for Comments 3053,
Network Working Group, January 2001
[4] Jim Bound,
"Dual Stack Transition Mechanism ",
INTERNET DRAFT, July 2003
[5] B. Carpenter, K. Moore,
"Connection of IPv6 Domains via IPv4 Clouds",
Request for Comments 3056,
Network Working Group, February 2001
[6] C. Huitema,
"An Anycast Prefix for 6to4 Relay Routers",
Request for Comments 3068,
Network Working Group, June 2001
[7] C. Huitema,
"Teredo: Tunneling IPv6 over UDP through NATs",
Internet Draft, February 5, 2004
[8] E. Nordmark,
"Stateless IP/ICMP Translation Algorithm (SIIT)",
Request for Comments 2765,
Network Working Group, February 2000
[9] G. Tsirtsis, P. Srisuresh,
"Network Address Translation –
Protocol Translation (NAT-PT)",
Request for Comments 2766,
Network Working Group, February 2000
[10] J. Hagino, K. Yamamoto,
"An IPv6-to-IPv4 Transport Relay Translator",
Request for Comments 3142,
Network Working Group, June 2001
[11] H. Kitamura,
"A SOCKS-based IPv6/IPv4 Gateway Mechanism",
Request for Comments 3089,
Network Working Group, April 2001
[12] M. Leech, M. Ganis, Y. Lee, R. Kuris,
D. Koblas, L. Jones,
"SOCKS Protocol Version 5",
Request for Comments 1928,
Network Working Group, March 1996
[13] K. Yamamoto, M. Sumikawa,
"Overview of Transition Techniques for
IPv6-only to Talk to IPv4-only Communication",
Internet Draft, March, 2000

Hírek

20 éves a Cisco Systems. Az 1984-ben alapított cég neve az elmúlt két évtizedben egybefonódott az Internet történetével. Len Bosack és Sandy Lerner, a Stanford Egyetem kutatói két évtizede alapították meg a Cisco Systems céget, amely nevét San Francisco városáról kapta. Bosack és Lerner a különálló hálózatok összekötésének lehetőségeit vizsgálta a Stanford Egyetem két épülete között. Ahhoz azonban, hogy a hálózatokat ténylegesen összekapcsolhassák, egy olyan új technológiára volt szükség, amely képes kezelni a különböző helyi hálózati protokollokat. Ez az elképzelés vezetett a többprotokollos útválasztó megszületéséhez.
Az alapítás óta eltelt két évtized alatt a Cisco a hálózati gazdaság előfutárából jelentős nemzetközi nagyvállalattá vált. A Cisco Systems IP alapú hálózati megoldásai biztosítják mind az Interneten, mind a legtöbb nagyvállalat, felsőoktatási és kormányzati intézmény számára az adatkommunikációs kapcsolatot. A világhálón közlekedő információk döntő részét a cég rendszerei szállítják.

A Cisco Systems Cisco Carrier Routing System (CRS-1) nevű terméke a világ legnagyobb kapacitású internetes útválasztójaként bekerült a Guinness-rekordok könyvébe.
A 92 terabites összteljesítményű útválasztórendszer az eddigieknél mintegy kétszer nagyobb adatforgalmat tesz lehetővé. Az Egyesült Államok kongresszusi könyvtárának teljes gyűjteménye 4,6 másodperc alatt letölthetővé válik. Ugyanennek az anyagnak a letöltése egy másodpercenként 56 kilobites sebességet biztosító behívásos modemmel körülbelül 82 évig tartana. A számok magukért beszélnek.
A valós idejű hangátviteli és csevegőszolgáltatásnak köszönhetően egyszerre akár egymilliárdan is játszhatják ugyanazt az online játékot. Az Egyesült Államok összes házttartása (105 480 101 otthon) 872 kbit/s sebességű nagy sávszélességű kapcsolathoz juthat. A hálózaton keresztüli egyéni videolejátszással egyszerre 15 millióan élvezhetik a 6 Mbit/s sebességű, kitűnő minőségű videoprogramokat. Egyszerre megközelítőleg 12 415 felhasználó töltheti le ugyanazt a 7,4 GB-os filmet, és ez mindössze 1 másodpercet vesz igénybe. A CRS-1 az internetes szolgáltatások és multimédiás alkalmazások eddig nem tapasztalt mértékű elterjedése előtt nyitja meg az utat.