13. Protocolul IPv6

13.1. Cuprins modul

Introducere

La începuturile sale, Internet-ul a fost folosit in mare măsură de universități, industria de vârf şi de guvernul Statelor Unite (in mod special de Departamentul Apărării). O dată cu explozia interesului față de Internet începând de la mijlocul anilor 1990, a început să fie utilizat de un grup diferit de persoane, în special persoane cu cerințe diferite. Pe de o parte, numeroase persoane cu calculatoare portabile fără fir îl folosesc pentru a ține legătura cu baza de acasă. Pe de altă parte, o dată cu iminenta convergență a industriilor calculatoarelor, comunicațiilor şi a distracțiilor, s-ar putea să nu mai fie mult până când fiecare telefon sau televizor din lume va fi un nod Internet, producând un miliard de gazde folosite pentru audio si video la cerere. În aceste condiții, a devenit clar că IP-ul trebuie să evolueze, să devină mai flexibil şi mai ales să asigure un număr mai mare de adrese.

Obiective

După parcurgerea acestei unități de învățare studenții vor fi capabili:

- ✓ Să argumenteze necesitatea protocolului IPv6
- ✓ Să opereze cu adrese IPv6
- ✓ Să descrie posibilitățile de tranziție de la IPv4 la IPv6

Durată medie de studiu individual

Durata medie de studiu individual: 2 ore

În plus față de aceste probleme tehnice, există un alt aspect întrezărit in fundal. Observând aceste probleme la orizont, IETF a început să lucreze in 1990 la o nouă versiune de IP, una care să nu îşi epuizeze niciodată adresele, să rezolve o gamă largă de alte probleme şi să fie totodată mai flexibilă şi mai eficientă. Obiectivele majore au fost:

1. Să suporte miliarde de gazde, chiar cu alocare ineficientă a spațiului de adrese.
2. Să reducă dimensiunea tabelelor de dirijare.
3. Să simplifice protocolul, pentru a permite ruterelor să proceseze pachetele mai rapid.
4. Să asigure o securitate mai bună (autentificare şi confidențialitate) față de IP-ul curent.
5. Să acorde o mai mare atenție tipului de serviciu, în special pentru datele de timp real.
6. Să ajute trimiterea multiplă, permițând specificarea de domenii.
7. Să creeze condițiile pentru ca o gazdă să poată migra fără schimbarea adresei sale.
8. Să permită evoluția protocolului în viitor.
9. Să permită coexistența noului şi vechiului protocol pentru câțiva ani.

Pentru a găsi un protocol care să îndeplinească toate aceste cerințe, IETF a emis o cerere de propuneri şi discuții în RFC 1550. Au fost primite douăzeci şi unu de răspunsuri, nu toate din ele propuneri complete. Până în decembrie 1992, au ajuns pe masa discuțiilor şapte propuneri serioase. Ele variau de la efectuarea de mici cârpeli la IP până la renunțarea completă la el şi înlocuirea cu un protocol complet nou.

IPv6 îndeplineşte obiectivele destul de bine. El menține caracteristicile bune ale IP-ului, le elimină sau atenuează pe cele rele şi adaugă unele noi acolo unde este nevoie. În general, IPv6 nu este compatibil cu IPv4, dar el este compatibil cu celelalte protocoale Internet auxiliare, incluzând TCP, UDP, ICMP, IGMP, OSPF, BGP şi DNS, câteodată fiind necesare mici modificări (majoritatea pentru a putea lucra cu adrese mai lungi). Principalele trăsături ale IPv6 sunt discutate mai jos. Mai multe informații despre el pot fi găsite in RFC 2460 până la RFC 2466.

În primul rând şi cel mai important, IPv6 are adrese mai lungi decât IPv4. Ele au o lungime de 16 octeți, ceea ce rezolvă problema pentru a cărei soluționare a fost creat IPv6: să furnizeze o sursă efectiv nelimitată de adrese Internet. În curând vom spune mai multe despre adrese.

A doua mare îmbunătățire a lui IPv6 este simplificarea antetului. El conține numai 7 câmpuri, (față de 13 in IPv4). Această schimbare permite ruterelor să prelucreze pachetele mai rapid, îmbunătățind astfel productivitatea şi întârzierea. De asemenea, vom discuta in curând şi antetul.

A treia mare îmbunătățire a fost suportul mai bun pentru opțiuni. Această schimbare a fost esențială în noul antet, deoarece câmpurile care erau necesare anterior sunt acum opționale. În plus, modul în care sunt reprezentate opțiunile este diferit, uşurând ruterelor saltul peste opțiunile care nu le sunt destinate. Această caracteristică accelerează timpul de prelucrare a pachetelor.

Un al patrulea domeniu în care IPv6 reprezintă un mare progres este în securitate. Autentificarea si confidențialitatea sunt trăsături cheie ale noului IP. Ulterior ele au fost adaptate şi în IPv4, astfel că în domeniul securității diferențele nu mai sunt aşa de mari.

În final, a fost acordată o mai mare atenție calității serviciilor. În trecut s-au făcut eforturi fără prea mare tragere de inimă, dar acum, o dată cu creşterea utilizării multimedia în Internet presiunea este şi mai mare.

13.2. Antetul principal IPv6

Antetul IPv6 este prezentat mai jos. Câmpul *Versiune* este întotdeauna 6 pentru IPv6 (şi 4 pentru IPv4). În timpul perioadei de tranziție de la IPv4, care va lua probabil mai mult de un deceniu, ruterele vor fi capabile să examineze acest câmp pentru a determina ce tip de pachet analizează. Ca un efect lateral, acest test iroseşte câteva instrucțiuni pe drumul critic, aşa încât multe implementări vor încerca să-l evite prin folosirea unui câmp din antetul legăturii de date ca să diferențieze pachetele IPv4 de pachetele IPv6. În acest mod, pachetele pot fi transmise direct rutinei de tratare de nivel rețea corecte. Cu toate acestea, necesitatea ca nivelul legătură de date să cunoască tipurile pachetelor nivelului rețea contravine complet principiul de proiectare care spune că fiecare nivel nu trebuie să cunoască semnificația biților care îi sunt dați de către nivelul de deasupra.

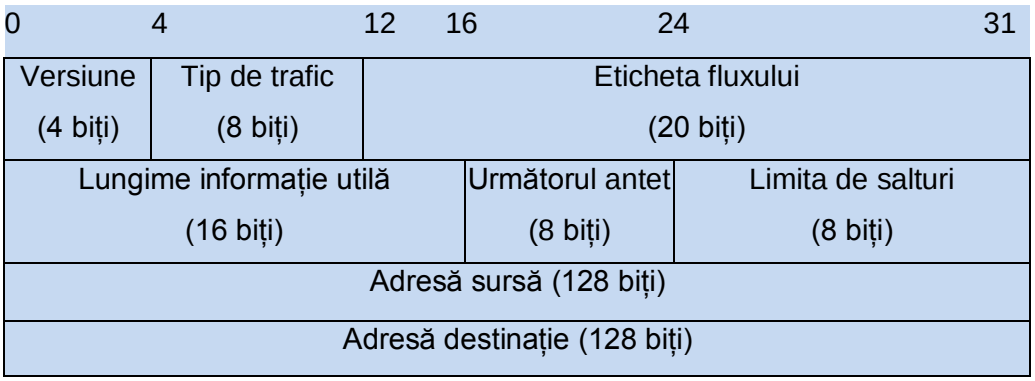

Figura 13-1 Antetul fix IPv6 (obligatoriu)

Câmpul *Tip de trafic* (*Traffic class*) este folosit pentru a distinge între pachetele care au diverse cerințe de livrare în timp real. Un câmp cu acest scop a existat in IP de la început, dar a fost implementat sporadic de către rutere. În acest moment se desfăşoară experimente pentru a determina cum poate fi utilizat cel mai bine pentru transmisii multimedia.

Câmpul *Eticheta fluxului* este încă experimental, dar va fi folosit pentru a permite unei surse şi unei destinații să stabilească o pseudo-conexiune cu proprietăți şi cerințe particulare. De exemplu, un şir de pachete de la un proces de pe o anumită gazdă sursă către un anumit proces pe o anumită gazdă destinație poate avea cerințe de întârziere stricte şi din acest motiv necesită capacitate de transmisie rezervată. Fluxul poate fi stabilit în avans şi poate primi un identificator. Când apare un pachet cu o *Eticheta a fluxului* diferită de zero, toate ruterele pot să o caute in tabelele interne pentru a vedea ce tip de tratament special necesită. Ca efect, fluxurile sunt o încercare de a combina două moduri: flexibilitatea unei subrețele cu datagrame şi garanțiile unei subrețele cu circuite virtuale.

Fiecare **flux** este desemnat de adresa sursă, adresa destinație şi numărul de **flux,** aşa încât, între o pereche dată de adrese IP pot exista mai multe fluxuri active in acelaşi timp . De asemenea, in acest mod, chiar dacă două fluxuri venind de la gazde diferite, dar cu acelaşi număr de **flux** trec prin acelaşi ruter, ruterul va fi capabil să le separe folosind adresele sursă şi destinație. Se aşteaptă ca numerele de flux să fie alese aleator, în loc de a fi atribuite secvențial începând cu 1, pentru că se aşteaptă ca ruterele să le folosească în tabele de dispersie.

Câmpul *Lungimea informației utile* spune câți octeți urmează după antetul de 40 de octeți din figura. Numele a fost schimbat față de câmpul Lungime totală din IPv4 deoarece semnificația este uşor modificată: cei 40 de octeți nu mai sunt parte a lungimii (aşa cum erau înainte).

Câmpul *Antetul următor* dă de gol proiectanții. Motivul pentru care antetul a putut fi simplificat este că există antete de extensie suplimentare (opționale). Acest câmp spune care din cele şase antete (actuale) de extensie, dacă există vreunul, urmează după cel curent. Dacă acest antet este ultimul antet IP, câmpul Antetul următor spune cărui tip de protocol (de exemplu TCP, UDP) i se va transmite pachetul.

Câmpul *Limita salturilor* este folosit pentru a împiedica pachetele să trăiască veşnic. El este, în practică, identic cu câmpul Timp de viață din IPv4, şi anume un câmp care este decrementat la fiecare salt dintr-o rețea în alta. În teorie, în IPv4 era un timp în secunde, dar nici

un ruter nu-l folosea în acest mod, aşa încât numele a fost modificat pentru a reflecta modul în care este de fapt folosit.

Apoi urmează câmpurile *Adresă sursă* şi *Adresă destinație*. După multe discuții,s-a decis că adresele cu lungime fixă de 16 octeți sunt cel mai bun compromis.

13.3. Adrese IPv6

Pentru scrierea adreselor de 16 octeți a fost inventată o nouă notație. Ele sunt scrise ca opt grupuri de câte patru cifre hexazecimale cu semnul: (două puncte) între grupuri, astfel:

8000:0000:0000:0000:0123:4567:89AB:CDEF

Din moment ce multe adrese vor avea multe zerouri în interiorul lor, au fost autorizate trei optimizări. Mai întâi, zerourile de la începutul unui grup pot fi omise, astfel încât 0123 poate fi scris ca 123. În al doilea rând, unul sau mai multe grupuri de 16 zerouri pot fi înlocuite de o pereche de semne două puncte (:). Astfel, adresa de mai sus devine acum

8000::123:4567:89AB:CDEF

Probabil că nu este necesar să fim atât de expliciți asupra acestui lucru, dar există o mulțime de adrese de 16 octeți. Mai exact, sunt 2^{128} adrese, care reprezintă aproximativ 3×10^{38}. Dacă întreaga planetă, pământ şi apă, ar fi acoperite cu calculatoare, IPv6 ar permite 7×10^{23} adrese IP pe metru pătrat.

Exista trei tipuri de adrese: (http://www.faqs.org/rfcs/**rfc4291**.html)

Unicast: Un identificator pentru o singura interfața. Un pachet trimis către o adresa unicast este livrat interfeței identificata prin acea adresa.

Anycast: Un identificator pentru un set de interfețe (de regula aparținând unor noduri diferite). Un pachet trimis către o adresa anycast este livrat doar uneia dintre interfețe (de regula cea mai apropiata conform metricii date de protocolul de rutare)

Multicast: Un identificator pentru un set de interfețe (de regula aparținând unor noduri diferite). Un pachet trimis către o adresa multicast este livrat tuturor interfețelor identificate prin acea adresa.

Nu exista adrese de broadcast ca la IPv4 funcția fiind preluata de adresele multicast.

Tip adresa	Prefix binar	Notatie IPv6
Nespecificat	00...0 (128 bits)	::/128
Loopback	00...1 (128 bits)	::1/128
Multicast	11111111	FF00::/8
Link-local unicast	1111111010	FE80::/10
Global unicast	Orice altceva	

13.3.1. Adrese IPv6 speciale

Bucla locala ::1 – datagramele trimise pe aceasta destinație sunt livrate local fiind tratate ca pachete primite

Adresa nespecificata 0::0 – folosita atunci când o interfața nu-si cunoaşte adresa

Link-local – pot fi folosite doar pe o legătura fizica, nefiind rutabile

Site-local – pot fi folosite doar in cadrul unei organizații (similare adreselor private IPv4)

Structura generala a unei adrese unicast globale este următoarea:

n biţi	m biți	128-n-m (de regula 64 biţi)
Prefix global de rutare	ID subrețea	Identificator interfața

unde prefixul global de rutare (având o structura ierarhica) este o valoare atribuita unui site (o colecție de subretele/legături), ID-ul subrețelei este reprezintă un identificator pentru o legătura din cadrul site-ului iar Identificatorul interfeței identifică in mod unic o interfața de rețea ataşata la acea legătura având de regula 64 de biți fiind stabilit pornind de la adresa de nivel 2 a interfeței.

În practică, spațiul de adrese nu va fi folosit eficient, însă chiar şi in cel mai pesimist scenariu, vor fi totuşi mult peste 1000 de adrese IP pe metru pătrat de suprafață planetară (pământ sau apă). În orice scenariu credibil, vor fi trilioane de adrese pe metru pătrat. Pe scurt, pare improbabil că vom epuiza adresele in viitorul previzibil. Este instructiv să comparăm antetul IPv4 cu antetul IPv6 pentru a vedea ce fost eliminat in IPv6. Câmpul IHL a dispărut pentru că antetul IPv6 are o lungime fixă. Câmpul *Protocol* a fost scos pentru că în câmpul *Antetul următor* se indică ce urmează după ultimul antet IP .(exemplu, un segment TCP sau UDP).

Toate câmpurile referitoare la fragmentare au fost eliminate, deoarece IPv6 are o abordare diferită a fragmentării. Pentru început, toate gazdele şi ruterele care sunt conforme cu IPv6 trebuie să determine dinamic mărimea datagramei care va fi folosită. Această regulă face ca, de la început, fragmentarea să fie mai puțin probabilă. Este mult mai eficient să obligi gazdele să trimită de la bun început pachete corecte dimensional, decât să obligi ruterele să le fragmenteze din mers.

Câmpul *Suma de control* este eliminat deoarece calculul acesteia reduce mult performanțele. Datorită rețelelor fiabile folosite acum, combinate cu faptul că nivelurile de legătură de date şi de transport au în mod normal propriile sume de control, valoarea a încă unei sume de control nu merita prețul de performanță cerut.

În sfârşit, câmpul *Opțiuni* nu mai face parte din antetul standard IPv6. Cu toate acestea opțiunile nu au dispărut. Câmpul opțiuni reprezintă unul din posibilele antete următoare. La fel cum antetele segmentelor TCP sau UDP pot reprezenta următorul antet dintr-o datagramă IP, tot aşa pot urmă şi câmpuri de opțiuni.

13.4. Antetele de extensie IPv6

Întrucât opțiunile din antetul IPv4 joacă un rol important în funcționarea protocolului această facilitate a fost menținută şi la IPv6. Pe de altă parte având în vedere impactul opțiunilor IPv4 asupra performanței, mecanismul IPv6 de tratare a opțiunilor a fost modificat semnificativ. Opțiunilor a fost eliminate din antetul principal, funcționalitatea fiind implementată prin antete adiționale denumite antete de extensie. Antetul principal are întotdeauna o dimensiune fixă (40 de octeți), antetele de extensie fiind adăugate atunci când este necesar. Acestea sunt plasate între antetul principal şi antetul protocolului de nivel superior încapsulat de datagrama IPv6. O datagramă IPv6 poate include zero) , unul sau mai multe antete de extensie.

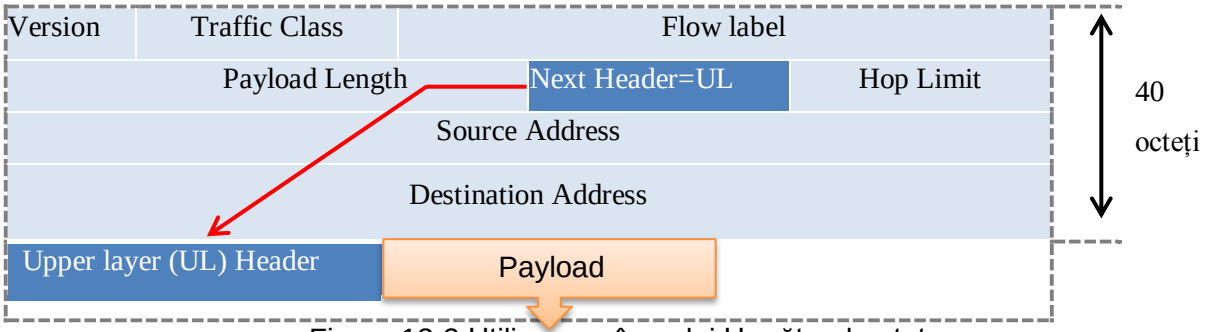

Figura 13-2 Utilizarea câmpului Următorul antet

Figura de mai jos prezintă modul în care sunt înlănțuite antetele. Aceste antete pot furniza informații suplimentare, codificate într-o manieră eficientă. Până în acest moment au fost definite mai multe antete de extensie, existând posibilitatea ca pe viitor să fie definite şi altele. Unele antete

au o dimensiune fixă, altele conțin un număr variabil de opțiuni de lungime variabilă codificate sub forma (Tip, Lungime, Valoare).

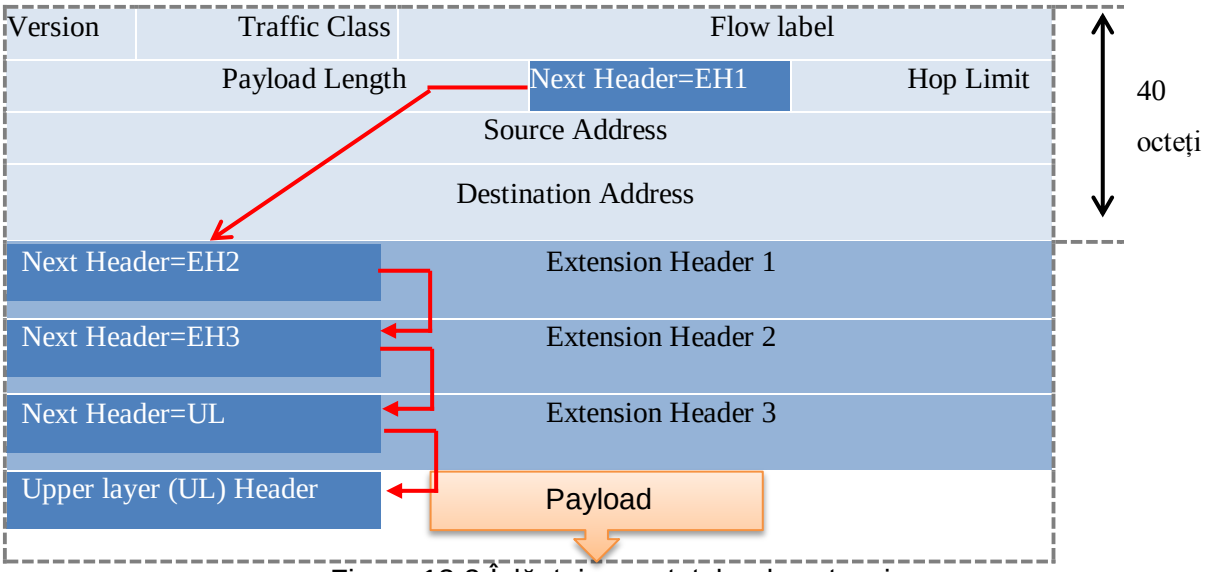

Figura 13-3 Înlănțuirea antetelor de extensie

13.5. Tranziția de la IPv4 la IPv6

După parcurgea detaliilor tehnice ale IPv6, să avem în vedere o chestiune foarte practică: cum va efectua Internetul public, bazat pe IPv4, tranziția la IPv6. Problema este că deşi noile sistemele IPv6 pot fi făcute compatibile cu IPv4 astfel încât să poată trimite, ruta şi recepționa datagrame IPv4, sistemele IPv4 deja existente nu sunt capabile să manipuleze datagrame IPv6. Sunt posibile mai multe opțiuni.

O posibilitatea ar fi declararea unei zile în care toate maşinile din Internet vor fi oprite şi actualizate de la IPv4 la IPv6. Ultima tranziție majoră în tehnologie (de la utilizarea NCP la utilizarea TCP pentru transport fiabil) a avut loc acum mai mult de 25 de ani. Chiar şi atunci [RFC 801], când Internetul era minuscul şi administrat de un număr mic de „magicieni", s-a ajuns la concluzia că o astfel de zi este imposibilă. O zi dedicată tranziției ce implică sute de milioane de maşini şi milioane de administratori de rețea şi utilizatori este inimaginabilă actualmente. RFC 4213 descrie două abordări (ce pot fi utilizate împreună sau separat) pentru integrarea graduală a ruterelor şi gazdelor IPv6 în rețeaua IPv4 (cu obiectivul pe termen lung ca toate nodurile să migreze la IPv6).

Probabil cel mai simplu mod de a introduce noduri IPv6 este abordarea bazată de stivă-dublă, unde nodurile IPv6 dispun de o implementare IPv4 completă. Un astfel de nod, referit ca nod IPv6/IPv4 în RFC 4213, poate trimite şi recepționa atât datagrame IPv4 cât şi datagrame IPv6. Atunci când interoperează cu un nod IPv4, nodul IPv6/IPv4 poate utiliza datagrame IPV4; când interoperează cu un nod IPv6 va folosi datagrame IPv6. Nodurile IPv6/IPv4 trebuie să dispună atât

de adresă IPv6 cât şi de adresă IPv4. În plus nodurile cu stivă dublă trebuie să determine dacă corespondentul este compatibil IPV6 sau doar IPv4. Această problemă poate fi rezolvată folosind DNS-ul, care va returna o adresă IPv6 dacă nodul este compatibil IPv6 sau, altfel va returna o adresă IPv4. Desigur dacă nodul care formulează cererea este compatibil doar cu IPv4 atunci DNS-ul va returna doar adresa IPv4.

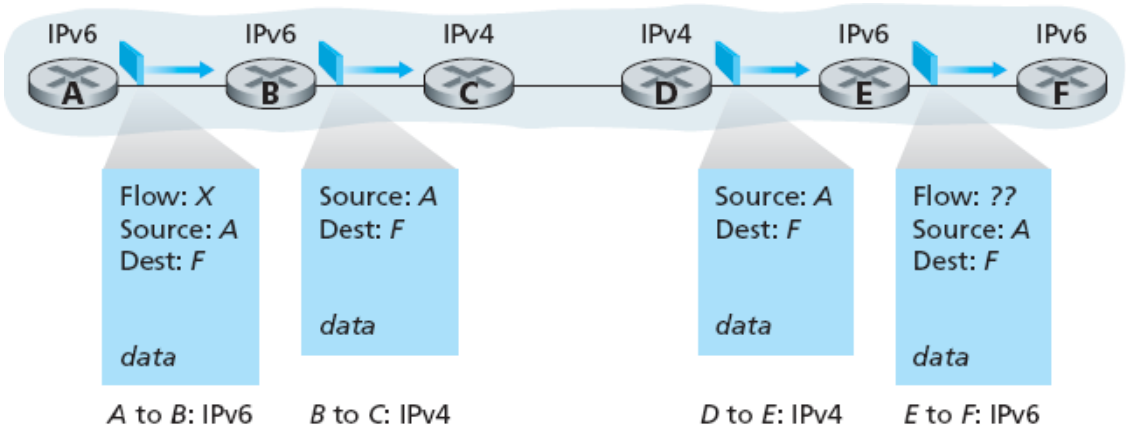

Figura 13-4 Abordarea cu stivă dublă

În cazul stivei duble, dacă fie emiţătorul, fie receptorul este compatibil doar cu IPv4, atunci se vor folosi datagrame IPv4. În consecinţă, este posibil ca două noduri compatibile IPv6 să sfârşească prin a comunica folosind IPv4. Situaţia este ilustrată în Figura 13-4. Să presupunem că nodul A este compatibil IPv6 şi doreşte să trimită o datagramă nodului F, care este de asemenea compatibil IPv6. Nodurile A şi B pot comunica folosind IPv6, însă nodul B trebuie să comunice cu C folosind IPv4. În mod evident încărcătura utilă a datagramei IPv6 ar putea fi copiată într-o datagramă IPv4, făcându-se şi o mapare corespunzătoare a adreselor. Cu toate acestea, la efectuarea conversiei de la IPv6 la IPv4, vor exista anumite câmpuri din antetul IPv6 (spre ex. eticheta fluxului), care nu au corespondent la IPv4. Informaţia din aceste câmpuri s-ar pierde. Astfel, deşi E şi F pot comunica prin datagrame IPv6, datagramele sosite la E de la D nu vor conţine toate câmpurile din datagrama originală creată de A.

O alternativă la stiva dublă, discutată în RFC 4213 este cunoscută sub denumirea de tunelare. Tunelarea poate rezolva problema de mai sus, permiţând spre exemplu ca E să obţină datagrama IPv6 creată de A. ideea de bază din spatele tunelării este următoarea: Să presupunem că două noduri (spre exemplu B şi E) doresc să interopereze folosind datagrame IPv6 dar sunt conectate prin intermediul unor rutere IPv4. Vom referi ruterele IPv4 interpuse între ruterele IPv6 ca tunel, aşa cum este ilustrat în Figura 13-5. Folosind tunelarea, nodul emiţător de la capătul tunelului (spre ex. B) preia întreaga datagramă IPv6 şi o încapsulează în câmpul informaţie utilă al datagramei IPv4.

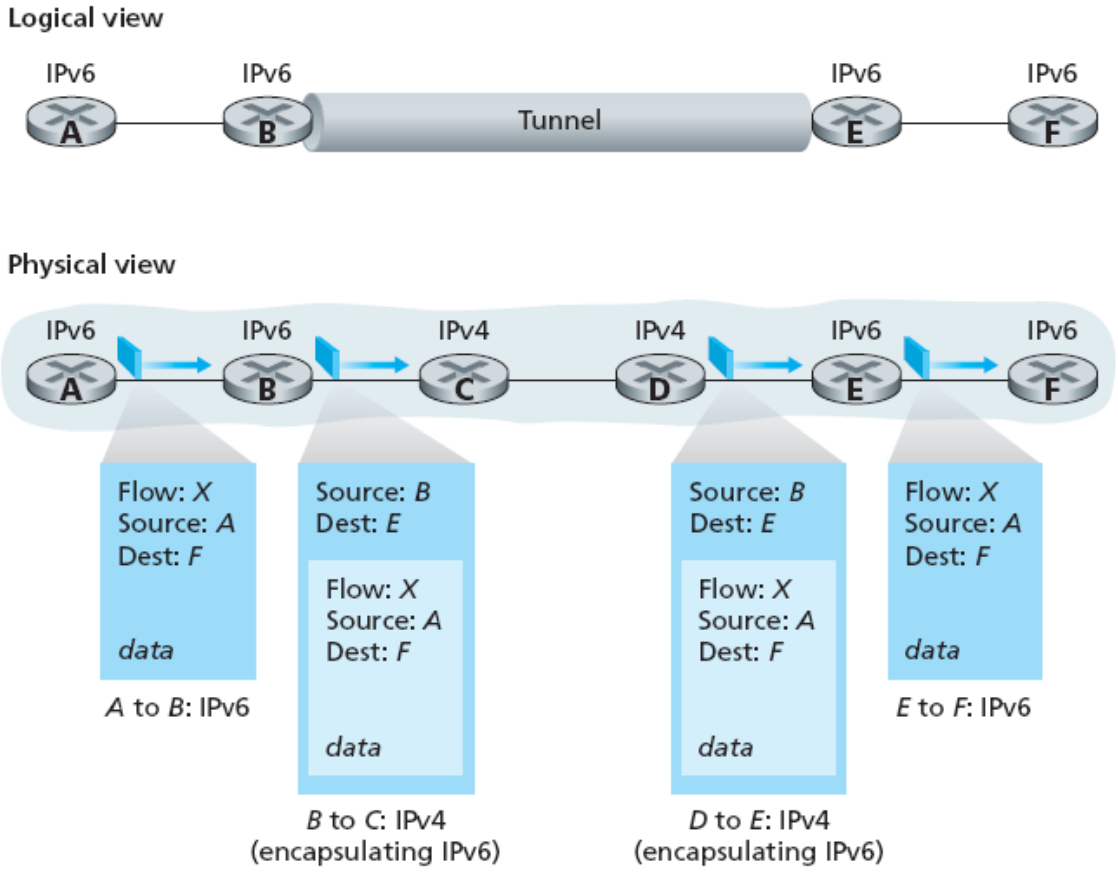

Figura 13-5 Tunelare

Această datagramă IPv4 este apoi adresată nodului IPv6 de la capătul receptor al tunelului (spre ex. E) şi trimisă primului nod in tunel (spre ex. C). Ruterele IPv4 interpuse rutează datagrama IPv4, ca pe orice altă datagramă, fără să intereseze faptul că aceasta conține o datagrama IPv6 încapsulată. Nodul IPv6 de la capătul receptor al tunelului va recepționa eventual datagrama IPv4 (el fiind destinația datagramei IPv4), va determina că aceasta conține o datagrama IPv6, va extrage datagrama IPv6 şi apoi va ruta datagrama IPv6 ca şi când aceasta a fost recepționată de la un vecin IPv6.

13.6. Autoconfigurarea adreselor IPv6

Deşi dezvoltarea Internetului a fost impresionantă, unul dintre factorii care inhibat acceptarea rapidă a tehnologiei a fost faptul că conectarea unui dispozitiv la Internet necesitata o unei vastă experienţe de administrare a sistemului. Mai exact, fiecare gazdă care este conectată la Internet, necesită configurarea unei adrese IP valide, a unei măşti de rețea, a adresei unui ruter implicit şi adresei unui server DNS. In aceste condiții nu e posibilă, despachetarea unui calculator nou şi conectarea acestuia la Internet fără o preconfigurarea prealabilă. Unul dintre obiectivele IPv6 este şi asigurarea suportului pentru autoconfigurare, referit şi ca operare *plug-and-play*.

Este posibilă şi o autoconfigurare pentru IPv4, însă aceasta depinde de existența unui server care transmite adresele şi alți informații de configurare către clienții DHCP (Dynamic Host Configuration Protocol, RFC 1531). Lungimea mai mare a adreselor IPv6, permite implementarea unei noi forme de autoconfigurare denumită autoconfigurare *stateless*, care nu depinde de existența unui server.

Reamintim că adresele IPv6 unicast sunt ierarhice, şi cea mai puțin semnificativă porțiune este ID-ul interfeței. Astfel, putem subdiviza problema autoconfigurării in două etape:

- Obținerea unui identificator de interfață care este unic pe legătura unde este ataşată gazda
- Obținerea prefixului pentru subrețea.

Prima parte este relativ simplă, întrucât fiecare interfață de rețea dispune de o adresă de nivel doi unică. Spre exemplu toate gazdele de pe un segment Ethernet dispun de o adresă unică pe 48 de biți. Aceasta poate fi transformată într-o adresa link-local validă prin adăugarea prefixului corespunzător (1111 1110 10) urmat de zerouri până la 128 de biți.

Dispozitivele care necesită o adresă unică global depind de existența unui ruter care anunță periodic prefixul subrețelei. Aceasta necesită ca ruterul să fie configurat cu prefixul corect, iar prefixul este ales astfel încât să existe suficient spațiu la sfârşit (48 de biți) pentru ataşarea adresei de nivel doi. De regulă prefixele au 64 de biți iar adresa identificatorul interfeței se formează conform schemei de mai jos.

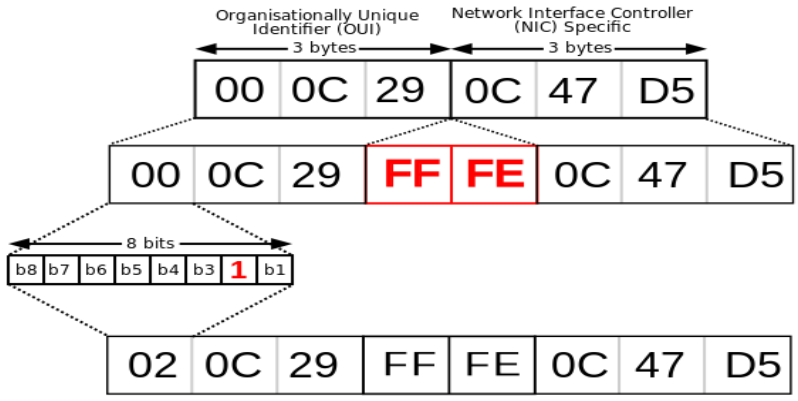

Figura 13-6 Crearea ID-ului de interfață pornind de la adresa MAC

13.7. Concluzii

Deşi adoptarea IPv6 a fost lentă la început, actualmente ritmul de adoptare s-a accelerat semnificativ (http://www.google.com/ipv6/statistics.html). Proliferarea unor dispozitive cum ar fi telefoane IP sau alte dispozitive portabile a pus presiune asupra implementării IPv6.

O lecție importantă ce poate fi învățată din experiența IPv6 este următoarea: este enorm de dificil să se modifice protocoalele de nivel rețea. De la începutul anilor 90, au fost anunțate multe noi protocoale de nivel rețea ca reprezentând următoarea revoluție majoră din Internet, însă majoritatea acestor protocoale au fost implementate la o scară redusă până acum. Aceste protocoale includ protocoalele IPv6 multicast şi protocoalele de rezervare a resurselor. Introducerea unor noi protocoale de nivel rețea este similară înlocuirii fundației unei case – dificil de realizat fără relocarea temporară a locatarilor. Pe de altă parte, se remarcă o dezvoltare rapidă a protocoalelor de nivel aplicație. Exemplele clasice sunt, desigur, Web-ul, mesageria instantă şi partajarea peer-to-peer. Alte exemple includ streaming-ul audio şi video şi jocurile distribuite. Introducerea unor noi protocoale de nivel aplicație este similară înlocuirii zugrăvelii dintr-o casă, este relativ simplu iar dacă alegi o culoare atractivă vecinii vor proceda la fel. În concluzie, putem asista în viitor la modificări ale nivelului rețea din Internet, însă aceste schimbări se vor produce cel mai probabil, mult mai lent decât schimbările de la nivelul aplicație.

Rezumat

IPv4 este utilizat intens de mai mult de 30 de ani. Acesta a funcționat foarte bine, fapt demonstrat prin creşterea exponențială a Internetului. Cu toate acestea IPv4 a devenit o victimă a propriei sale popularități, fiind pe cale să-şi epuizeze spațiul de adrese. Soluția pe termen lung este trecerea la adrese mai lungi. IPv6 este un proiect de înlocuire a IPv4 care pe lângă extinderea spațiului de adrese, optimizează şi alte câteva caracteristici ale IP-ului curent. IPv6 utilizează adrese pe 128 de biți; o epuizare a acestui spațiu de adrese nu e predictibilă actualmente. În ciuda cestor îmbunătățiri, IPv6 s-a dovedit dificil de implementat. Este un protocol de rețea diferit, incompatibil cu IPv4, deşi există o serie de similarități. Soluțiile de tranziție de la IPv4 la IPv6 sunt stiva dublă şi tunelarea.

Bibliografie

James F. Kurose and Keith W. Ross, *Computer Networking A Top Down Approach*, 5/E, Pearson Education, 2009

Larry L. Peterson, Bruce S. Davie, Computer Networks – a systems aproach, Elsevier, 2012

A. Tanenbaum, *Rețele de calculatoare* , Ed. Byblos, ed. a IV-a, 2004

RFC4291 - *IP Version 6 Addressing Architecture*, http://www.faqs.org/rfcs/rfc4291.html