

Laboratorul 8 – Protocolul IPv6

În cadrul acestui laborator vom investiga protocolul IPv6 (Internet Protocol version 6). Deși a funcționat extrem de bine pentru mai multe decenii, protocolul IPv4 a devenit victima propriei popularități: creșterea exponențială a Internet-ului a dus aproape la epuizarea adreselor IPv4. În anii 1990 IETF a demarat lucrul pentru o nouă versiune IP, denumită IPv6. Pe lângă soluționarea problemei adreselor, proiectarea unui nou protocol a constituit o ocazie excelentă de îmbunătățire a neajunsurilor protocolului IPv4. Principalele noutăți aduse de IPv6 pot fi grupate pe patru categorii, după cum urmează:

- Capabilități extinse de adresare:

IPv6 a mărit dimensiunea adresei IP de la 32 de biți la 128 de biți. Astfel se elimină posibilitatea epuizării adreselor chiar și în cazul unei utilizări ineficiente, pot fi folosite mai multe niveluri ierarhice de adresare și apare posibilitatea autoconfigurării simple a adreselor. În plus față de adresele unicast și multicast a fost definit un nou tip de adresa “anycast”; aceasta reprezintă un identificator pentru un set de interfețe de regulă aparținând unor noduri diferite, datagrama fiind livrată către cea mai apropiată dintre acestea (conform metricii de rutare). Adresele de difuzare au fost eliminate.

- Simplificarea formatului antetului:

S-a definit un nou mecanism de tratare a opțiunilor având ca scop creșterea vitezei de procesare și sporirea flexibilității. Cu toate că antetul IPv6 fără opțiuni are o dimensiune dublă față de antetul IPv4 (40 de octeți și respectiv 20 de octeți în cazul IPv4), 32 de octeți sunt reprezentați de adresele sursă și destinație, rămânând doar 8 octeți pentru restul câmpurilor (față de 12 octeți în cazul IPv4). Funcționalitatea asigurată nodurilor este cel puțin aceeași ca și în cazul IPv4. Antetul IPv6 nu include suma de control.

- Suport îmbunătățit pentru extensii și opțiuni:

Modificările din structura antetului IPv6 permit o retransmitere mai rapidă, nu impun limite stricte în privința dimensiunii opțiunilor și permit o mai mare flexibilitate în introducerea de noi câmpuri opționale.

- Capabilități de etichetare a fluxurilor:

Aceasta capacitate permite etichetarea pachetelor ce aparțin unor fluxuri de trafic particulare pentru care emițătorul solicita o tratare specială, cum ar fi o calitate a serviciilor alta decât cea implicită sau un serviciu în timp real [RFC 2460]. De exemplu transmisiile audio/video ar putea fi tratate ca fluxuri, pe când aplicațiile de rețea tradiționale nu vor fi tratate ca fluxuri.

Figura 1. ilustrează structura antetului IPv6, așa cum este ea prezentată în RFC 2460 și RFC 2474.

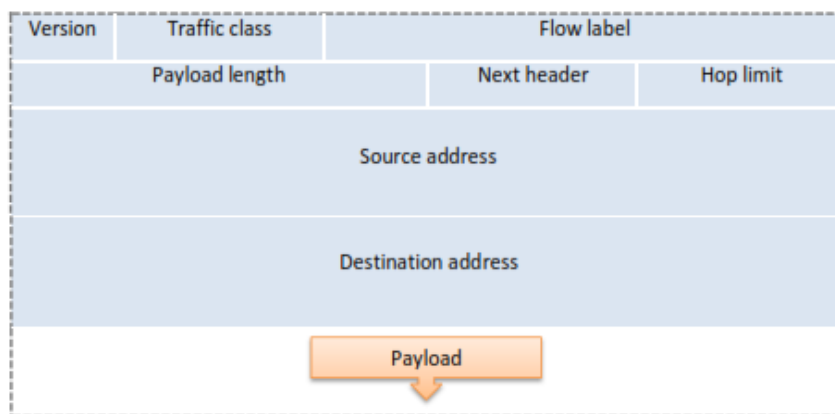


Figura 1 - Antetul datagramelor IPv6

Semnificația câmpurilor este următoarea:

- Versiune (Version), 4 biți – specifică versiunea de protocol căreia îi aparține datagrama.
- Clasa de trafic (Traffic class), 8 biți – este utilizat pentru a distinge între diverse clase sau priorități ale datagramelor.
- Eticheta fluxului (Flow label), 20 biți - acest câmp este utilizat pentru a identifica un flux de datagrame.
- Lungimea încărcăturii (Payload length), 16 biți – reprezintă lungimea încărcăturii exprimată în octeți (toate datele ce succed antetul principal fie că aparțin unor antete de extensie sau unui protocol de nivel superior).
- Următorul antet (Next header), 8 biți – identifică tipul de antet ce urmează după antetul principal IPv6. Valori uzuale sunt: 6 (TCP), 17 (UDP) și 58 (ICMPv6). Acest câmp joacă un rol important în implementarea opțiunilor IPv6 (antete de extensie).
- Limita de salturi (Hop limit), 8 biți – este decrementat cu 1 de fiecare nod ce retrimite datagrama. Are rolul de a preveni hoinăreala la infinit a datagramelor dacă apar bucle de rutare.

- Adresa sursă, adresa destinație, 128 biți fiecare – indică numărul de rețea și numărul de gazdă al stației care a creat și respectiv care trebuie să recepționeze datagrama.



Experimentul 1

1. Porniți Wireshark. Deoarece nu se poate utiliza Wireshark pentru interceptarea de pachete, din cauza lipsei unor privilegii, în cadrul acestui laborator vom utiliza fișierul de captura „tracerute” de pe platforma e-learning.
2. Captura Wireshark va afișa o serie de mesaje ICMPv6 Echo (ping) Request trimise de calculatorul vostru precum și o serie de mesaje ICMPv6 Time exceeded recepționate de la ruterele intermediare de pe calea sursă - destinație. Pentru a afișa doar tipurile de mesaje ICMPv6 (Echo request, Echo reply, Time exceeded) aplicați următorul filtru de afișare:

`icmpv6.type == 129 or icmpv6.type == 128 or icmpv6.type == 3`

3. Selectați primul mesaj ICMPv6 Echo request trimis de calculatorul și expandați secțiunea Internet Protocol Version 6 a pachetului în fereastra de detalii pachete. Care este adresa IPv6 a calculatorului ?

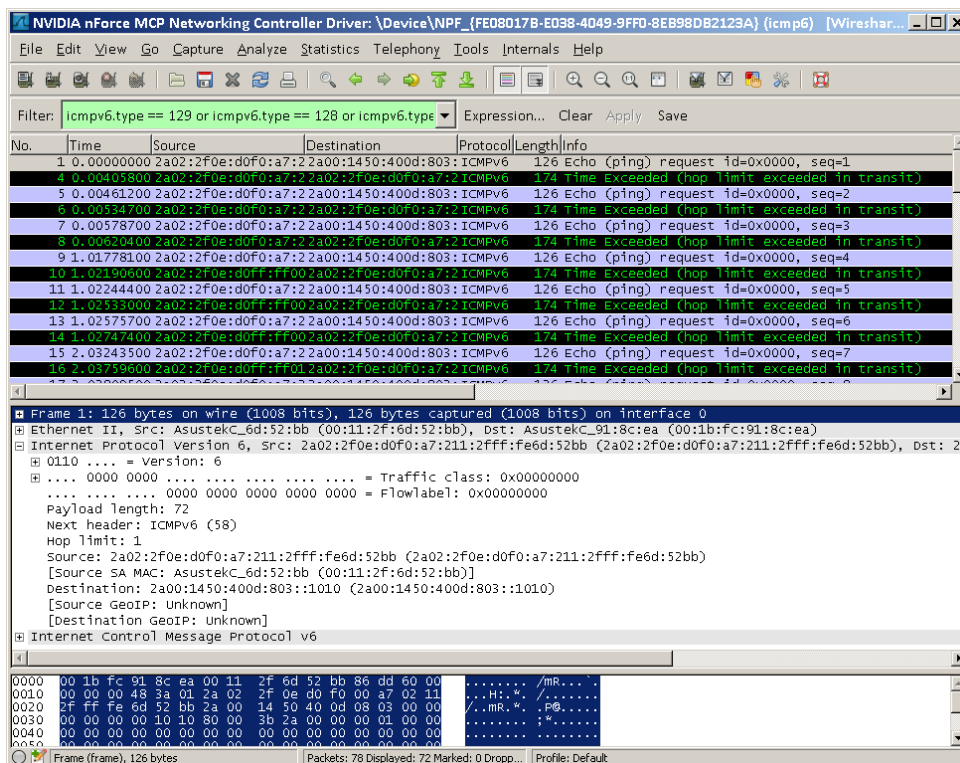


Figura 2 - Lista de mesaje ICMPv6

4. Care este valoarea câmpului „Următorul antet” aflat în componenta antetului IPv6?
5. Câți octeți conține încărcătura utilă a datagramei IPv6? Câți octeți are antetul datagramelor IPv6? Cum ați determinat acest lucru?

Analizați primele trei datagrame IPv6 trimise de calculatorul și:

6. Identificați ce câmpuri din componența antetului IPv6 se schimbă și care rămân nemodificate.
7. Care dintre câmpuri trebuie să se modifice și care trebuie să rămână constante? Explicați.
8. Care este valoarea câmpului Hop limit din antetul acestor datagrame?
9. Care este dimensiunea maximă a unei datagrame IPv6 (antet principal + încărcătura).
10. Ce filtru de captură trebuie utilizat pentru a intercepta doar datagramele IPv6? Ce filtru de afișare trebuie utilizat pentru a elimina datagramele IPv6 din lista de pachete?



Experimentul 2

1. Porniți Cisco Packet Tracer.

2. Asignarea adreselor IPv6:

Adresele IP pot fi asignate static sau dinamic. Asignarea statică poate fi realizată folosind un interface ID manual sau un interface ID EUI-64. Asignarea dinamică se poate face prin autoconfigurare stateless sau prin DHCP pentru IPv6.

Asignarea statică folosind un interface ID manual presupune atribuirea manuală atât a prefixului (network) cât și a interface ID-ului (host). Configurarea unei adrese IPv6 pentru interfețele echipamentelor Cisco se face cu comanda:

```
Router(config-if)#ipv6 address ipv6-address/prefix-length
```

Exemplu de configurare:

```
Router>enable
```

```
Router#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Router(config)#interface fastEthernet 0/0
```

```
Router(config-if)#ipv6 address 2001:C30:20:2:209:7CFF:FE4D:1501/64
```

Router(config-if)#no shutdown

Asignarea statică folosind un interface ID EUI-64 presupune atribuirea manuală a prefixului (network) și derivarea interface ID-ului (host) din adresa MAC a dispozitivului, cunoscută ca și EUI-64 interface ID. Configurarea unei adrese IPv6 pentru interfețele echipamentelor Cisco se face cu comanda:

Router(config-if)#ipv6 address ipv6-prefix/prefix-length eui-64

Exemplu de configurare:

Router>enable

Router#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#interface fastEthernet 0/0

Router(config-if)#ipv6 enable

Router(config-if)#ipv6 address 2001:C30:20:2::/64 eui-64

Router(config-if)#no shutdown

Comanda `ipv6 address` poate configura o adresa IPv6 globală. Adresa link-local este configurată automat când o adresă este asignată interfeței.

Asignarea dinamică prin autoconfigurare stateless configurează automat adresa IPv6 folosind informațiile din mesajele router advertisement (RA). Pentru asignarea dinamică prin autoconfigurare stateless lungimea prefixului transmis din mesajele RA trebuie să fie de 64 biți. Extensia default router preference (DRP) furnizează o metrică preferențială (high, medium, low) pentru ruterele default (gateway). DRP-ul ruterului default este semnalizat în mesajele RA. Mesajele router advertisement sunt transmise de la fiecare interfață a rutelor, periodic ca și răspuns la mesajele router solicitation. Mesajele router solicitation sunt transmise de către hosturi la pornirea sistemului. Configurarea extensiei DRP pentru interfețele echipamentelor Cisco se face cu comanda (în simulatorul Packet Tracer v.5.2 această comandă nu este implementată):

Router(config-if)#ipv6 nd router-preference {high | medium | low}

Exemplu de configurare:

Router>enable

Router#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#**interface fastEthernet 0/0**

Router(config-if)#**ipv6 nd router-preference high**

Asignarea dinamică prin DHCP pentru IPv6 presupune transmiterea parametrilor de configurare nodurilor IPv6 de la serverele DHCP prin protocolul DHCPv6 (stateful). Configurarea DHCPv6 Configuration Pool pentru echipamentele Cisco se face cu comenzile:

Router(config)#**ipv6 dhcp pool poolname**

Router(config-dhcp)#**domain-name domain**

Router(config-dhcp)#**dns-server ipv6-address**

Router(config-dhcp)#**prefix-delegation ipv6-prefix/prefix-length client-duid [iaid iaaid] [lifetime]**

Router(config-dhcp)#**prefix-delegation pool poolname [lifetime valid-lifetime preferred-lifetime]**

Router(config-if)#**ipv6 dhcp server poolname [rapid-commit] [preference value] [allow-hint]**

Vizualizarea DHCPv6 unique identifier (DUID) se face cu comanda:

Router#**show ipv6 dhcp**

Exemplu de configurare:

Router>**enable**

Router#**show ipv6 dhcp**

This device's DHCPv6 unique identifier (DUID): 0003000100097C4D1501

Router#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)# **ipv6 dhcp pool rc**

Router(config-dhcp)# **domain-name rc.ro**

Router(config-dhcp)# **dns-server 2001:C30:20:2:1:1:1:1**

```
Router(config-dhcp)#prefix-delegation 2001:C30:20:2::/64 0003000100097C4D1501
```

```
Router(config-dhcp)#exit
```

```
Router(config)#interface fastEthernet 0/0
```

```
Router(config-if)# ipv6 dhcp server rc
```

Vizualizarea adreselor ipv6 se face cu comanda:

```
Router#show ipv6 interface [brief] [type number] [prefix]
```

3. Strategii de tranziție IPv6:

Cele mai comune tehnici de tranziție de la IPv4 la IPv6 sunt dual stacking si tunneling. În dual stacking echipamentele sunt configurate pentru a suporta ambele protocoale, IPv6 fiind protocolul preferat. Cele mai utilizate tehnici de tunneling sunt: manual IPv6-over-IPv4 tunneling si dynamic 6to4 tunneling. În cazul manual IPv6-over-IPv4 tunneling pachetele IPv6 sunt încapsulate în protocolul IPv4. Dynamic 6to4 tunneling stabilește automatic conexiunea rețelelor IPv6 prin rețele IPv4.

4. Rutarea cu IPv6:

IPv6 folosește rutarea bazată pe potrivirea celui mai lung prefix (longest prefix match routing). Protocoalele de rutare pentru IPv6 sunt versiuni modificate ale celor mai uzuale protocoale de rutare.

Activarea IPv6 pe un ruter Cisco se face în doi pași. Primul pas presupune activarea înaintării traficului IPv6 iar al doilea pas este configurarea fiecărei interfețe care necesită IPv6. Activarea înaintării traficului IPv6 între interfețe se face cu comanda:

```
Router(config)#ipv6 unicast-routing
```

Exemplu de configurare:

```
Router>enable
```

```
Router#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Router(config)#ipv6 unicast-routing
```

Configurarea unei rute statice pentru echipamentele Cisco se face cu comanda:

```
Router(config)#ipv6 route ipv6-prefix/prefix-length {ipv6-address | interface-type  
interface-number [ipv6-address]} [administrative-distance] [administrative-multicast-  
distance | unicast | multicast] [tag tag]
```

Exemplu de configurare:

```
Router>enable
```

```
Router#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Router(config)# ipv6 route 2001:A30:10:2::/64 2001:C30:20:1:290:2BFF:FE71:6702
```

Vizualizarea tabelii de rutare pentru echipamentele Cisco se face cu comanda:

```
Router#show ipv6 route [ipv6-address | ipv6-prefix/prefix-length | protocol |  
interface-type interface-number]
```

Pentru a configura routarea RIP:

```
Router(config)#ipv6 router rip {word}
```

Exemplu de configurare:

```
Router>enable
```

```
Router#configure terminal
```

```
Router(config)#ipv6 unicast-routing
```

```
Router(config)#ipv6 router rip lab8
```

```
Router(config)#int fa0/1
```

```
Router(config)#ipv6 rip lab8 enable
```

5. Vizualizarea si setarea informațiilor

Pentru sistemul de operare Windows vizualizarea și setarea informațiilor se face cu ajutorul comenzilor ipconfig, route, netstat, netsh. Pentru sistemul de operare Linux vizualizarea și

setarea informațiilor se face folosind comenzile ifconfig, route, netstat. Interogarea DNS pentru sistemele de operare Windows si Linux se face cu ajutorul comenzii nslookup.

6. Testarea conectivității

Pentru sistemul de operare Linux si echipamentele Cisco testarea conectivității se face cu ajutorul comenzilor ping si traceroute. Pentru sistemul de operare Windows testarea se face folosind comenzile ping si tracert.

7. Desfășurarea lucrării

- Se vor testa pe stațiile din laborator comenzile pentru vizualizarea și setarea informațiilor și testarea conectivității.
- Folosindu-se simulatorul Packet Tracer se va configura rețeaua de mai jos:

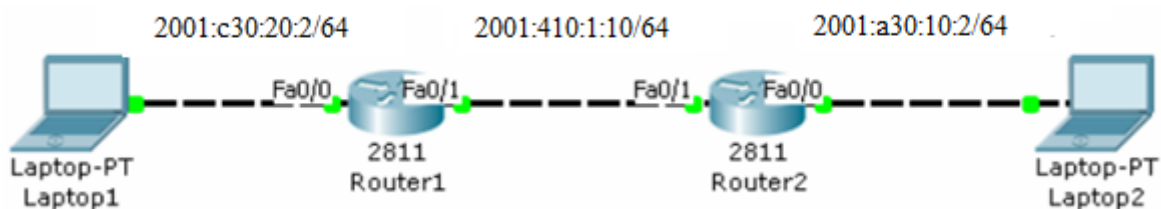


Figura 3 – Topologia de realizat

- a. Adresele interfețelor hosturilor se vor asigura static.
- b. Adresele interfețelor ruterele se vor asigura static.
- c. Ruterele 1 si 2 se vor configura folosind rutarea rip.
- d. Se vor vizualiza informațiile referitoare la adresele IPv6, tabelele de rutare IPv6 și se va testa conectivitatea.