Facultatea de Electronică, Telecomunicații și Tehnologia Informației

Rețele de Calculatoare și Internet

Internet Control Message Protocol

Hampău Bogdan
Master IISC An 2

Cuprins

I. ICMP version 4 3
1. Protocolul ICMP 3
2. Principalele tipuri de ICMP: 4
3. Exemplu de mesaj ICMP : Destination Unreachable 5
4. Moduri de utilizare 6
II. ICMP version 6 9
1. Protocolul ICMPv6 9
2. Tipuri de mesaje ICMPv6 10
3. Interacțiunea dintre ICMP și nivelul legătură de date 11
4. Determinarea adresei sursei mesajelor 12
5. Reguli de procesare a mesajelor 13
Bibliografie 15

I. ICMP version 4

1. Protocolul ICMP

Protocolul de mesaje de control pentru internet(ICMP) definită în RFC 792 este un protocol din suita TCP/IP folosit de către routere intermediare sau de hostul destinație pentru a raporta expeditorului pachetului o problemă care a apărut la procesarea lui. Mesajele ICMP sunt purtate în payloadul pachetelor IP (valoare câmpului protocol pentru ICMP e 1). Un mesaj ICMP e compus dintr-un header de 8 octeți și un payload de lungime variabilă ce conține de obicei primul octet din pachetul ce a cauzat transmisia mesajului ICMP.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Version|  IHL  |    DS Field   |          Total Length         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         Identification        |Flags|      Fragment Offset    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Time to Live |    Protocol   |         Header Checksum       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       Source Address                          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Destination Address                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |     Code      |          Checksum             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                             Data                              |
~                                                               ~
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|      IPv4 header of errored packet + 64 bits of payload       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Fig. 1 ICMP IPv4 [1]

În headerul ICMP folosește câmpurile Type și Code pentru a indica tipul problemei care a fost detectată de expeditorul mesajului ICMP. Câmpul Checksum protejează întreg mesajul ICMP de erori de transmisie și câmpul Data conține informații pentru unele mesaje ICMP.
Dacă nu e specificat altfel valorile headerului IP sunt următoarele:

Version

4

Type of Service

0

Total Length

Lungimea headerului IP

Identification, Flags, Fragment Offset

Folosite la fragmentare

Time to Live

Câmp special care este decrementat de fiecare dată când pachetul trece printr-un router. Valoarea sa ar trebui să fie cel puțin egală cu numărul de Gatewayuri prin care va trece pachetul.

Protocol

ICMP = 1

Header Checksum

16 biți în complement față de 1 a sumei tuturor cuvintelor de 16 biți din header. Ar trebui să fie 0.

Source Address

Adresa gatewayului sau hostului care a compus mesajul.

Destination Address

Adresa gatewayului sau hostului către care e trimis mesajul

2. Principalele tipuri de mesaje ICMP:

- *Destination Unreachable* : mesaj ICMP trimis de un router care nu a găsit o rută către subnetul ce conține adresa destinație a pachetului. Poate fi de mai multe tipuri:
    - *Network unreachable* : nu a găsit o rută către subnetul ce conține adresa destinație a pachetului
    - *Host unreachable* : mesajul a fost trimis de un router atașat subnetului ce conține adresa destinație a pachetului, dar aceasta nu poate fi accesată în acest moment
    - *Protocol unreachable*: mesajul ICMP trimis de hostul destinație când acesta a primit pachetul dar nu suportă protocolul de transport indicat de câmpul Protocol a pachetului.

- *Port unreachable* : mesaj ICMP trimis de hostul destinație când a primit un pachet destinat altui port, dar nici un proces server nu e legat de acest port.
-

- *Fragmentation needed* : mesaj ICMP trimis de un router ce a primit un pachet cu flagul DF (Do not Fragment), dar care e mai mare decât MTU-ul interfeței de ieșire.
- *Redirect*: mesaj ICMP ce poate fi trimis când există două routere în același LAN. Acest mesaj este utilizat pentru a anunța sursa să redirecteze pachetele pe o rută mai bună. Dacă mesajul vine de la un router intermediar atunci sistemul sursă va trimite următoarele datagrame către routerul care are același IP cu cea din mesajul ICMP.
- *Parameter Problem* : mesaj ICMP trimis când un router sau un host a primit un pachet ce conține o eroare.
- *Source quench(depracated) :* un router trimitea acest mesaj când trebuia să renunțe la pachete datorită congestiei. Nu se mai folosește de când s-au introdus mecanismele de control a congestiei din TCP.
- *Time Exceeded* : aceste mesaje sunt de două tipuri:
  - *TTL exceeded:* trimis de un router când renunță la un pachet pentru că câmpul TTL al acestuia a ajuns la 0.
  - *Reassembly time exceeded :* mesaj ICMP trimis când o destinație nu a putut reasambla toate fragmentele unui pachet înaintea expirării timpului de reasamblare.
- *Echo request* și *Echo reply: mesaje ICMP folosite de debuggerul de rețea ping(8).*

3. Exemplu de mesaj ICMP : Destination Unreachable

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |     Code      |          Checksum             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                             unused                            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|      Internet Header + 64 bits of Original Data Datagram      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Fig. 2 Mesaj ICMP Destination Unreachable

Câmpuri IP :

Destination Address

Rețeaua și adresa sursă din datele datagramei originale

Câmpuri ICMP:

Type

3

Code

0 = net unreachable;
1 = host unreachable;
2 = protocol unreachable;
3 = port unreachable;
4 = fragmentation needed and DF set;
5 = source route failed.

Checksum

Suma pe 16 biți în complement față de 1 a mesajului ICMP începând cu ICMP Type. Pentru calculul checksum-ului, câmpul checksum trebuie să fie 0.

Internet Header + 64 bits of Data Datagram

Primii 64 de biți de date din datagrama originală. Aceste date sunt folosite de către host pentru a corela mesajul cu procesul corespunzător. Dacă un protocol de nivel mai înalt folosește porturi atunci se presupune că fac parte din primii 64 biți de date din datagrama originală.

4. Moduri de utilizare

- **Mesajele de tip *ICMP redirect*** sunt utile când mai multe routere aparțin aceluiași LAN, dar creează riscuri majore de securitate. Man in the middle este un atac ce are loc când atacatorul poate primi, procesa sau modifica și trimite mai departe toate pachetele schimbate între sursă și destinație. Deoarece atacatorul primește toate

pachetele acesta poate cu ușurință obține numere de cont bancar, parole sau chiar injecta informații false într-o conexiune TCP. În figura de mai jos hostul H care e atașat aceluiași LAN ca A și R1. Dacă H îi trimite lui A un mesaj ICMP redirect pentru prefixul 138.48.0.0/16 A forwardează lui H toate pachetele pe care dorește să le trimită acestui prefix. H le poate apoi trimite la R2. Pentru a evita aceste atacuri hosturile trebuie să ignore mesajele ICMP redirect pe care le primesc.

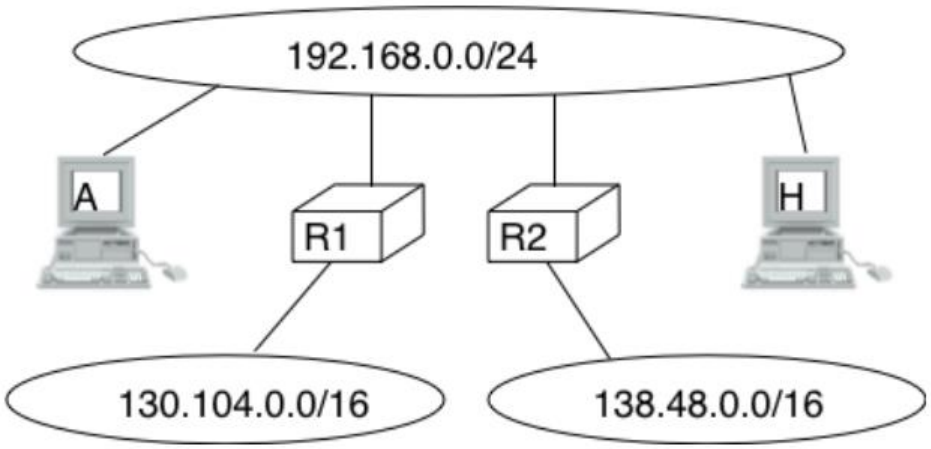

Fig. 3 ICMP redirect [2]

- **ping(8)** e folosit de administratori de rețea pentru a verifica dacă o adresă IP e accesibilă. Fiecare host răspunde cu un mesaj ICMP *Echo Reply* când primește un mesaj *ICMP Echo request.* Un exemplu de utilizare ping(8) e demonstrat mai jos:

```
ping 130.104.1.1 PING 130.104.1.1 (130.104.1.1): 56 data bytes
64 bytes from 130.104.1.1: icmp_seq=0 ttl=243 time=19.961 ms
64 bytes from 130.104.1.1: icmp_seq=1 ttl=243 time=22.072 ms
64 bytes from 130.104.1.1: icmp_seq=2 ttl=243 time=23.064 ms
64 bytes from 130.104.1.1: icmp_seq=3 ttl=243 time=20.026 ms
64 bytes from 130.104.1.1: icmp_seq=4 ttl=243 time=25.099 ms
 --- 130.104.1.1 ping statistics ---
 5 packets transmitted, 5 packets received, 0% packet loss
 round-trip min/avg/max/stddev = 19.961/22.044/25.099/1.938 ms
```

- **tracerout(8)** este Un alt tool util pentru debugging care printează routerele intermediare prin care trec pachetele pentru a ajunge la host. Traceroute folosește mesajele ICMP TTL exceeded. Când un router primește un pachet cu valoare câmpului TTL 1, acesta trebuie să decrementeze TTL și să răspundă hostului sursă un mesaj ICMP TTL Exceeded care să conțină headerul și primii octeți din pachetul IP abandonat. Pentru a descoperi toate routerele dintr-o rută o soluție simplă e să se trimită un pachet cu TTL 1 , după care un pachet cu TTL 2, etc. Următorul exemplu de output tracerout a descoperit 17 „hopuri” între sursă și destinație.

traceroute www.ietf.org

```
 traceroute to www.ietf.org (64.170.98.32), 64 hops max, 40 byte packets
1 CsHalles3.sri.ucl.ac.be (192.168.251.230) 5.376 ms 1.217 ms 1.137 ms
2 CtHalles.sri.ucl.ac.be (192.168.251.229) 1.444 ms 1.669 ms 1.301 ms
 3 CtPythagore.sri.ucl.ac.be (130.104.254.230) 1.950 ms 4.688 ms 1.319 ms
4 fe.m20.access.lln.belnet.net (193.191.11.9) 1.578 ms 1.272 ms 1.259 ms
5 10ge.cr2.brueve.belnet.net (193.191.16.22) 5.461 ms 4.241 ms 4.162 ms
6 212.3.237.13 (212.3.237.13) 5.347 ms 4.544 ms 4.285 ms
7 ae-11-11.car1.Brussels1.Level3.net (4.69.136.249) 5.195 ms 4.304 ms 4.329 ms
8 ae-6-6.ebr1.London1.Level3.net (4.69.136.246) 8.892 ms 8.980 ms 8.830 ms
9 ae-100-100.ebr2.London1.Level3.net (4.69.141.166) 8.925 ms 8.950 ms 9.006 ms
10 ae-41-41.ebr1.NewYork1.Level3.net (4.69.137.66) 79.590 ms
ae-43-43.ebr1.NewYork1.Level3.net (4.69.137.74) 78.140 ms
ae-42-42.ebr1.NewYork1.Level3.net (4.69.137.70) 77.663 ms
11 ae-2-2.ebr1.Newark1.Level3.net (4.69.132.98) 78.290 ms 83.765 ms 90.006 ms
12 ae-14-51.car4.Newark1.Level3.net (4.68.99.8) 78.309 ms 78.257 ms 79.709 ms
13 ex1-tg2-0.eqnwnj.sbcglobal.net (151.164.89.249) 78.460 ms 78.452 ms 78.292 ms
14 151.164.95.190 (151.164.95.190) 157.198 ms 160.767 ms 159.898 ms
```

15 ded-p10-0.pltn13.sbcglobal.net (151.164.191.243) 161.872 ms 156.996 ms 159.425 ms
16 AMS-1152322.cust-rtr.swbell.net (75.61.192.10) 158.735 ms 158.485 ms 158.588 ms
17 mail.ietf.org (64.170.98.32) 158.427 ms 158.502 ms 158.567 ms

- **Path MTU discovery mechanism (RFC1191)** : mesajele ICMP combinate cu flagul DF(Don't fragment) pot fi folosite pentru a determina valoarea maximă pentru MTU (Maximum Transimssion Unit) permisă pentru ca pachetul să ajungă la destinație fără fragmentare. Majoritatea implementărilor TCP includ Path MTU discovery, astfel toate segmentele din pachetele IPv4 vor avea flagul DF setat. Acest lucru interzice routerelor intermediare să fragmenteze aceste pachete. Dacă un router trebuie să forwardeze un pachet nefragmentabil pe o rută cu un MTU mai mic, returnează un mesaj ICMP *Fragmentation needed* către sursă care indică MTU-ul căii de ieșire în câmpul Data. Când primește mesajul sursa își ajustează MSS (Maximum Segment Size astfel ca pachetele trimise ulterior să poată fără să necesite fragmentare.

II. ICMP version 6

1. Protocolul ICMPv6

ICMP version 6 (definit în RFV 4443) e un protocolul asociat IPv6, cum ICMP version 4 e pentru IPv4. ICMPv6 e folosit de routere și hosturi pentru a raporta probleme în procesarea pachetelor IPv6.
Utilizarea tradițională a ICMPv6 e asemănătoare cu ICMPv4. Mesajele ICMPv6 sunt transportate în pachetele IPv6. Fiecare mesaj ICMPv6 e precedat de un header IPv6 și 0 sau mai multe headere de extensie IPV6. Headerul ICMPv6 e identificat de valoarea 58 a câmpului Next Header din headerul IPv6 imediat precedent.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |     Code      |          Checksum             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                         Message Body                          +
|                                                               |
```

Fig 4. Header ICMP

Type indică tipul mesajului. Valoarea sa determină formatul datelor rămase.
Code depinde de tipul mesajului și e specifică detalii suplimentare pentru tipul mesajului.
Checksum e folosit pentru a detecta coruperi de date în mesajul ICMP și în anumite părți din headerul IPv6.

2. Tipuri de mesaje ICMPv6

Mesajele sunt grupate în două clase: mesaje de eroare și mesaje informaționale. Mesajele de eroare au 0 în bitul cel mai semnificativ din câmpul message type, valorile câmpului putând fi între 0 și 127. Mesajele informaționale au valori cuprinse între 128 și 255.
RFC 4443 specifică 4 tipuri de erori de mesaje:

1. *Destination Unreachable*: trimis când adresa destinație a unui pachet e inaccesibilă. Câmpul Code din headerul ICMP conține informații adiționale despre motivul pentru care e inaccesibilă:
    - 0: nu există rută către destinație. Routerul care a trimis mesajul nu avea o rută către adresa destinația acestuia.
    - 1: comunicația cu destinația interzisă de administrator. Indică faptul că un firewall a refuzat să forwardeze pachetul către destinație.
    - 2: dincolo e scopul adresei sursă. Acest mesaj poate fi trimis dacă sursa folosește adrese link-locale pentru a ajunge la o adresă unicast din afara subnetului ei.
    - 3: address unreachable. Acest mesaj indică faptul că pachetul a ajuns la subnetul destinației dar hostul cu adresa respectivă e inaccesibil.
    - 4: port unreachable: pachetul IPv6 a ajuns la destinație dar nu exista nici o aplicație ce asculta pe portul respectiv.

2. *Packet to Big*: pachetul ce trebuia trimis mai departe de router mai mare decât MTU-ul legăturii de ieșire. Mesajul ICMPv6 conține MTU-ul acestei legături în octeți. Acest lucru permite hostului sursă să implementeze Path MTU Discovery.
3. *Time Exceeded* : mesaj de eroare ce poate fi trimis de un router sau un host, Un router va seta Code la 0 pentru a raporta un pachet a cărui limită de hopuri a ajuns la 0. Un host va seta Code la 1 pentru a raporta că nu a reușit să reasambleze fragmentele IPv6 primite.
4. *Parameter Problem* : folosit pentru a raporta un mesaj IPv6 cu un header greșit (câmpul Type setat la 0) sau o valoare necunoscută pentru câmpul *Next Header* sau *IP Option* (Type 1 sau 2). Corpul mesajului va conține pachetele greșite IPv6 și primii 32 biți din corpul mesajului vor conține un pointer la eroare.

   Există două tipuri de mesaje de informație : *Echo Request* și *Echo Reply* folosite la verificarea accesibilității unei destinații cu ping6(8).
   De asemenea ICMPv6 permite de asemenea Path Discovery: descoperirea unei căi între sursă și destinație folosind traceroute6(8).

3. Interacțiunea dintre ICMP și nivelul legătură de date

Spre deosebire de IPv4 în IPv6 interacțiunea dintre nivelul de rețea și nivelul legătură de date se realizează prin intermediul protocolului ICMPv6.
ICMPv6 e folosit pentru a afla adresa din nivelul legătură de date corespunzătoare unei adrese Ipv6. Această parte din IPv6 poartă numele de Neighbour Discovery Protocol (NDP) definit în RFC 4861. NDP e similar cu ARP (Address Resolution Protocol) , dar cu două diferențe majore. În primul rând mesajele NDP sunt trimise ca parte din mesajele ICMP, în timp ce mesajele ARP sunt transmise ca frame-uri în nivelul legătură de date. În al doilea rând un request ARP e trimis ca un frame broadcast în timp ce unele mesaj de solicitare NDP e transmis ca un pachet ICMPv6 multicast ce e purtat într-un frame multicast. Modul de funcționare a NDP e similar cu ARP. Pentru a obține maparea unei adrese un host trimite un mesaj de tipul Neighbour Solicitation Message. Acest mesaj e transmis în interiorul unui mesaj ICMP ce plasat într-un pachet IPv6 a cărui adresă sursă este adresa hostului solicitant și adresa destinație este adresa multicast all-hosts(FF02::1) pe care ascultă toate hosturile IPv6. Hostul cu adresa cerută face reply trimițând un mesaj

unicast de tipul Neighbour Advertisement message către hostul solicitant. NDP și ARP suferă de probleme de securitate similare, însă NDP poate fi securizat folosind adrese CGA (Cryptographically Generated IPv6 Addresses) definite în RFC 3972. Protocolul SEND(Secure Neighbourhood Discovery) este definit în RFC 3972.

Rețelele IPv6 suportă și Dynamic Host Configuration Protocol(DHCP definit în RFC 3315). Un alt mecanism folosit pentru a asigna adrese IPv6 hosturilor este SLAC(Stateless Address Configuration) definit în RFC 4862. Când un host bootează, își un identificator pe 64 de biți din adresa sa din nivelul legătură de date și îl concatenează cu prefixul FE80::/64 pentru a obține adresa link-locală. După care transmite un mesaj de tip Neighbour Solicitation ce are ca țintă adresa sa link-locală pentru a verifica dacă vreun alt host folosește aceeași adresă link-locală în acest subnet. Dacă primește un mesaj Neighbour Advertisment ce indică adresa link-locală e folosită de către alt host atunci generează un alt id e 64 de biți și trimite un alt Neighbour Solicitation. Dacă nu primește răspuns consideră adresa link-locală ca fiind validă și o va folosi pentru toate mesajele NDP trimise în subnet. Pentru a-și putea configura automat adresa IPv6 hostul trebuie să cunoască global routing prefix folosit în subnetul local. Routerele IPv6 trimit regular mesaje de tip Router Advertisment ce indică prefixul IPv6 asignat fiecărui subnet. La primirea unui astfel de mesaj hostul poate obține adresa IPv6 globală concatenând identificatorul de 64 de biți cu prefixul primit. Pentru a finaliza SLAC trimite un mesaj Neighbour Solicitation având ca destinație adresa sa globală IPv6 pentru a se asigura că nici un alt host nu o folosește.

4. Determinarea adresei sursei mesajelor

Un nod ce creează un mesaj ICMPv6 trebuie să determine atât adresa sursei cât și adresa destinației în headerul IPv6 înainte de a calcula checksumul. Dacă nodul are mai mult de o adresă unicast, trebuie să aleagă adresa sursă a mesajului după una din regulile următoare:

- Dacă mesajul e un răspuns la un mesaj trimis la una din adresele unicast a nodului, adresa sursă a mesajului de reply trebuie să fie aceeași.
- Dacă mesajul e un răspuns la un mesaj trimis de o altă adresă, cum ar fi:

-o adresă multicast de grup
-o adresă anycast implementată de nod
-o adresă unicast ce nu aparține nodului
adresa sursă a pachetului ICMPv6 trebuie să fie o adresă unicast ce aparține nodului.

5. Reguli de procesare a mesajelor

- Dacă este primit un mesaj de eroare ICMPv6 de tip necunoscut trebuie cedat procesului de nivel superior de la care provine pachetul ce a cauzat eroare, dacă acesta poate fi identificat.
- Dacă se recepționează un mesaj informațional de tip necunoscut, acesta trebuie abandonat .
- Fiecare mesaj de eroare ICMPv6 (type ; 128) trebuie să includă cât mai mult din pachetul ce l-a cauzat fără a depăși MTU-ul IPv6 minim permis.
- În cazul în care protocolul TCP/IP trebuie să transmită un mesaj de eroare ICMPv6 unui proces de nivel superior, tipul protocolului de nivel superior e extras din pachetul original (conținut în corpul mesajului de eroare ICMP) și folosit pentru a selecta procesul de nivel superior corespunzător.

  În cazul în care acest lucru nu este posibil mesajul este fără nici o notificare după procesarea pe nivelul IPv6. Un exemplu este un mesaj ICMPv6 cu numeroase headere de extensie (extension headers) care nu conține protocolul de nivel superior datorită trunchierii pachetului original pentru a satisface limita MTU-ului minim IPv6.

- Un mesaj de eroare ICMPv6 nu trebuie să fie generat de:
  1. Un mesaj ICMPv6
  2. Un mesaj ICMPv6 de redirectare
  3. Un pachet destinat unei adrese multicast IPv6 (excepții făcând mesajul Packet to Big Message pentru a permite MTU Path Discovery să funcționeze pentru multicast IPv6 și mesajul Parameter Problem ce

are Code 2ce raportează opțiune IPv6 nerecunoscută și are cei mai semnificativi biți din Option Type setați la 10).

4. Un pachet multicast pe nivelul legătură de date
5. Un pachet trimis ca broadcast pe nivelul legătură de date, excepțiile de la 3 aplicându-se și aici.
6. Un pachet al cărei adresă sursă nu identifică în mod unic un singur nod.

- Pentru a limita lărgimea de bandă și costul de forwardare ce corespund trimiterii de mesaje de eroare ICMPv6 , un nod ICMPv6 trebuie să limiteze rata de creare a mesajelor ICMPv6.

Bibliografie

[1]http://www.saylor.org/site/wp-content/uploads/2012/02/Computer-Networking-Principles-Bonaventure-1-30-31-OTC1.pdf

[2] https://tools.ietf.org/html/rfc792

[3] https://tools.ietf.org/html/rfc4443

[4] http://calin.comm.pub.ro/Didactice/ARI/Notite%20curs/Notite/c10_Niv%203%20-%20ARP-RARP-ICMP-BOOTP-DHCP.pdf

[5] https://tools.ietf.org/html/rfc4861