NOUL PROTOCOL IPv6

Tema are ca scop cunoaşterea noului protocol IPv6, a caracteristicilor sale, a modului de configurare şi utilizare a acestui protocol de rețea.

După parcurgerea acestei teme, studentul va cunoaşte:

- Caracteristicile principale ale IPv6
- Adresarea IPv6 (formate de adresă, tipuri de adrese, scopul şi aplicabilitatea diverselor tipuri de adrese)
- Modurile de configurarea a adreselor IPv6 pe echipamente de rețea
- Antetul pachetului IPv6 şi comparația cu IPv4
- Rutarea în rețelele IPv6
- Metode şi tehnici de tranziție între IPv4 şi IPv6

Cuprins

- Necesitatea unui nou protocol IP
- Caracterisricile IPv6
- Pachetul IPv6 şi câmpurile sale
- Adresarea IPv6
- Strategii nde tranziție între IPv4 şi IPv6
- Configurarea IPv6 pe sisteme de operare

1. Necesiatea unui nou protocol IP

IETF (*Internet Engineering Task Force*) a început în anul 1990 să lucreze la o nouă versiune de IP care:

- să dispună de un spațiu de adrese practic nelimitat (care să nu se termine nici peste sute de ani)
- să reducă, pe cât posibil, dimensiunea tabelelor de routare

- să asigure o securitate (autentificare şi confidenţialitate) mai bună faţă de actuala versiune IP
- să simplifice protocolul, astfel încât routerele să poată procesa mai eficient pachetele de date
- să acorde o mai mare atenţie tipului de serviciu (de ex. Datele aplicaţiilor de timp real să aibă prioritate mai mare)
- să faciliteze trimiterea multiplă prin permiterea specificării de domenii,
- să permită o flexibilitate mai mare a protocolului, astfel încât îmbunătăţirile viitoare să se facă într-un timp cât mai scurt
- să creeze condiţiile pentru ca un host să poată migra în alte spaţii geografice, fără schimbarea adresei sale
- să permită coexistenţa noului şi vechiului protocol pentru câţiva ani

2. Caracteristici ale protocolului IPv6

IP versiunea 6 sau *IP Next Generation* (***IPng***) este noua versiune a Protocolului Internet (IP). Acesta substituie în mod progresiv actuala versiune IPv4 a protocolului de nivel reţea pe baza căruia a funcţionat şi încă mai funcţionează Internetul.

IPv6 a fost proiectat în primul rând pentru a extinde actuala problemă a spaţiului de adrese care devine insuficient şi pentru asigurarea creşterii în număr a reţelelor pe glob prin cei 128 biţi lungime a adresei IP. Ca urmare, spaţiul de adrese se măreşte la:

2^{128}-1 = 340282366920938463463374607431768211455 adrese IP!!!!

Câteva din specificaţiile îmbunătăţite, noi ale IPv6:

- **Configurare "plug-and-play".**
- **Routare/manipulare mai eficientă.**
- **Identificare prin "flow label" a unei conexiuni.**
- **Mecanism de securitate.**
- **Descoperirea vecinilor**
- **Mobilitate.**
- **Posibilitatea unei tranziţii optime de la IPv4 la IPv6.**

Atâta timp cât stivele de protocoale IPv6 şi IPv4 nu pot interopera în mod direct, au fost introduse standarde de compatibilităţi între IPv4 şi IPv6 care se realizează prin posibilitatea de "tunelări" a unui protocol în celălalt astfel încât IPv6 să poată fi transportat de exemplu prin reţeaua IPv4.

3. Formatul antetului IPv6 vs. IPv4

În figura 1 se observă antetul IPv4 comparativ cu antetul IPv6 din care rezultă că:

- unele câmpuri au fost păstrate (cu unele denumiri schimbate)
- unele câmpuri au dispărut
- unele câmpuri s-au mutat în headere opționale

Headerul IPv6 are 40 de octeți si este reprezentat în figura de mai jos.

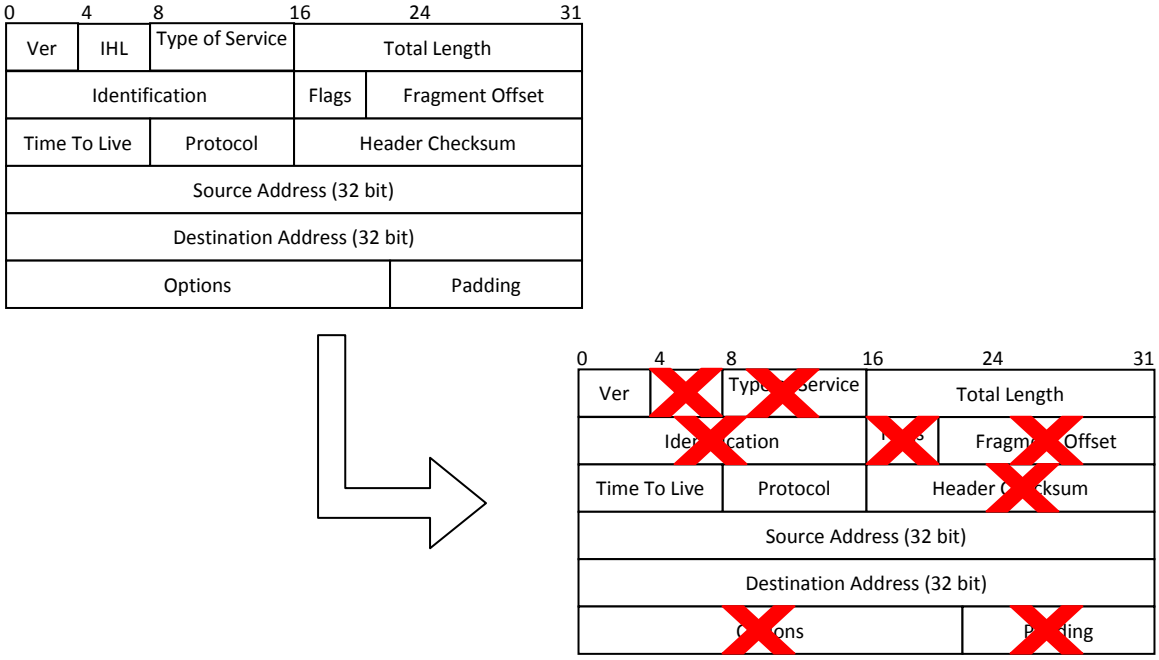


Figura 1 – Modificari aduse antetului IPv6

3.1 Descrierea câmpurilor antetului IPv6

Version

Acest grup de 4 biți sunt: 0110 (=6) şi indică versiunea de protocol. Acelaşi grup într-un pachet IPv4 sunt setați la: 0100 (=4) adică pachetele astfel marcate sunt distinse de către stiva sistemului de operare care le va interpreta.

Traffic Class

Acest număr pe 8 biți specifică **prioritatea pachetului**. IPv6 împarte traficul în două categorii: ***'congestion-controlled'*** şi ***'non-congestion controlled'***. Traficul de tip congestion-controlled **poate fi întârziat dacă traficul e congestionat** (supraîncărcat) pe când traficul de tip non-congestion controlled nu e permis să fie controlat în nici o situație de congestie ca urmare nu se permite nici un fel de aruncare a pachetelor la o congestie.

Traficul de tip 'non-congestion controlled' se pretează cu aplicații de tip real-time cum ar fi cele audio şi video.

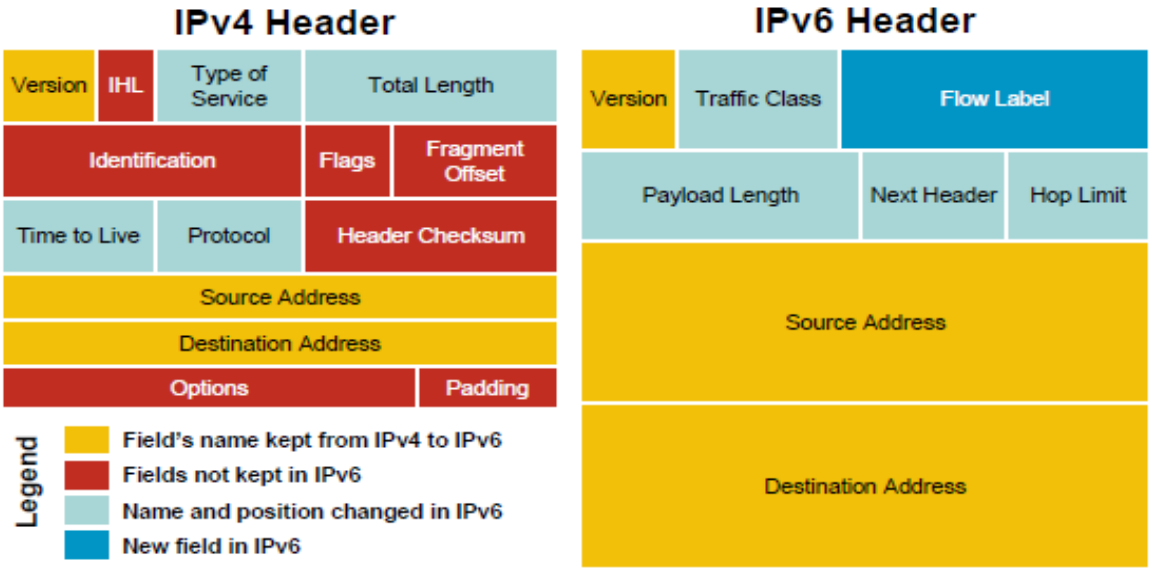


Figura 2 - Antetul IPv6 aliniat pe 64 de biti

Valori ale priorităților 0-7 sunt asociate traficului de tip 'congestion-controlled traffic' după tabelul de mai jos:

0	Nu se specifică nici o prioritate
1	Trafic neimportant – ex. news
2	Transfer date mărunt – ex. e-mail
3	Rezervat
4	Transfer de tip 'bulk' – ex.. FTP
5	Reservat
6	Traffic interactive – ex. remote logins
7	Control trafic - ICMP, SNMP, informații de rutare

Flow Label[1]

Aceşti 20 de biți sunt identificatorii unui "flux" de date de la un punct la altul. Acesta permite **posibilitatea rutării unui trafic particular prin rute particulare** atât timp cât aceasta valoare e vizibilă tuturor ruterelor intermediare prin care parcurg. Acesta poate simplifica jobul ruterelor, ruterele fiind capabile de o urmărire a unui trafic particular sursă/destinație.

Deocamdată în actualele implementații IPv6 Flow Label-ul este experimental.

Payload Length[2]

[1] Flow label – Câmp în antetul IPv6 (descries în RFC 3697)
[2] Payload Length - Câmp în antetul IPv6(descries în specificatiile IPv6 - RFC 2460)

Această valoare de 16 biți indică mărimea volumului de date atașat după header ce necesită a fi transportat. Această valoare adunată cu mărimea headerului 10x32 biți dă mărimea efectivă a pachetului IP.

Next Header[3]

Acesta în mare parte e similar câmpului protocol din IPv4 şi defineşte tipul transportului. (udp, icmp…).

Fiecare opțiune are un header. Valorile codate pe 8 biți pot fi:

0	Hop-by-Hop Options Header
4	Internet Protocol
6	Transmission Control Protocol (TCP)
17	User Datagram Protocol (UDP)
41	Encapsulated IPv6 Header
43	Routing Header
44	Fragment Header
45	Interdomain Routing Protocol
46	Resource Reservation Protocol
50	Encapsulating Security Payload
51	Authentication Header
58	Internet Control Message Protocol (ICMPv6)
59	No Next Header
60	Destination Options Header

Hop Limit

Această valoare determină cât de departe poate să ajungă o datagramă mai exact câte routere poate să strabată. În IPv4 se cheamă TTL (*Time To Live*) şi a fost introdus pentru a preveni un pachet să circule la infinit în Internet. Valoarea este decrementată cu o unitate de fiecare nod care retrimite pachetul. Când valoarea ajunge la 0 se renunță la pachet. Deoarece valoarea câmpului este pe 8 biți, numărul maxim de noduri pe care un pachet îl poate străbate este 255.

Source Address

[3] Next Header - Câmp în antetul IPv6(descries în specificatiile IPv6 - RFC 2460)

Indică adresa de origine a pachetului.

Destination Address

Indică adresa de destinație a pachetului.

Modificări aduse antetului

- **lungimea adreselor a fost mărită la 128 biți**
- **câmpurile opționale şi cel care specifică fragmentarea pachetelor au fost eliminate**
- **a fost eliminat câmpul care conținea suma de control a headerului**

  Motivația ar putea fi următoarea:
  - în zilele noastre legăturile de date sunt mai bune
  - nivelele superioare (de ex. TCP, UDP, ICMPv6) realizează calculul sumei de control
- **a fost eliminat câmpul care conținea lungimea antetului (acestea au lungime fixă)**
- **a fost introdus un câmp nou, flow label**
- **unele câmpuri au fost redenumite**
  - ToS (Type of Service) → Traffic Class
  - Protocol → Next Header
  - Time to Live → Hope limit
- **aliniamentul a fost modificat la 64 de biți**
- **a fost îmbunătățit suportul pentru headere suplimentare**

3.2 Extensii de antete IPv6 (Extension Headers[4])

Sunt **headere suplimentare** ce pot apare în pachete IPv6 conform unei structuri standard.

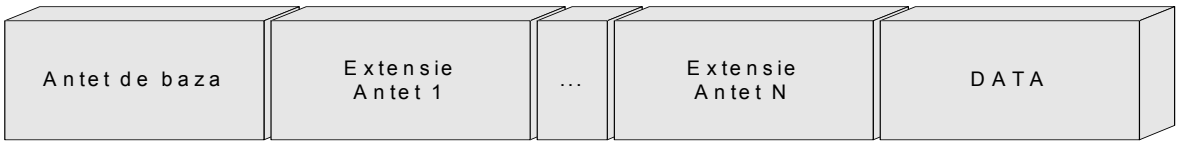


Figura 3 – Extensii de antete IPv6

Avantajele obținute sunt următoarele:

- numărul şi dimensiunea headerelor suplimentare **sunt nelimitate**
- headerele suplimentare au **numere de ordine** pentru a simplifica procesarea în routere
- se poate defini comportamentul în cazul opțiunilor necunoscute / nesuportate
- mai puține câmpuri în antetul principal ceea ce realizează o **procesare mai rapidă** a acestuia

[4] Extension header - Descris în specificațiile IPv6 - RFC 2460

- creşte eficienţa deoarece
  - headerele suplimentare sunt **procesate numai când sunt prezente**
  - majoritatea opțiunilor sunt **procesate numai la destinație**

Headerele opționale definite până în prezent sunt:

- **Hop-by-Hop Option header**

Headerul Hop-by-Hop Option trebuie procesat de fiecare nod prin care trece pachetul. Formatul este prezentat în figura de mai jos, în care trebuie specificat că lungimea câmpului *option* poate varia. Astfel, lungimea sa trebuie specificată în câmpul *header ext length*.

Next header	header ext length	
options		

Figura 4 – Option header

Formatul câmpului *option* este ilustrat în figura următoare: fiecare opțiune trebuie să înceapă cu un câmp de 8 biți în care se specifice tipul, urmat de un câmp de 8 biți pentru lungime.

Option type	Option data length	Option data

Figura 5 – Option

Opțiunile care pot implica toate nodurile de pe traseu sunt în general asociate cu funcții de management şi depanare.

Până în prezent au fost definite următoarele opțiuni:

- două tipuri de opțiuni folosite pentru a asigura **aliniamentul pe 64 de biți** (*type=0)*
- opțiunea ***Payload jumbogram*** *(type=194)*, descrisa de RFC 2675
- opțiunea **Router Alert**, descrisă de RFC 2711

- **Destination Options header**

Formatul este asemănător cu al headerului suplimentar hop-by-hop. Este singurul header suplimentar care poate apărea de două ori în acelaşi pachet, în două poziții diferite. Dacă este **plasat înainte de headerul de rutare** va fi **procesat de primul nod** care apare în câmpul destinație al antetului IPv6. În toate celelalte cazuri este vizibil numai la destinație.

- **Routing header**[5]

Antetul rutare este folosit de o sursă pentru **a găsi toate nodurile pe care un pachet trebuie să le traverseze** pentru a ajunge la destinație. Este identificat printr-o valoare a câmpului

[5] Routing header - Descries în specificatiile IPv6 - RFC 2460

next header egală cu 43 în headerul imediat anterior. Formatul acestui header suplimentar este prezentat în figura de mai jos:

Next header	hdr ext len	Routing Type	Segment Left
type-specific data			

Figura 6 – Routing header

Când este folosit acest tip de header de rutare, headerul inițial IPv6 conține prima adresă din listă ca adresă destinație. La fiecare hop, nodul intermediar o înlocuieşte cu următoarea din listă şi decrementează valoarea câmpului *Segment Left*

Next header	hdr ext len	Routing Type=0	Segment Left
Reserved			
Address [1]			
...			
Address [n]			

Figura 7 – Routing header cu adresele de destinatie

- **Fragmentation header**[6]

Una din inovațiile introduse de IPv6 este **eliminarea fragmentării** pachetelor la trecerea prin noduri. Cu noul protocol, **fragmentarea este administrată la capete prin intermediul unui header suplimentar**.

Dacă pachetul este prea mare pentru a încăpea în MTU maxim pentru legătura pe care pachetul trebuie trimis, nodul il abandonează şi trimite un mesaj de eroare ICMP înapoi la sursă. Dacă o datagramă trebuie trimisă şi a cărei încărcare depăşeşte dimensiunea permisă pentru legătură, în funcție de valoarea MTU, IPv6 permite sursei să fragmenteze pachetul. Folosind antetul pentru fragmentare i se permite destinației să reasambleze corect pachetele.

Next header	Reserved	Fragment Offset	Res	M
Identification				

Figura 8 – Fragmentation header

Fiecare pachet consistă dintr-o parte nefragmentabilă şi o parte fragmentabilă.

Parte nefragmentabilă	Parte fragmentabilă

Figura 9 – Fragmentation header cu parte nefragmentabila si parte fragmentabila

[6] Fragmentation header - Descries în specificatiile IPv6 - RFC 2460

Partea nefragmentabilă include headerul IPv6 şi celelalte headere care trebuie procesate de fiecare nod şi trebuie repetate identic pentru fiecare pachet. Sunt două excepţii: este necesar a se actualiza câmpul *payload length* şi câmpul *Next Header* din ultimul fragment, care trebuie să indice că antetul de fragmentare este prezent.

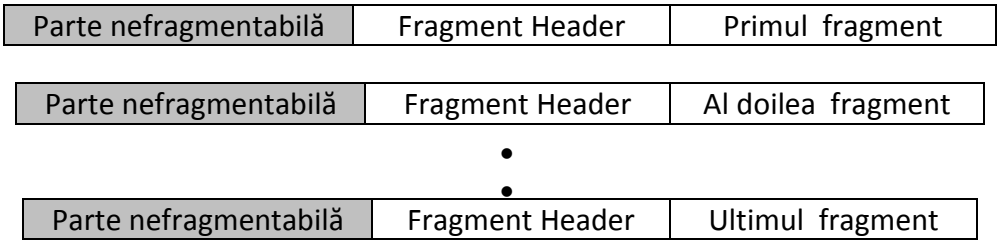


Figura 10 – Antetul de fragmentare

- **Authentication header şi Encapsulating Security Payload header**

IPv6 furnizează un **serviciu standard de autentificare şi criptare end-to-end** prin intemediul a două headere opţionale.

Antetul de autentificare (AH = Authentication Header) este proiectat pentru a garanta autenticitatea şi integritatea pachetului în care este plasat sau, cu alte cuvinte, pentru a verifica dacă acel pachet a fost modificat pe drum sau a fost generat de cineva care nu este autorizat să acceseze resursa respectivă.

Pe de altă parte, **antetul pentru criptare** (ESP = Encapsulating Security Payload) pune la dispoziţie un mecanism pentru procesarea datelor în aşa fel încât acestea să nu poată fi citite decât la sfârşitul rutei.

În ambele cazuri, sursa şi destinaţia trebuie să se înţeleagă în privinţa cheii secrete şi a algoritmului utilizat, dar şi a valorilor care să fie atribuite parametrilor ulteriori. Împreună, această informaţie formează aşanumită **Security Association** , sau **SA**, identificată prin câmpul **SPI** (*security parameter index*) împreună cu adresele sursă şi destinaţie.

Negocierea unei asocieri securizate (SA) este o parte completă a protocolului de interschimbare a cheii.

Implementările IPv6 trebuie să suporte algoritmul MD5 pentru autentificare şi controlul integrităţii şi DES_CBC ca algoritm de criptare. Deoarece specificaţiile nu sunt dependente de aceşti algoritmi, alte tehnici pot fi utilizate o dată ce asocierea securizată a fost stabilită.

ESP este antetul opţional care poartă parametri şi cheile utilizate pentru criptare de la un cap la celălalt (end-to-end). Când este utilizat, trebuie să fie al doilea header din lanţ deoarece el ascunde complet nivelul următor de date şi antetele următoare.

Sunt două soluţii posibile:

- modul transport
- modul tunel

În primul caz doar încarcătura (datele) pachetului IPv6 sunt criptate.

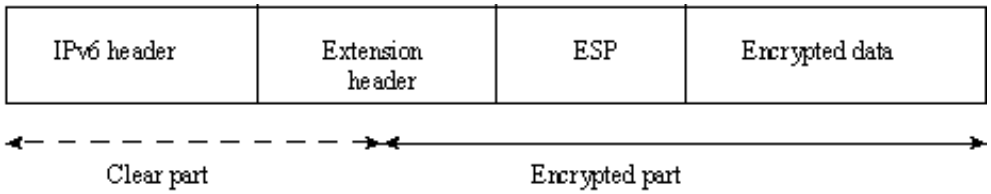


Figura 11 – Criptarea pachetelor IPv6

Dacă este necesar un grad mai ridicat de securitate, este posibil a se utiliza modul tunel, în care întregul pachet este criptat şi apoi incapsulat în alt pachet. În acest fel este vizibil doar la capăt, ceea ce măreşte eficienţa criptării dar se măreşte şi overhead-ul (cantitatea de informaţie nefolositoare)

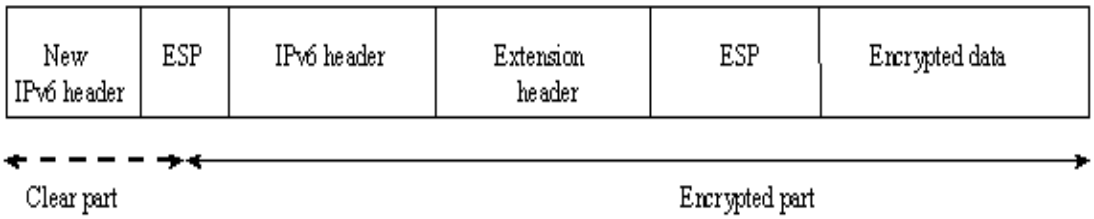


Figura 12 – Criptarea IPv6 folosind modul tunel

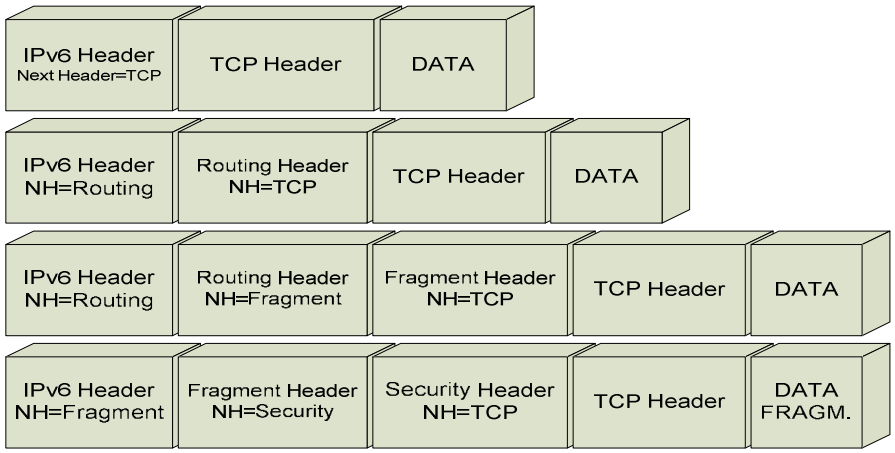


Figura 13 – Exemple de pachete IPv6

3.3 Fragmentarea pachetelor în IPv6

Versiunea 6 a protocolului Internet interzice fragmentarea pachetelor în reţea. Va exista doar aşanumita fragmentare ***End-to-End***. Aceasta presupune ca doar sursa poate realiza fragmentarea. Routerele NU vor fragmenta.

Headerul unui fragment este următorul:

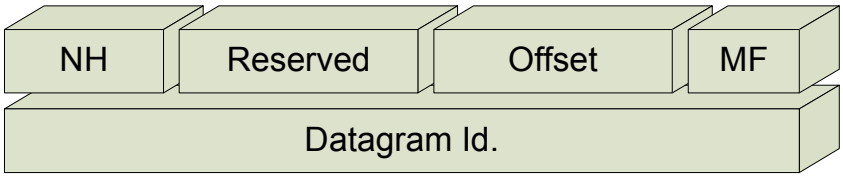


Figura 14 – Headerul unui fragment

Mecanismul de fragmentare a fost descris anterior .

3.4 Suportul IPv6 pentru QoS

Două câmpuri din header au legătură cu QoS

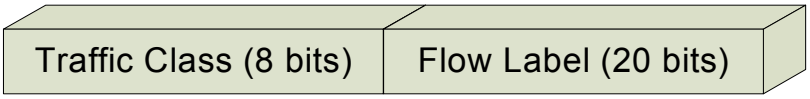


Figura 15 – Campuri din header pentru QoS

- Traffic Class
  - Oferă suport pentru servicii diferențiate (RFC 2474)
  - Corespunde câmpului ToS de la IPv4
- Flow Label
  - Permite o clasare eficientă a fluxului IPv6 bazată numai pe câmpuri din pozitii fixe ale headerului de bază IPv6

4. Mesaje de Control în IPv6 (ICMPv6)

ICMPv6 (*Internet Control Message Protocol*) este relatat identic pentru IPv6 ca şi cum ICMPv4 (RFC792) este relatat pentru IPv4. Primele 10 cuvinte a unui header ICMPv6 sunt identice cu următoarele 10 cuvinte ale IPv4 urmat de un câmp cu valoarea 58 ce defineşte tipul protocolului (*icmpv6*). În continuare este urmat de un nou câmp în care avem valoarea cod a mesajului în sine şi doi octeți de checksum aşa se găseşte în RFC 1885.

1	Mesaj de eroare pentru destinație inexistentă
2	Mesaj de eroare pentru dimensiune prea mare a pachetului
3	Mesaj de eroare pentru expirare timp
4	Mesaj de eroare pentru problemă parametru
128	Mesaj pentru cerere ecou
129	Mesaj pentru reply ecou

130	Interogare membru grup
131	Raport membru grup
132	Group membership termination
133	Solicitare router
134	Anunțare router
135	Solicitare vecin
136	Anunțare vecin
137	Redirecționare mesaj

În plus față de funcționalitățile ICMP original (mesaje de eroare şi diagnostic), ICMPv6 oferă cadrul pentru:

- **Autoconfigurare**
- **Rezoluții de adresa (Neighbor Discovery)**
- **Path MTU Discovery**
  - proces ce utilizează mesaj pentru dimensiune prea mare a pachetului (*Packet Too Big Message*) pentru a realiza transmisia pachetelor IPv6 cu dimensiuni mai mari de 1280 bytes.
- **Detecția adreselor duplicate** (DAD)
- **IPv6 mobility**

5. Neighbour Discovery

Definit in RFC 2461, este similar protocolului **ARP** în IPv4. Este utilizat de nodurile IPv6 de pe aceeaşi legătură pentru

- A descoperi prezența fiecăruia
- A determina adresele nivelului legăturii de date ale fiecăruia
- A descoperi routere
- A menține informații despre disponibilitatea şi despre calea către fiecare vecin activ

Înlocuieşte ARP, ICMPv4 Router Discovery şi ICMPv4 Redirect.

Elimină utilizarea broadcast-ului pentru rezoluția adreselor (utilizare inteligentă a multicastului). Ca răspuns la o solicitare/interogare putem avea mesajele:

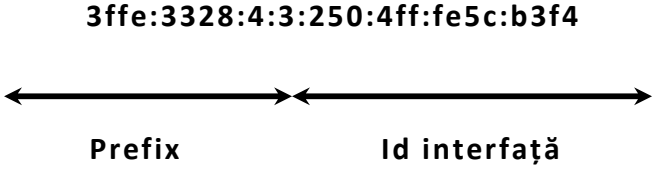
0	No route to destination
1	Communication prohibited
2	Not a neighbour (strict routing failure)
3	Not a neighbour (strict routing failure)
4	Port unreachable

Pentru o solicitare "*neighbour*" putem avea valorile 0 sau 4 în funcție dacă avem de a face cu un router sau un host.

6. Adresarea în IPv6

6.1 Reprezentarea textuală a adreselor

Din cauza lungimii mari, reprezentarea unei adrese IPv6 este îngreunată, astfel că se foloseşte numerotația hexazecimală, reprezentarea standard a unei adrese IPv6 fiind:



Structura adresei este următoarea:

Adresa Ipv6 = Prefix + Id Interfață

- **Prefixul depinde de topologia retelei**
- **Id-ul identifică o interfață**

6.2 Tipuri de adrese IPv6

1. **Adrese unicast** – identifică o singură interfață din interiorul unui grup (scope) de tipuri de adrese. **Scopul** (**domeniul**) de adrese este o regiune de rețea IPv6 în care adresele sunt unice. Pachetele trimise unei adrese unicast sunt livrate unei singure interfețe.
2. **Adrese multicast** – identifică zero sau mai multe interfețe. Pachetele trimise spre o adresă multicast, într-o topologie adecvată de rutare multicast sunt livrate tuturor interfețelor identificate de adresa multicast.
3. **Anycast** – identifică mai multe interfețe.

Adrese unicast sunt de următoarele tipuri:

- Agregabile global (Aggregatable global unicast addresses)
- Local-link
- Site-local
- Speciale
- De compatibilitate (Compatibility addresses)

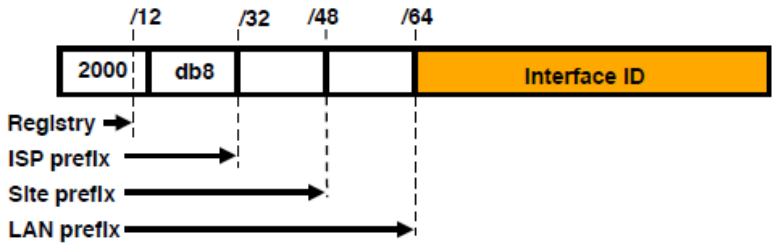
- NSAP

Type	Binary	Hex
Unspecified	000…0	::/128
Loopback	000…1	::1/128
Global Unicast Address	0010	2000::/3
Link Local Unicast Address	1111 1110 10	FE80::/10
Unique Local Unicast Address	1111 1100 1111 1101	FC00::/7
Multicast Address	1111 1111	FF00::/8

Fig. 16 Tipuri de adrese IPv6

Adrese unicast agregabile global

Sunt numite şi **adrese globale** şi sunt identificate prin **prefixul 001** FP (FP- formatul prefixului). În hexa 001x înseamnă că prima cifră este 2 sau 3, adică primul grup de 4 cifre hexa se întinde de la **2000 la 3FFF.**



Sunt echivalente adreselor publice IPv4. Sunt rutabile global în Internet şi pot fi atinse orinde în Internet. Permit agregarea (sumarizarea) în rețele ierarhice şi asigură o infrastructură eficientă de rutare. Spre deosebire de Internet IPv4 care este o combinație de tehnici de rutere ierarhice şi plate, Internetul IPv6 a fost gândit de la început să suporte adresare şi rutare ierarhică, eficientă. Domeniul (scope) adreselor unicast globale este întregul Internet.

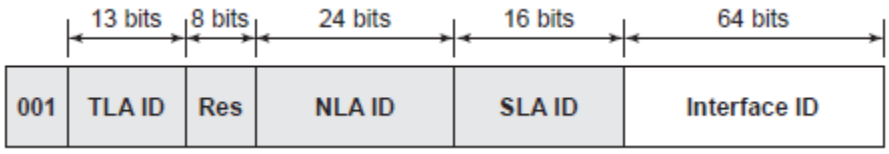


Fig. 17 Structura adresei unicast agregabilă global

Câmpurile din structura acestui tip de adresă sunt:

TLA ID – Top-Level Aggregation Identifier are lungimea de 13 biți şi identifică cel mai înalt nivel în ierarhia de rutare.

ID-urile TLA sunt administrate de IANA şi sunt alocate registrilor Internet locali care, la rândul lor, alocă ID-uri TLA individuale la ISP-uri mari, capabili de transport de date pe distanțe mari. Cei 13 biți permit existența a 8 192 de ISP-uri diferiți de TLA. Ruterele din nivelul de top de rutare în Internet (denumite rutere default-free) nu au o rută default.

Res – sunt biti rezervați expandarea în viitor, fie a TLA IDs, fie a NLA IDs.

NLA ID – Next-Level Aggregation Identifier are lungimea de 24 biți. Acest nivel permite ISP-istilor să creeze nivele multiple de ierarhii de adresare în interiorul rețelei proprii, atât pentru adresarea si rutarea ISP-istilor descendenți (downstream), cît şi identifiarea site-urilor organizaționale. Structura rețelei unui ISP nu este vizibilă spre ruterele default.

SLA ID – Site-Level Aggregation Identifier este folosit de o organizație individuală pentru a identifica sbrețelele din interiorul său. Câmpul are 16 biți, astfel că se pot organiza 65 536 de subrețele, care pot fi structurate ierarhic pe mai multe niveluri si crea o intrastructură de adresare si rutare eficientă. Structura rețelei de organizație nu este vizibilă de către ISP –ul lui.

Interface ID – indică o interfață pe o subrețea specificată. Are 64 de biți şi corespunde unui identificator de nod sau de gazdă din IPv4.

Adresarea globală prin structura de adresă unicast globală crează o structură topologică de rețea cu trei niveluri.

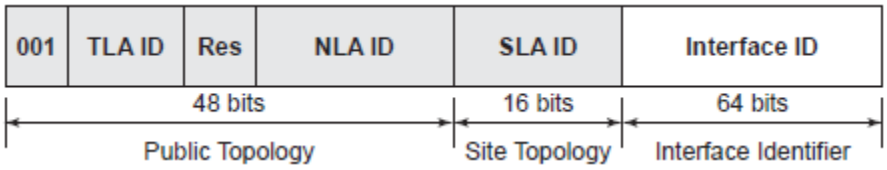


Fig.18 Structura topologică a adresării globale

Topologia publică este o colecție de rețele ISP mai mari sau mai mici care asigură acces la Internet. Topologia subrețea este o colecție de subrețele în interiorul unei organizații (site). Identificatorul de interfață specifică o interfață unică pe o subretea din interiorul unei organizații.

Adrese unicast de uz local (Local-use Unicast Addresses)

Există două tipuri de adrese unicast de uz local:

1. **Adrese link-local** – folosite de vecinii conectați pe un link şi pentru procesul de descoperire a vecinilor.

2. **Adrese site-local** folosite de nodurile care comunică cu alte noduri în acelaşi site

Adresele link-local sunt identificate prin formatul de prefix 1111 1110 10 (**FE80::/10**). Sunt folosite de noduri care comunică pe acelaşi link. Domeniul (scope) unde se aplică aceste adrese este un link local (din interiorul unui site). De exemplu, pe o retea IPv6 cu un singur link, fără ruter, hosturile comunică pe baza acestei adrese. Adresele link-local sunt echivalente adreselor APIPA (Automatic Private IP Addressing) din IPv4 autoconfigurate pe Microsoft Windows Server 2003, Windows XP, etc.

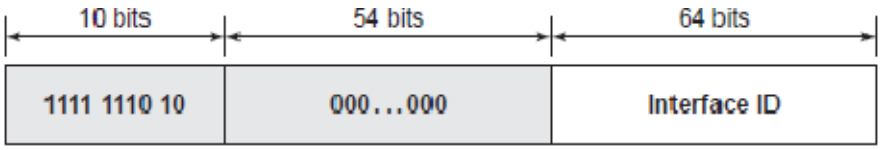


Fig. 19 Structura adresei link-local

Adresa link începe intotdeauna cu FE80 si are prefixul de retea FE80::/64. Un ruter nu va ruta niciodată o asemenea adresă.
Adresa link local se mai foloseşte în procesul de descoperire a vecinilor şi este automat configurată în absența unei alte adrese unicast. (se va discuta ulterior la autoconfigurarea adreselor).
Adresele site-local sunt identificate cu FP **1111 1110 11** (**FEC0::/10**) si **sunt echivalente adreselor private** din IPv4: 10.0.0.0/8, 172.16.0.0/16, 192.168.0.0/24. De exemplu, rețelele private care nu au legătură direct, rutată la Internet v6 pot folosi adrese site-local fără a intra în conflict cu adrese globale. Domeniul (scope) adreselor site-local este site-ul local. Ele nu pot fi trimise în alte situri si nu pot fi primite din alte site-uri.

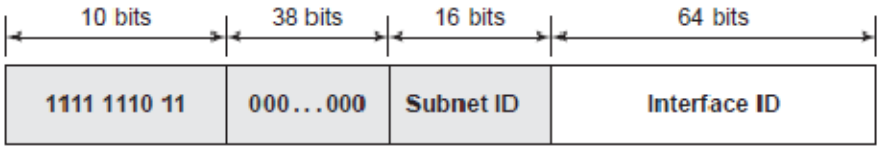


Fig. 20 Structura adresei site-local

Adrese IPv6 speciale

Adresa nespecificată este de forma 0:0:0:0:0:0:0:0 sau :: şi indică lipsa orcărei adrese. Este folosită ca adresă a sursei când aceasta încă nu a fost determintă.

Adresa de buclă locală este de forma 0:0:0:0:0:0:0:1 sau ::1 si identifică o interfață folosită ca buclă locală. Ea permite unui nod să-ți trimită pachete lui însuşi. Este echivalentă adresei loopback 127.0.0.0 din IPv4. Packetele trimise pa acastă adresă nu vor fi transmise pe un link sau înaintate unui ruter.

6.3 Compatibilitatea adreselor IPv6 cu IPv4

Pentru a ajuta migrarea de la IP4 la IP6 si coexistența lor au fost definite următoarele adrese.

- **Adrese IPv6 definite din adrese IPv4**
  0:0:0:0:0:0:w.x.y.z, unde w.x.z.y este reprezentarea zecimală a unei adrese publice IPv4. Este folosită de nodurile IPv6/IPv4 care comunică cu IPv6 peste o infrastructură care foloseşte IPv4, cum ar fi Internet
- **Adrese IPv4 mapate în adrese IPv6**
  Sunt de forma 0:0:0:0:0:w.x.y.z sau echivalent ::ffff:w.x.y.z si sunt folosite pentru a reprezenta adresa unui nod IPv4 în format IPv6
- **Adrese 6over4**
  Sunt de forma <prefix de 64 biți>0:0:WWXX:ZZYY unde WWXX:ZZYY este reprezentarea hexazecimală a adresei IPv4 publice sau private W.X.Y.Z. Se foloseşte pentru gazdele ce aplică **mecanismul de tunelare** cunoscut ca **6over4**.

  Altă formă de adresă 6over4 este următoarea:
  <prefix de 64 biți>:WWXX:ZZYY:<SKA ID>:<Interface ID>. Se foloseşte în acelaşi context
- **Adrese ISATAP**
  Sunt de forma <prefix de 64 biți>:0:5EFE:w.x.y.z unde w.x.y.z este o adresă IPv4 publică sau privată a unui nod ce foloseşte mecanismul Intra_site Automatic Tunneling Addressing Protocol (ISATAP).

Adrese IPv6 multicast

Traficul multicast în IPv6 operează asemănător cu IPv4. Noduri IPv6 arbitrar locate pot asculta pentru trafic multicast pe orice adrese multicast IPv6. Nodurile se pot asocia sau dezasocia orcând de la un grup multicast.
Formatul de prefix multicast este 1111 1111, adică începe cu FF. El continuă cu 4 biți flag si 4 biti scope.
Flags - indică prin ultimul bit (bitul T transient) durata adresei multicast. T=1 arată că adresa este transitorie (nepermanentă), pe când T=0 arată o adresă permannetă.

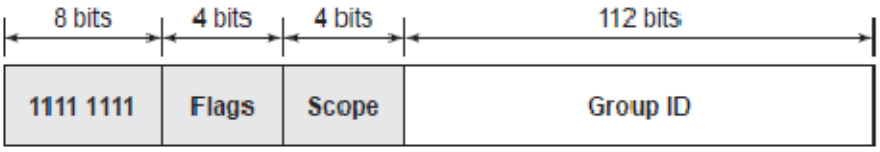


Fig. 21 Structura adresei IPv6 multicast

Scope – indică scopul (extinderea) rețelei IPv6 pentru care se intenționează livrarea de trafic multicast. De asemenea dacă traficul poate fi fowardat sau nu. De exemplu, o adresă multicast de forma FF02::2 are un scop link-local. Un ruter nu va forwarda niciodată traficul dincolo de linkul local.

Scope Field Value	*Scope*
0	Reserved
1	Node-local scope
2	Link-local scope
5	Site-local scope
8	Organization-local scope
E	Global scope
F	Reserved

Group ID identifică membrii grupului multicast si este unic în interiorul unui scop. ID-urile de grup asignate permanent sunt independente de scop. Cele tranzitorii au relevanță doar intr-un scop specificat.
Pentru a identifica toate nodurile cu scopuri nod-local şi link-local, au fost definite următoarele adrese:

- FF01::1 (scop nod-local toate nodurile adresă multicast)
- FF02::1 (The link-local scope all-nodes multicast address)
- FF01::2
- FF02::2
- FF05::2

Adrese multicast recomandate
Cu cei 112 biți se pot forma 2^{112} ID-uri de grup. Practic se recomandă ca ultimii 32 de biți să fie pentru group ID.

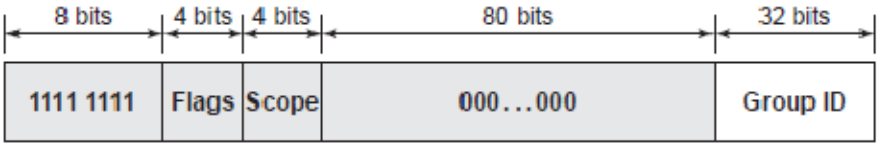


Fig. 22 Structura recomandată pentru adresele multicast

Adrese IPv6 anycast

O adresă anycast este atribuită mai multor interfețe. Pachetele trimise către o adresa anycast sunt livrate de structura de rutare spre cea mai apropiată interfață care are atribuită o astfel de adresă. Pentru a facilita livrarea, infrastuctura de rutare trebuie informată (be aware) despre interfețele

care au adrese anycast si distanța lor în termeni de metrică de rutare. Această informare (awareness) este realizată prin propagarea rutelor gazdă prin structura de rutare a porțiunii de rețea care nu poate sumariza adresa anycast utilizând un prefix de rutare.

Adresele anycast nu au un format special, ele pot fi adrese de tip unicast si devin „automat" anycast atunci când sunt atribuite mai multor interfețe. La configurarea unei interfețe cu o adresă anycast, acest lucru se specifică prin cuvântul cheie anycast

```
interface tunnel 0
  tunnel mode ipv6ip 6to4
  tunnel source ethernet1
  ipv6 address 2001:0db8:1::1/64
  ipv6 address 2002:0db8:6301::/128 anycast
```

Conform PRFC 2373 o adresă anycast poate fi doar adresă destinație (nu sursă) şi asignate numai pe rutere. Adresele anycast sunt atribuite din spațiul de adrese unicast şi scopul uneie adrese anycast este acelaşi cu al tipului de adresă unicast de la care a fost asignat. Nu este posibil să se determine dacă o adresă unicast dată este si o adresă anycast. Doar nodurile care au fost prevenite sunt rutere care folosesc rute host pentru a forwarda traficul anycast spre cel mai apropiat membru al unui grup anycast.

Adresa anycast pentru ruter de subrețea

Este creată din **prefixul de subrețea al unei interfețe** date, restul de biți fiind zero. Toate interfețele unui ruter ataşat la o subrețea au asignată adresa anycast de ruter de subrețea. Este folosită pentru a comunica cu cel mai apropiat ruter conectat pe o subretea specificată. Când este costruită o adresă anycast de subrețea, biții din perfixul de subrețea rămân ficşi la valoarea lor specificată, iar restul sunt zero (a se vedea fig. de mai jos). Toate interfețele ruterului atasate la o subrețea au atribuită adresă anycast din acea subrețea.

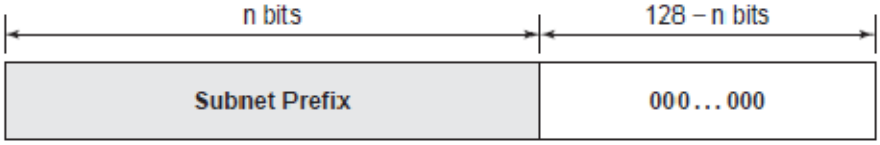


Fig.23 Structura adresei anycast pentru ruter de subrețea

Adrese IPv6 pentru un host

Un host IPv4 cu un singur adaptor de rețea are în mod tipic o singură adresă IPv4 ataşată adaptorului. Spre deosebire, un adaptor IPv6 are, în mod normal, mai multe adrese.
Pe **interfețele unui ruter IPv6 trebuie configurate** următoarele adrese:

- **Adresă link-local pe fiecare interfață**
- **Adrese unicast suplimentare pe fiecare interfață** (care poate fi adresă de site local sau una ori mai multe adrese unicast globale)
- **Adresa de loopback** (::1) pentru intefața loopback

În plus, **interfețele ruterului IPv6 ascultă pentru trafic pe următoarele adrese multicast**:

- Node-local scope all-nodes multicast address (FF01::1)
- Node-local scope all-routers multicast address (FF01::2)
- The link-local scope all-nodes multicast address FF02::1
- The link-local scope all-routers multicast address FF02::2
- The site-local scope all-routers multicast address FF05::2
- Solicited-node address for each unicast address
- Multicast addresses of joined group

7. Strategii de tranziție la IPv6

IPv6 nu este compatibil înapoi cu IPv4, astfel că trebuie făcută o schimbare de la IPv4 la IPv6, nu o upgradare.

Cerințele care se impun procesului de tranziție sunt:

- Internetul nu se poate opri
- Internetul este o rețea mare eterogenă în care nu există centralizare
- Interoperabilitatea v4-v6 este o necesitate, ceea ce presupune că IPv6 va fi o evoluție nu o revoluție

Aceste cerințe sunt îndeplinite deoarece IPv6 a fost proiectat având în vedere tranziția, ceea ce a făcut ca acesta să câştige în fața altor tehnologii alternative.

7.1 Tipuri de noduri

- **noduri care implementează numai IPv4**
  - Aceste noduri au numai adrese IPv4. Nu suportă IPv6. Majoritatea hosturilor şi ruterelor instalate în prezent sunt noduri numai IPv4

- **noduri care implementează numai IPv6**
  - Aceste noduri au numai adrese IPv6 şi pot comunica numai cu noduri şi aplicații IPv6. Acest tip de noduri nu este întâlnit în prezent dar va fi utilizat pentru dispozitive de dimensiuni reduse cum ar fi telefoanele celulare sau dispozitive de tip handheld care vor implementa stiva IPv6
- **noduri IPv6/IPv4**
  - Aceste noduri au implementate ambele protocoale IPv6 şi IPv4.
- Noduri IPv4
  - Acest nod implementează IPv4 (trimite şi recepționează pachete IPv4). Un nod IPv4 poate fi un nod numai IPv4 sau un nod IPv6/IPv4
- Noduri IPv6
  - Aceste noduri implementează protocolul IPv6 (trimit şi recepționează pachete IPv4). Un nod IPv6 poate fi un nod numai IPv6 sau un nod IPv6/IPv4

Migrarea este considerată realizată atunci când toate nodurile IPv4 sunt convertite la noduri IPv6. Însă, în mod practic, se poate considera migrarea realizată atunci când cât mai mult posibile noduri IPv4 vor fi convertite la IPv6 (în viziunea firmei Microsoft). Nodurile numai IPv4 pot comunica cu noduri numai IPv6, doar utilizând un **proxy IPv4-to-IPv6** sau un gateway de translație.

7.2 Mecanisme de coexistență

Se utilizează numai protocolul IPv6, astfel că nu este nevoie de compatibilitate. Aceasta presupune existența în paralel a unei alte rețele şi a altor aplicații. Reprezintă cea mai simplă modalitate de tranziție dar implică construirea unor noi rețele, crearea de noi aplicații, dar şi de noi piețe. Scenariile de tranzițiile referitoare la furnizorii de servicii internet (**ISP** = Internet Service Provider) implică realizarea de către aceştia, în paralel, a unei alte infrastructuri.

Pentru a coexista cu o infrastructură IPv4 şi pentru a realiza o eventuală migrare la o infrastructură bazată numai pe IPv6, următoarele mecanisme sunt utilizate:

- nivel IP dublu în stivă
- tunelare IPv6 prin IPv4
- infrastructura DNS

7.3 Nivel IP dual în stivă

Nivelul IP dual este o implementare a suitei de protocoale TCP/IP care include si un nivel Internet IPv4 şi un nivel Internet IPv6. Acesta este un mecanism folosit de nodurile IPv6/IPv4 pentru a comunica şi cu noduri IPv4, dar şi cu noduri IPv6.

Aceasta soluție nu implică nici o modificare fizică. În schimb trebuie portate aplicațiile, astfel incât să poată realiza atât conexiuni folosind IPv4 dar şi IPv6.

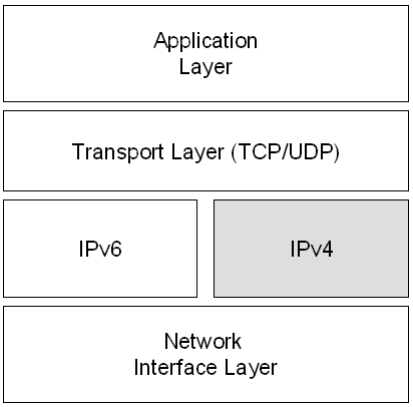


Figura 24 – Nivelul IP dual în stivă

7.4 Tunelare IPv6 prin IPv4

Tunelarea IPv6 prin IPv4 este încapsularea pachetelor IPv6 cu un header IPv4 astfel încât pachetele IPv6 să poată fi trimise printr-o infrastructură IPv4.

În interiorul headerului IPv4:

- câmpul ***Protocol*** din headerul IPv4 este setat la valoarea 41, care reprezintă un pachet IPv6 încapsulat.
- Câmpurile ***Sursă*** şi ***Destinație*** sunt setate la valorile IPv4 ale capetelor traseului.

Reprezentarea mecanismului de tunelare este următoarea:

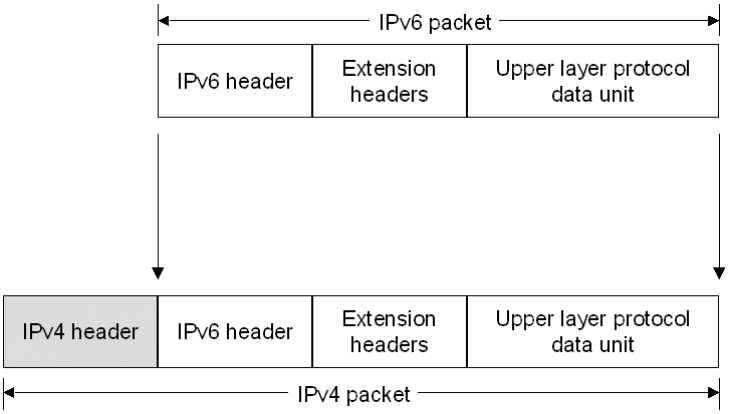


Figura 25 – Mecanismul de tunelare

Se utilizează următoarele tipuri de tuneluri, aşa cum este descris în RFC 2893:

- tuneluri configurate
- tuneluri automate

7.5 Tuneluri configurate

Un tunel configurat necesită configurarea manuală a capetelor tunelului. Într-un tunel configurat, adresele IPv4 ale capetelor nu sunt derivate din adresele codate în câmpurile de adresă şi destinaţie ale headerului IPv6 şi nici din adresa următorului hop de pe traseu. Nodurile din capetele tunelului trebuie să fie noduri cu stivă dublă. Adresele IPv4 ale capetelor tunelului trebuie să fie adrese externe (să nu existe NAT între nodurile din capete).

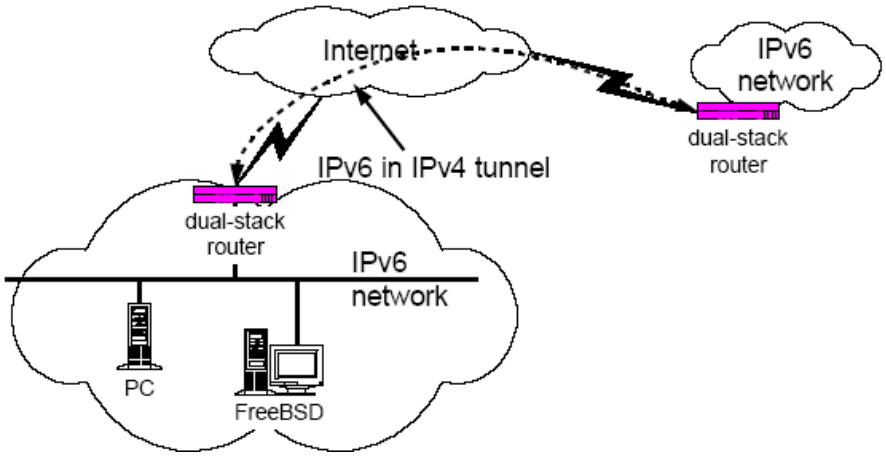


Figura 26 – Tuneluri configurate

7.6 Tuneluri automate

Un tunel automat este un tunel care nu necesită configurare manuală. Capetele tunelului sunt determinate de rută şi adresele sursă şi destinaţie IPv6. Nodului i se asignează o adresă compatibilă IPv4 (de ex. ::206.123.31.101). Dacă destinaţia este o adresă IPv4 compatibilă, tunelarea automată este utilizată.

În Windows Server 2003 sunt suportate următoarele tehnologii de tunelare automată:

- 6to4 (implicit activat)
  Nodurile IPv4 din capetele tunelului sunt identificate în prefixul domeniului IPv6. Prin acest procedeu routerul de ieşire al domeniului IPv6 crează un tunel către alt domeniu

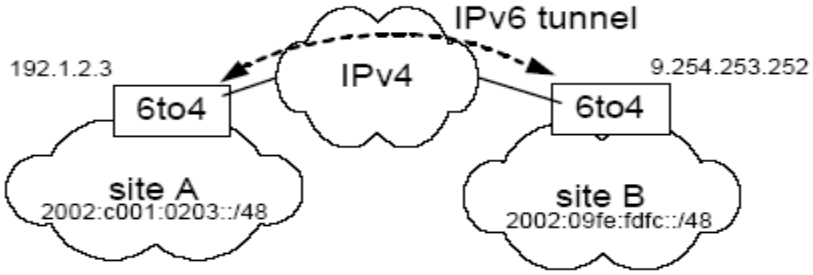


Figura 27 – Tuneluri automate

- ISATAP (implicit activat)
- tunelare IPv6 automată (implicit dezactivat)

- 6over4 (implicit dezactivat)
  Realizează interconectarea unor domenii IPv6 izolate în spațiul IPv4.

Alte tehnologii de tunelare:

7.7 Tunnel Broker

Conectează un host la rețeaua Inernet IPv6. Nodul client trebuie să fie dual stack (IPv4/IPv6) iar adresa IPv4 a clientului trebuie să fie rutabilă extern (nu prin NAT).

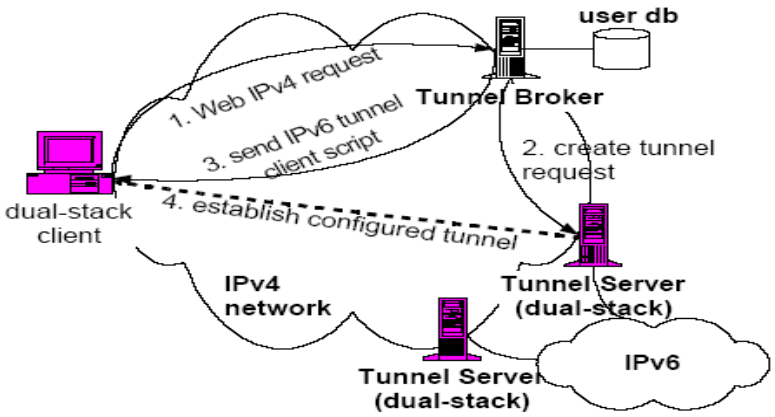


Figura 28 – Tunel Broker

8. Tunnel Server

Pe site-ul ***http://www.freenet6.net*** se găseşte un concept pentru IPv6. Este oferit suport IPv6 Plug-and-Play utilizănd pentru transport nivelul Internet IPv4 curent.

- Este furnizată conectivitate IPv6 la cerere
- Asignează o adresă IPv6 hostului
- Conectează hostul la rețeaua Internet IPv6

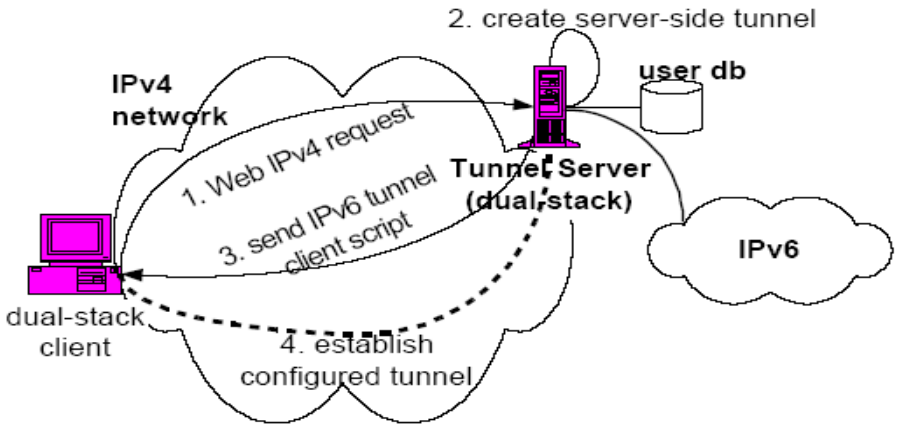


Figura 29 – Tunel Server

9. Implementări ale protocolului IPv6 în sistemele de operare

9.1 Instalarea şi configurarea protocolului IPv6 în Windows VISTA şi Windows 7

La fel ca în protocolul IPv4 în protocolul IPv6 se pot folosii un server DHCPv6 pentru alocarea adreselor IPv6 automat sau se pot introduce adresele şi manual. Folosind comanda netsh se pot face toate setările dorite, această opțiune nu foloseşte interfața grafică (GUI).

Pentru vizualizarea adreselor IPv6 în Windows 7 se da comanda:

- ***netsh interfaces ipv6 show address***

Pentru configurarea adreselor IPv6 în modul manual folosind interfața grafică (GUI) se poate, urmând paşi de mai jos.

a. Autentificarea cu drepturi de administrator pe calculator.
b. Deschide *Network and Sharing Center* şi se alege opțiunea *Change adapter settings*
c. Click dreapta pe *Local area connection* şi se selectează *Properties*
d. Selectați *Internet Protocol Versiunea 6* şi selectați *Properties*
e. Se introduce adresa de IPv6 dorită, în exemplul de mai jos este *2340:AAAA:1111:1::100*
f. Se introduce prefixul rețelei, în exemplul de mai jos este 64
g. Daca este cazul se introduce şi o poartă (gateway) pentru a avea accesa şi în alte rețele
h. Se apasa tasta OK şi se inchid şi celelalte ferester deschise anterior (*Local area connection, Network and Sharing Center*).
i. Pentru a testa noua adresă configurată folosi comanda *ping* , suntem nevoiți să configurăm si regulile de gestionare a traficului ICMP prin sistemul de protecție al calculatorului (firewall). Din command prompt tastați:
   - ***netsh advfirewall firewall add rule name="ICMPv6" protocol=icmpv6:any dir=in action=allow***

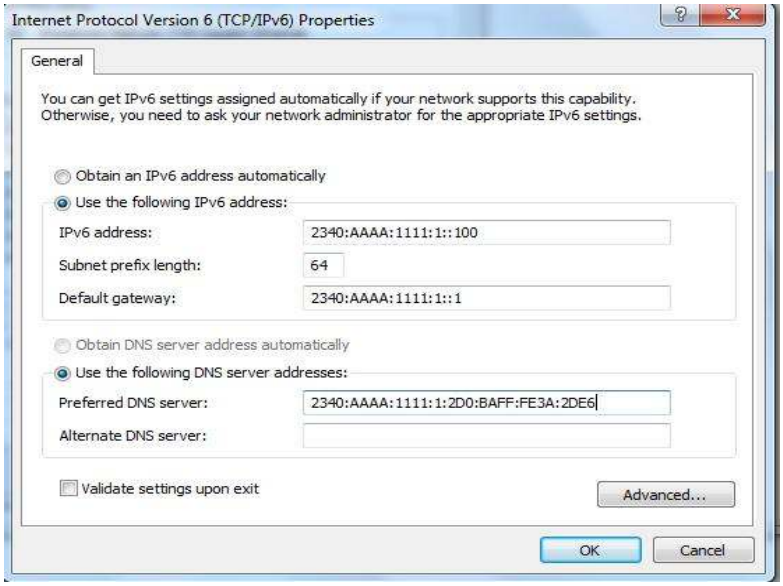


Figura 31 – Configurarea manuala a adreselor IPv6 în windows 7

j. Folosind acelaşi command prompt se tastează *ping 2340:AAAA:1111:1::100* pentru a testa conectivitatea locală

Pentru configurarea adreselor IPv6 folosind subcomenzile *netsh* (şi nu se utilizează GUI)se tasteaza următoarea comandă:

- ***netsh interface ipv6 set address „local area connection" 2340:AAAA:1111:1::100.***

9.2 Instalarea şi configurarea protocolului IPv6 în Linux

Primul cod IPv6 adăugat kernelului a fost în vesiunea 2.1.8 a kernelului în 1996 de către Pedro Roque şi se baza pe un simplu port din stiva BSD[7] care era unică (OpenSource) în acel timp, ajungând în momentul de față la un număr mult mai mare de developeri care se ocupă de progresul stivei IPv6 a kernelului, codul fiind suficient de matur doar în momentul de față în familia 2.4.x a kernelului în care avem o stivă aproape complet implementată conform tuturor specificațiilor RFC inspirată de această dată din mai multe proiecte ale mai multor organizații: KAME (bsd),USAGI, TAHI, şi având de asemenea şi posibilități avansate: filtering şi manipulare a packetelor IPv6 la un mod destul de avansat cu diverse utilitare (***ip6table***) ce sunt imperative pentru utilizarea în producție IPv6.

Distribuțiile moderne de Linux deja sunt implicit incluse cu suport IPv6 atât la nivel de nucleu (ca module) cât şi aplicațiile sunt pregătite să ruleze peste implementarea IPv6. Deoarece stiva IPv6 este compilată ca modul nu este necesar ca distribuția să fie obligatoriu şi cu suport IPv6, e doar opțional, ramâne la latitudinea utilizatorului să activeze aceste opțiuni prezente.

Pentru vizualizarea configurației IP a interfețelor în linux este suficient să tastăm comanda *ifconfig* în terminal pentru a afla ce adrese IP conține fiecare interfață.

Sumar

IPv6 este un nou protocol de nivel rețea aflat în curs de generalizare în Internet. Este un protocol simplificat față de IPv4, dar cu facilități suplimentare cum ar fi autoconfigurarea, autentificarea şi confidențialitatea transferului de pachete, mobilitatea stațiilor în rețea etc. Asigură un spațiu de adresare foarte mare, lungimea adresei fiind pe 128 de biți, iar formatul de adresă şi tipurile de adrese IPv6 permit o structurare mai bună a rețelelor IP. Protocoalele de rutare pentru rețele IPv6 sunt asemănătoare celor din rețele IPv4 (RIP, OSPF, EIGRP etc), dar au particularități specifice, sunt rescrise şi au denumiri specifice cum ar fi RIPng, OSPF3 etc. La fel şi alte protocoale cum ar fi protocolul de control în Internet este ICMPv6 sau DHCPv6.

IPv6 nu este compatibil cu IPv4, ca urmare coexistența lor pe o anumită durată de timp impune elaborarea şi aplicarea unor mecanisme de tranziție: stiva dual, tunelarea sub diverse moduri, translația de adrese.

[7] BSD – (Berkeley Software Distribution) este numele unei distribu□ii UNIX (dezvoltata înte 1977 – 1995 de CSRG) ce a fost adoptata de o serie larga de dezvoltatori precum DEC (ULTRIX), Sun Microsystems (SunOS) □i Apple Inc (Mac OS X)

Întrebări de verificare

1. Care sunt principalele tipuri de adrese IPv6, cum se deosebesc şi la ce sunt folosite?
2. Care este formatul de antet al pachetului IPv6 şi ce rol au câmpurile din antet?
3. Care este formatul primului grup de 4 cifre hexa al adreselor globale unicast?
4. Ce fel de adresă este 2aff:1234:c26::10/64?
5. Care este structura unei adrese IPv6 rutabilă global în Internet
6. Cum se alocă (distribuie) adresele IPv6 în Internet
7. Ce se întelele prin adresă link local, ce foarmă are şi care este utilitatea ei
8. Ce sunt extensiile de header din pachetul IPv6 şi la cefolosesc?
9. Cum se mai poate scrie adresa2031:0000:130F:0000:0000:09C0:876A:130B?
10. Ce reprezintă următoarele adrese IPv6 şi la ce folosesc 0:0:0:0:0:0:0:1 , 0:0:0:0:0:0:0:0?
11. Ce puteți spune despre următoarea adresă IPv6 2001:db8:12::/40?
12. Care este structura unui prefix de rețea IPv6 de rutare globală?
13. Ce sunt Regiştrii Regionali Internet?
14. Cum se formează o adresă de interfață din adresa MAC?
15. Ce este o adresă multicast, care este prefixul ei şi la ce foloseşte?
16. Cum comunică echipamentele conectate pe un link local într-o rețea IPv4 şi într-o rețea IPv6?
17. Ce este un site local într-o rețea IPv6 şi cu se comunică pe acesta?
18. Ce puteți spune despre următoarea comandă dată pe un ruter Cisco?
    ipv6 route 2001:db8::/64 2001:db8:0:CC::1 110
19. În ce constă mecanismul de traziție IPv6 – IPv4 bazat pe tehnica dual-stack?
20. Ce funcție a unui ruter asigură comanda *ipv6 unicast-routing?*De ce este obligatorie la configurarea unui ruter?
21. Ce este o rețea broadcast multiacces ? Dați un exemplu
22. Ce este o rețea nonbroadcast multiacces? Dați un exemplu
23. În câte moduri se poate configura o adresă IPv6 pe interfața unui ruter?
24. Cîte adrese unicast globale se pot cofigura pe interfața unui ruter ?
25. Care este consecința executării comenzii următoare dată pe un ruter Cisco:
    Router(config-if)#ipv6 enable
26. Cum se poate vizualiza tabela de rutare pe un Cisco folosind aplicația Packet Tracer?
27. Ce este ID-ul unui ruter într-un proces OSPFv3 şi cum se poate configura?
28. Există autentificare în OSPFv3, aşa cum există în OPPFv2? Argumentați răspunsul.
29. Pe un ruter pot rula simultan mai multe protocoale de rutare dinamică?
30. Ce face comanda de mai jos dată pe un ruter configurat IPv6?
    Router(config)#ipv6 route 2001:db8::/64 2001:db8:0:cc00::1 110

Exerciții şi aplicații

Exercițiul 1

Pentru rețeaua din figura 1 de mai jos:

1. Pe interfața F0/0 ruterului să se autoconfigureze o adresă IPv6 folosind prefixul de rețea specificat şi adresă de interfață tip EUI-64
2. Pe interfeța F0/1 ruterului să se configureze o adresă statică IPv6 folosind prefixul de rețea specificat şi adresă de interfață statică
3. Pe stații se alege opțiunea *IPv6 autoconfig*
4. Să se verifice cum s-au autoconfigurat adresele IPv6 pe stații, din adresele MAC
5. Să se verifice câte adrese IPv6 s-au configurat pe stații şi pe ruter şi să se explice utilitatea lor

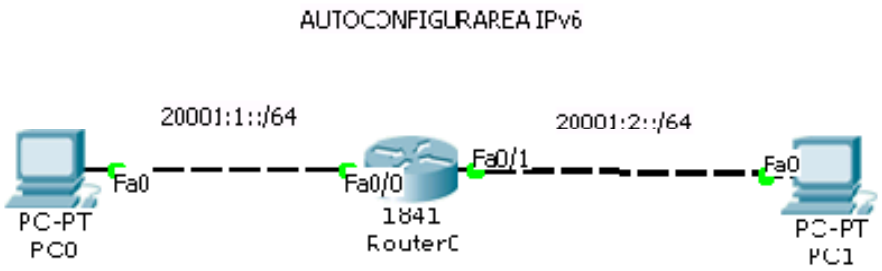


Fig. 1

O soluție se poate vedea în fişierul următor

```
Ruterul0 are configurate static adrese ipv6 pe cele doua interfete:
  pe F0/0 s-a specificat prefixu si s-a continuat cu EUI-64
  pe F0/1 s-a configurat static toata sdresa

Router#sh ipv6 int brief
FastEthernet0/0        [up/up]
    FE80::2E0:B0FF:FE0C:3701
    2001:1::2E0:B0FF:FE0C:3701
FastEthernet0/1        [up/up]
    FE80::2E0:B0FF:FE0C:3702
    2001:2::2
Vlan1                  [administratively down/down]
```

```
Pe calculatoare s-a selectat IPv6 autoconfig
Ca urmare, ele au luat prefixul de la ruter si au completat adresa cu eui-64

PC0                                  PC1
IPv6 Address                         IPv6 Address
2001:1::2D0:FFFF:FE63:7292/64        2001:2::2E0:F7FF:FEC9:29E0

FE80::2D0:FFFF:FE63:7292             FE80::2E0:F7FF:FEC9:29E0
```

Exercițiul 2

Folosindu-se simulatorul Packet Tracer se va configura 2 reteaua de mai jos.

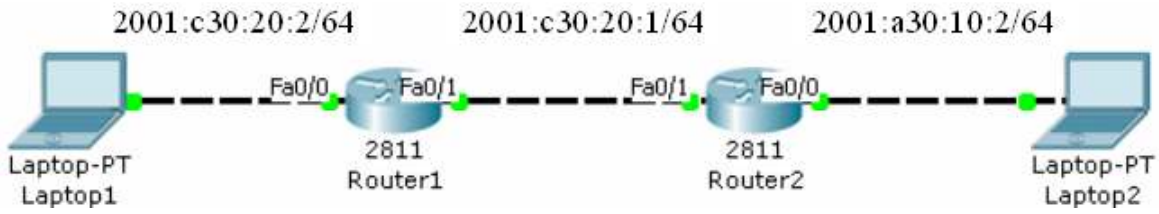


Fig. 2

a. Adresele interfetelor hosturilor se vor asigna static
b. Adresele interfetelor ruterelor se vor asigna static folosind interface ID EUI-64.
c. Pentru rutere se vor configura rute default.
d. Se vor vizualiza informatiile referitoare la adresele IPv6, tabelele de rutare IPv6 si se va testa conectivitatea.
e. Pentru ruterele 1 si 2 se vor sterge rutele default si se vor configura rute pentru retelele 2001:a30:10:2/64 si respectiv 2001:c30:20:2/64.
f. Se vor vizualiza informatiile referitoare la adresele IPv6, tabelele de rutare IPv6 si se va testa conectivitatea.

Exercițiul 3

Pe ruterul 1 din fig. 3 să se configureze o rută implicită de ieşire spre Internet

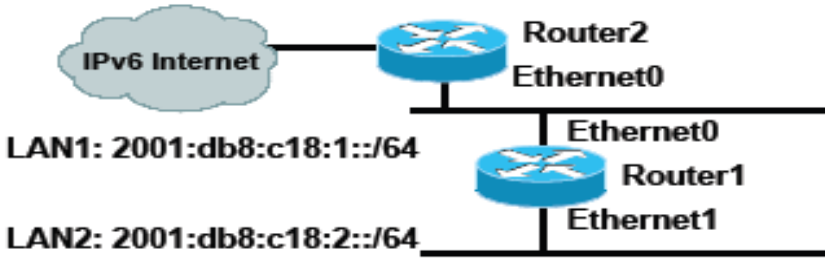


Fig 3

Soluție:

```
ipv6 unicast-routing
!
interface Ethernet0
 ipv6 address 2001:db8:c18:1::a/64
!
interface Ethernet1
 ipv6 address 2001:db8:c18:2::a/64
!
ipv6 route ::/0 <address of R2 ethernet0>
```

Teme de casă

T1. Pentru rețeaua din figură 4

1. sa se configureze echipamentele în rețelele precizate
2. să se configureze rute statice astfec încât să existe conectivitate totală în rețea
3. Să se îndepărteze rutarea statică şi să se configureze rurare dinamică RIPng

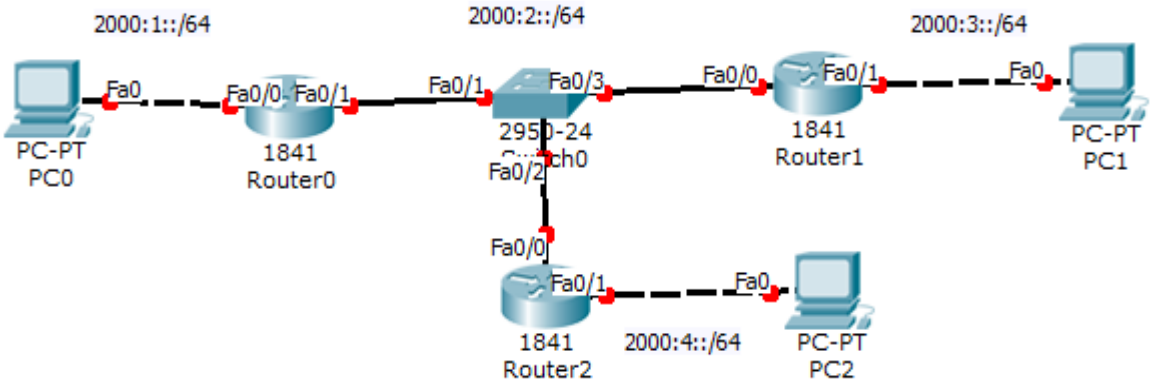


Fig. 4

T2. Pe rețeaua IPv6 din fig 4 sa se configureze rutarea dinamică OSPFv3. Să se afișeze: tabele de rutare din rutere, baza de date cu starea legăturilor, tabela de topologie, starea interfețelor, caracteristicile procesului OSPF

T3. **P**entru rețeaua din figura 5 să se configureze manual un tunelIPv6 IP între ruterele R0 şi R1 şi alt tunel IPv6IP între R0 şi R2. Acestea vor conecta rețelele IP6 2000:10::664 şi 2000:10:3::/64 printr-o rețeaua IPv4 (tunel 0), respectiv rețelele IPv6 2000:10:2::/64 şi 2000:10:3::/64 printr-altă rețea IPv4 (tunel1).

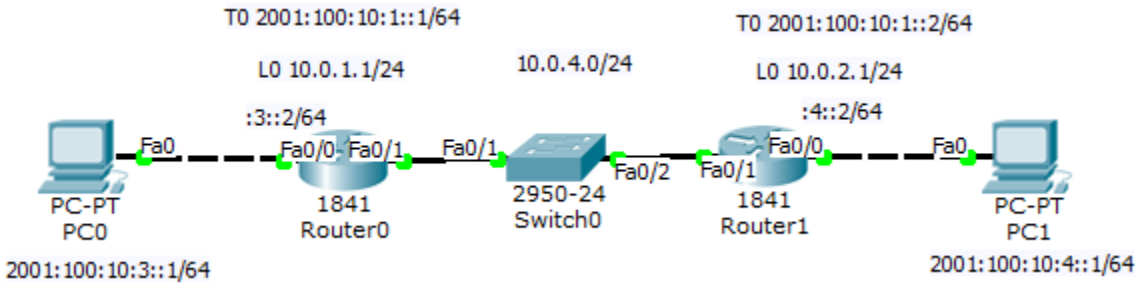


Fig. 5