Protocolul Internet

Studenti: Cadîr Eren

Nichifor Ruxandra Lorena

Grupa:441A

Profesor: : Conf.Dr.Ing. ȘTefan STĂNCESCU

**Cuprins:**

**Protocolul Internet**

* IPv 4 (Nichifor Ruxandra Lorena)

      Pachete IPv4

      ICMP version 4

      Interactiunea intre IPV4 si nivelul legatura de date

* IPv6 (Cadîr Eren)

      Arhitectura de adresare a IPv6

      Pachete IPv6

      ICMP version 6

      Interacțiunea IPv6 cu nivelul legătură de date

* Concluzii (Nichifor Ruxandra-Lorena)

Bibliografie

**Protocolul Internet versiunea 4**

Pentru ca două calculatoare să poată comunica unul cu celălalt, amîndouă trebuie să respecte acelaşi set de reguli. Ingineria software ne învaţă că pentru a construi sisteme complexe trebuie să le împărţim în piese mai simple, pe care apoi le putem folosi independent. Datorita acestui fapt, o reţea de calculatoare specifică mai multe protocoale independente pe care utilizatorii trebuie să le respecte. Pentru fiecare subproblemă care trebuie rezolvata exista un protocol.

Internetul este bazat pe anumite protocoale. Cele mai important protocol folosit de utilizatorii Internet se numeşte IP (Internet Protocol). TCP(Transport Control Protocol) funcţionează numai cu IP.

Protocolul IP este cel care mută pachetele dintr-un loc într-altul, posibil peste multe conexiuni, iar TCP asigură fiabilitatea comunicaţiei.

IP  are sarcina de a livra pachete de date de la gazdă la destinație pe baza adreselor lor. Ȋn acest scop, protocolul Internet definește metode de adresare și structuri de ȋncapsulare a datagramelor (pachete de date). Prima versiune de adresare a structurii, acum denumită Internet Protocol versiunea 4 (IPv4), este ȋncă protocolul de Internet dominant. S-a dezvoltat apoi Internet Protocol versiunea 6 (IPv6) pentru a înlocui protocolul IPv4 care va deveni insuficient ca spaţiu de adrese IP.

Protocolul Internet versiunea 4 (IPv4) este a patra dezvoltare a Protocolului Internet (IP) şi

prima versiune a protocolului utilizat pe scară largă. Împreună cu IPv6, au la baza

standarde si metode de Internetworking. IPv4 este descris în publicaţia IETF RFC 791 (septembrie 1981).

**Pachete IPv4**

IPv4 este un protocol fără conexiune utilizat pe pachete comutate, precum reţelele Ethernet. Acesta funcţionează pe modelul de livrare “cel mai bun efort”, în măsura în care nu garantează livrarea şi nu asigură succesiunea corectă sau evitarea de pachete duplicat.

 Aceste aspecte, inclusiv de integritate a datelor, sunt abordate printr-un protocol de transport strat superior, cum ar fi Transmission Control Protocol (TCP).

Cuprinde toate protocoalele si procedurile necesare pentru ca o conexiune sa parcurgă retele multiple. Pachetele de date de la acest nivel trebuie, deci, sa fie rutabile.

Protocolul IPv4 este fără conexiune (de tip datagramă): pachetele îsi caută singure drumul prin reţea.

Protocolul IPv4 utilizează o schemă de adresare binară pe 32 biţi care identifică în mod unic calculatoarele conectate, dispozitivele de reţea şi reţeaua, atât pentru sursă, cât şi pentru destinaţia pachetului. Adresele IP sunt înregistrate si administrate de către centrele regionale NIC (Network Information Center).

Adresele IP neînregistrate oficial pot fi utilizate numai în cadru restrâns, în reţeaua locală respectivă, ele nefiind recunoscute în afară.

Protocolul IPv4 foloseste cinci clase de adrese .

Ele se reprezinta în mod uzual în format zecimal (sau hexazecimal) pe 4 octeţi, separaţi prin punct (de ex. 192.168.10.1), deşi adresele sunt binare.

- Clasa A defineşte adrese de host de la 1.0.0.0 la 126.0.0.0 (primul bit din adresa are valoarea 0); fiecare adresa de reţea clasa A conţine 16.774.214 adrese distincte de host;

- Clasa B defineşte adrese de host de la 128.1.0.0 la 191.254.0.0 (primii doi biti din adresa au valoarea 10); fiecare adresa de retea clasa B suporta 65.534 adrese distincte de host;

- Clasa C defineşte adrese de host de la 192.0.1.0 la 223.255.254.0 (primii trei biti din adresa au valoarea 110); fiecare adresa de retea clasa C conţine 254 adrese distincte de host;

- Clasa D defineşte adrese de tip difuzare multiplă (multicast), dar nu are o utilizare prea largă (primii patru biţi din adresa au valoarea 1110); adresele din clasa D au valori cuprinse între 224.0.0.0 şi 239.255.255.254;

- Clasa E a fost definită, dar este rezervată pentru uzul intern NIC.

Aceasta împartire în clase poate conduce în mod uzual la pierderi semnificative de adrese IP. Pentru a se evita aceasta pierdere de adrese, mai ales în cazurile în care necesitatea reală pentru o reţea nu acoperă în întregime o clasă, s-a dezvoltat CIDR (Classless Interdomain Routing).

  **ICMP version 4**

Toate protocoalele Internet folosesc IP ca mecanism de bază pentru transportul datelor. IP este un protocol de comunicaţie de tip datagramă (care nu se bazează pe conexiune) care include facilităţi pentru adresare, specificaţii despre tipul serviciului, fragmentarea şi reasamblarea pachetelor şi securitate.

ICMP şi IGMP sunt considerate ca fiind părţi componente ale IP, de altfel ele sunt arhitectural, nivele peste IP. ICMP trimite rapoarte privind erorile de transmisie, controlul fluxului, primul gateway şi alte funcţii privind mentenanţa şi controlul comunicaţiei. IGMP furnizează modalitati prin care host-urile şi routerele se alătură şi formează un grup multicast.

Siguranţa transferurilor de date este dată în Internet de protocoalele nivelului transport şi anume de Transmission Control Protocol (TCP), care furnizează retransmisia între sursă şi destinaţie, resegmentarea şi controlul conexiunii. Serviciile care nu se bazează pe conexiune de nivel transport sunt oferite de User Datagram Protocol (UDP).

Internet Control Message Protocol (abreviat ICMP) este un protocol din suita [TCP/IP](https://ro.wikipedia.org/wiki/TCP/IP) care folosește la semnalizarea și diagnosticarea problemelor din [rețea](https://ro.wikipedia.org/wiki/Re%C8%9Bea). Protocolul este definit in [RFC792](http://www.ietf.org/rfc/rfc792.txt). Mesajele ICMP sunt încapsulate în interiorul pachetelor [IP](https://ro.wikipedia.org/wiki/IP). Versiunea ICMP ptr IPv4 este adesea cunoscuta ca ICMPv4; in schimb [IPv6](https://ro.wikipedia.org/wiki/IPv6) dispune de un protocol similar cunoscut sub abrevierea ICMPv6.

ICMP este cel mai utilizat in interogările de ping si traceroute.

Ping trimite mesaje ICMP de tip “[echo](https://ro.wikipedia.org/w/index.php?title=Echo_(comunica%C8%9Bii)&action=edit&redlink=1) request” către [calculatorul](https://ro.wikipedia.org/wiki/Computer) destinatar și așteaptă de la acesta mesaje ICMP de tip “echo reply” (răspunsul de tip ecou). Dacă acestea nu sunt primite, se poate presupune că ceva este în neregulă cu conexiunea dintre cele două calculatoare.

Toate [pachetele](https://ro.wikipedia.org/w/index.php?title=Pachet&action=edit&redlink=1) IP au în antet un câmp special numit [TTL](https://ro.wikipedia.org/w/index.php?title=TTL&action=edit&redlink=1) (Time To Live). Acest câmp este decrementat de fiecare dată când trece printr-un [ruter](https://ro.wikipedia.org/wiki/Ruter). Pentru a evita buclele de routare, în momentul în care câmpul TTL ajunge la zero, este trimis de catre routerul care l-a decrementat ultima data un mesaj de tip “time exceeded” catre calculatorul-sursă şi pachetul nu este trimis mai departe. Programul [traceroute](https://ro.wikipedia.org/wiki/Traceroute) foloseşte acest mecanism și trimite către calculatorul destinatar, pachete [UDP](https://ro.wikipedia.org/wiki/User_Datagram_Protocol) cu valori ale câmpului TTL din ce în ce mai mari, pentru a obține mesaje time exceeded de la toate routerele din componenţa reţelei ce crează traseul.

*Structura segmen****u****ului ICMP*

* Antetul

Antetul (headerul) ICMP începe după antetul IPv4. Toate pachetele ICMP au de un antet de 8 octeți și o secțiune de date utile de lungime variabilă.

* Tip - tipul pachetului ICMP
* Cod - subtipul pachetului ICMP în funcție de tipul selectat anterior
* Suma de control - Calculată în funcție de câmpurile antet ICMP, şir de date (este descrisa în [RFC 1071](http://tools.ietf.org/html/rfc1071)).
* Restul antetului - câmp de 4 octeți ce variază ca și conținut pe baza tipului/codului antetului ICMP.

Protocolul ICMP

 ICMP (Internet Control Message Protocol) este un protocol din suita TCP/IP care foloseşte la semnalizarea şi diagnosticarea problemelor din reţea.

 Mesajele ICMP sunt încapsulate în interiorul pachetelor IP.

|  |  |
| --- | --- |
| IP header | ICMP mesaj |

**Pachet IP**

Încapsularea mesajelor ICMP într-un pachet IP

ICMP poate genera un număr mare de pachete care trimise în reţea către o destinaţie pot întoarce informaţii utile unor soft-uri de monitorizare sau administratorului de sistem al reţelei, la optimizarea şi depanarea software şi hardware a reţelei.

|  |  |  |
| --- | --- | --- |
| Tip | Cod | Suma de control |
| Conţinutul mesajului  |

Formatul protocolului ICMP

Există o serie de mesaje ICMP, dintre care cele mai importante sunt:

-Mesajul (Destination Unreachable) DESTINAŢIE INACCESIBILĂ- folosit atunci când subreţeaua sau un anumit router nu pot localiza destinaţia, sau un pachet nu poate fi livrat

-Mesajul  ([Time Exceeded](https://en.wikipedia.org/wiki/ICMP_Time_Exceeded)) TIMP DEPĂŞIT – trimis când un pachet este eliminat datorită contorului său ajuns în zero.

-Mesajul (Parameter Problem: Bad IP header) PROBLEMĂ DE PARAMETRU – indică detectarea unei valori nepermise într-un câmp din antet.

-Mesajul (Source Quench)OPRIRE SURSĂ - folosit pentru a limita traficul hosturilor ce trimit prea multe pachete.

-Mesajul (Redirect Message)REDIRECTARE –este folosit atunci când un router crede că un pachet este dirijat greşit.

-Mesajele  ([Echo Request](https://en.wikipedia.org/wiki/Ping_%28networking_utility%29)  & [Echo Reply](https://en.wikipedia.org/wiki/Ping_%28networking_utility%29))CERERE ECOU şi RĂSPUNS ECOU - folosite pentru a observa dacă o anumită destinaţie este accesibilă şi activă.

-Mesajele (Timestamp& Timestamp Reply)CERERE AMPRENTĂ DE TIMP şi RĂSPUNS AMPRENTĂ DE TIMP – folosite pentru a măsura performanţele reţelei. Cele două mesaje sunt similare, cu excepţia faptului că în răspuns sunt înregistrate timpul de sosire a mesajului şi de plecare a răspunsului.

**Interactiunea intre IPV4 si nivelul legatura de date**

**OSI (Open System Interconnection)** este un model dezvoltat de **ISO (International Organization for Standardization)** pentru a standardiza aparatura din care este alcatuită o reţea. Practic, orice dispozitiv construit după regulile definite de OSI poate funcţiona într-o reţea de echipamente făcute de alţi producători care respectă standardul. Este un **model abstract de referinţă,**  ce este pus în practică de seturi de protocoale precum TCP/IP.

Ideea fundamentală a OSI este împărţirea unui sistem de comunicaţii în mai multe grupări, denumite **layere (nivele)**. Fiecare nivel din stiva creată, interacţionează doar cu cel aflat deasupra lui (căruia îi realizează un serviciu) şi cu cel de dedesubt (căruia îi cere un serviciu). Avantajele sunt numeroase: practic un sistem complex este divizat în multe sub-sisteme, fiecare fiind independent (în afară de interacţiunea specificată mai sus) şi având un anume rol bine definit, printr-un set de funcţii. Orice modificare sau dezvoltare are loc la un anume nivel şi nu crează necesitatea de a schimba tot sistemul, ci doar o anumita parte din el.

**OSI este împărţit în 7 nivele/layere**, un layer N aducând servicii layerului N+1 şi cerând de la N-1.

* **Layerul 1(Physical) :** defineşte specificaţiile fizice şi electrice pentru dispozitive
* **Layerul 2 (Data Link) : Într-o reţea reţine** procedurile şi funcţiile necesare transferului de date
* **Layerul 3(Network):** acest nivel se ocupă de transferul pachetelor sale (numite **Packets sau** PDU-uri) între dispozitive aflate în reţele diferite, prin funcţii de reasamblare, rutare şi fragmentare.
* **Layerul 4(Transport):** acest nivel se ocupă cu transmisia datelor între end-device-uri şi controlează fiabilitatea legăturilor prin controlul fluxului de date, a erorilor şi prin segmentare (la acest nivel PDU-ul se numeşte **Segment**).
* **Layerul 5: Session** -controlează dialogul între două dispozitive (dintre aplicaţia locală şi cea remote). Se definesc proceduri de începere, menţinere, terminare, resetare a transmisiilor (acestea pot fi simplex/ half-duplex/ full-duplex).
* **Layerul 6: Prezentare**-Acest nivel rezolvă diferenţele ce pot apărea din cauză că diverse aplicaţii pot folosi sintaxe şi semantici diferite.
* **Layerul 7: Application**- Nivelul cel mai aproape de utilizator, care interacţionează direct cu software-ul ce trebuie să aibă acces la reţea. Aici se identifică partenerii ce vor sa comunice, se determină câte resurse sunt alocate şi se sincronizează comunicaţia.

Stratul “reţea” separă atât domeniile de coliziune (strat fizic), cât şi domeniile de broadcast (strat legătură de date). În acest strat, o adresă fizică MAC, hardware este translatată în adresă rutabilă (IP - Internet Protocol, sau IPX - Netware, AppleTalk)

Pachetele sunt pasate la nivelul “Legatură de date”, unde are loc adresare fizica a datelor, denumite frame-uri. In cadrul retelelor de tip LAN(Local Area Network), cea mai des folosită adresa este adresa MAC, specifică protocolului Ethernet. Adresa de nivel “Legatură de date” este:

* plata (nu are o structura ierarhica)
* fizica (înscrisă în ROM-ul plăcii de reţea, numită şi adresă BIA – Burned in Address)
* locala (se poate schimba pe fiecare segment din reteaua locală)

Adresa MAC este o adresă pe 48 de biţi şi se reprezintă sub forma a 12 cifre hexazecimale. Adresa MAC destinaţie va fi determinată dupa urmatoarele criterii:

* daca sursa şi destinaţia fac parte din aceiaşi subreţea, atunci adresa MAC destinaţie va fi cea a dispozitivului destinaţie
* daca sursa şi destinaţia nu fac parte din aceiaşi subreţea, atunci adresa MAC destinaţie va fi adresa default gateway-ului, mai exact adresa MAC de pe interfata fa0/0 a router-ului R1.

Pentru a verifica dacă se află pe acelaşi subnet cu destinaţia, clientul va compara rezultatul operaţiunii de aplicare a operatorului “AND” între IP-ul său şi subnet-ul maştii asociate şi rezultatul aplicării operatorului “AND” intre IP-ul destinatie si subnet maştii sale (clientul). Daca cele doua rezultate sunt identice, cele doua dispozitive fac parte din aceiaşi subreţea, si sursa va trimite direct frame-urile catre destinaţie. Daca rezultatele nu sunt identice, atunci sursa va trimite frame-urile către “default gateway”, care se va ocupa de ajungerea lor la destinaţie.

În momentul de faţă, procesul de încapsulare a luat sfarşit, datele fiind plasate pe mediul de transmisie la nivelul “Fizic”.

 Stratul aplicatie insereaza un antet (header) în pachetul de date, identificând gazda si portul destinatie. Protocolul host to host, în functie de aplicatie TCP sau UDP, segmentează acest bloc de date în fragmente care au fiecare un antet TCP. Noua structura se numeste segment TCP. Fiecare segment este trimis protocolului IP, care îi adauga antetul propriu (adrese IP, tipul protocolului de nivel superior etc). Apoi pachetul este trimis stratului Legaturi de Date (nivelul 2).

Clientul web primeste frame-urile, le decapsuleaza la nivelul “Legatură de date”, la nivelul “Reţea” şi la nivelul “Transport” unde plasează pagina primită de la serverul web către browser pentru a fi afişată şi prezentată utilizatorului.

**2. Protocolul Internet versiunea 6**

Creşterea explozivă a nodurilor conectate la Internet a determinat apariţia unor probleme a căror soluţionare devine obligatorie într-un timp cât mai scurt:

* iminenta terminare a spaţiului de adrese IPv4;
* necestitatea de a dirija/ruta trafic între un număr tot mai mare de reţele care formează Internetul.

Protocolul IPv4 defineşte adrese pe 32 de biţi, rezultând un număr de maxim 232 (4.294.967.296) adrese. Alocarea spaţiilor de adrese nu a fost făcută în mod eficient, acest lucru constituind în prezent un alt motiv care determină iminenta epuizare a adreselor IPv4. A doua problemă este cauzată de creşterea dimensiunii tabelelor de rutare. Routerele care formează coloana vertebrală (backbone) a Internetului trebuie să memoreze informaţii complete de rutare. Problema rutării nu se rezolvă doar prin instalarea unor memorii suplimentare în routere cu scopul de putea stoca tabele de rutare mai mari; în plus, este nevoie şi de putere de calcul sporită, astfel încât să nu fie eliminată nici o rută din cauza creşterii volumului de trafic şi a intrărilor în tabele de rutare. Soluţia acestor probleme constă în implementarea noului protocol IPv6 (IP Next Generation – IPng).

 IPv6 are urmatoarele avantaje în comparatie cu IPv4

* managementul si delegarea adreselor devine mai usoara;
* autoconfigurarea usoara a adreselor;
* IPsec încorporat;
* rutare optimizata;
* depistarea adreselor duble.

**2.1 Arhitectura de adresare a IPv6**

Proiectul IPng a rezultat in IPv6 in 1995. Pe langa adresele sursei si destinatiei si alte informatii fiecare pachet IP contine si un numar de versiune. Din motive nestiute pachetele curente IP sunt versiunea 4 iar primul numar de versiune valabil pentru noul protocol era 6. Astfel, vechiul IP este acum numit IPv4 iar cel nou este IPv6. Pe langa autoconfigurare si alte detalii minore, IPv6 suporta in primul si cel mai important rand adrese mai mari. Mult mai mari. 40 sau 48 biti ne-ar fi dat mai mult de un trilion sau respectiv 281 trilioane de adrese, iar 64 biti ar fi fost un numar rotund. Dar IETF au optat pentru 128 biti. Numaru total de posibile adrese ce ne sunt astfel oferite este:

340.282.366.920.938.463.463.374.607.431.768.211.456

Adresele IPv4 sunt scrise prin impărțirea lor in 4 valori pe 8 biți și adăugarea punctelor intre ele, de exemplu 192.0.2.31. Adresele IPv6 pe de altă parte, sunt scrise ca 8 valori pe 16 biți cu două puncte (:) între ele, iar fiecare valoare de 16 biți este afișată în hexazecimal. Un exemplu de adresă IPv6 este 2001:db8:31:1:20a:95ff:fef5:246e. Nu este neobișnuit ca adresele IPv6 să aibă secvențe consecutive de zerouri. In aceste cazuri, exact una dintre acele secvențe poate fi eliminată. Astfel,2001:db8:31:0:0:0:0:1 devine 2001:db8:31::1 iar adresa loopback IPv6 0:0:0:0:0:0:0:1 devine ::1.

Deşi în aproape toate privinţele IPv6 este tot IP şi funcţionează în mare măsură la fel ca IPv4, noul protocol se depărtează de IPv4 în unele privinţe. Cu IPv4 este nevoie de un server DHCP pentru a-ţi spune adresa ta dacă nu vrei să o configurezi manual. Acest lucru funcţionează foarte bine dacă este un singur server DHCP, dar nu la fel dacă sunt mai mult de unul şi oferă informaţii conflictuale. Poate de asemenea să fie greu să se obţină aceeasi adresă după rebooturi cu DHCP. Cu IPv6, DHCP este în mare măsură inutil datorită autoconfigurării stateless (stateless autoconfiguration). Acesta este un mecanism prin care routerii trimit “router advertisements” (RA) ce conţin primii 64 de biţi ai unei adrese IPv6, iar hostul generează restul de 64 de biţi pentru a forma o adresă completă.
  Tradiţional, ultimii 64 de biţi ai unei adrese IPv6 sunt generaţi de la o adresă MAC prin înlocuirea unui bit şi adăugarea biţilor ff:fe în mijloc. Astfel, adresa Ethernet MAC 00:0a:95:f5:24:6e devine 20a:95ff:fef5:246e ca ultima parte a unei adrese IPv6, parte numită “interface identifier”. Astfel, dacă toate routerele trimit acelaşi prefix pentru primii 64 de biţi, hostul va configura mereu aceeaşi adresă IPv6 pentru el însuşi. Nu este necesară niciun fel de configurare, nici pe host nici pe serverul DHCP. În mod alternativ, un host poate genera adresa IPv6 folosind un număr aleator pentru ca adresa MAC să rămână ascunsă faţă de restul Internetului. Windows foloseşte acest tip de adrese pentru outgoing sessions pentru a îmbunătăţi siguranţa. Alte sisteme de operare pot de asemenea genera aceste adrese temporare (una noua este generată la fiecare 24 de ore) dar nu fac asta implicit.
  Când un router trimite mai multe prefixuri de adresă, sau mai multe routere trimit prefixuri diferite, hosturile pot pur şi simplu crea adrese de la fiecare din aceste prefixuri. Routerele pot face ca hosturile conectate la ele să modifice adresa IPv6 prin eliminarea vechiului prefix şi folosirea celui nou.
  Deşi protocolul DCHPv6 (versiunea IPv6 a DHCP) poate atribui adrese IPv6 în acelaşi mod cum serverele DHCP IPv4 atribuie adrese IPv4, nu s-au întalnit servere sau clienţi DHCPv6 ce folosesc această proprietate. Cu IPv6, DHCP este folosit în special pentru a distribui informaţii adiţionale precum adrese de servere DNS, deşi va exista un mod de a face asta prin RA în curând micşorând şi mai mult nevoia de DHCP în IPv6.

**2.2 Pachete IPv6**

În IPv6, antetul pachetului și procesul de forwardare a pachetelor de către routere au fost simplificate. Deși antetele de IPv6 sunt de 2 ori mai mari decât cele de IPv4, procesarea pachetelor este mai eficientă:

* Antetul de IPv6 a fost simplificat prin mutarea câmpurilor rar folosite în antete de extensie opționale.
* Routerele IPv6 nu fragmentează pachetele. Gazdele cu IPv6 trebuie ori să descopere dimensiunea maximă a pachetelor acceptate de toate ruterele de pe cale, să fragmenteze pachetele la capetele transmisiunii sau să folosească un MTU de 1280 de octeți, care este minimul acceptat de protocol.
* Antetul IPv6 nu este protejat de o sumă de control (checksum), făcându-se presupunerea că integritatea datelor este asigurată atât la nivelul legătură de date, cât și la nivelul transport. În acest fel, routerele IPv6 nu trebuie să recalculeze suma de control atunci când schimbă unul din elementele pachetului.
* Câmpul *TTL* din IPv4 a fost redenumit în *Hop Limit*, deoarece ruterele nu mai trebuie să calculeze timpul petrecut de pachet în cozile dispozitivelor de rețea.

****

**Fig.3 Antet Ipv6**

* Version (Versiune) -4 biți - Identifică versiunea protocolului IP care generează pachetul.
* Traffic Class / Flow Label (Clasă de trafic şi Etichetă flux) – 8 biți, respectiv 20 biți - câmpuri pentru definirea politicilor de Quality of Service; deşi nu s-au definit utilizări explicite ale acestor două câmpuri, s-a intenţionat utilizarea acestora într-un context asemănător “multiplexării” de fluxuri.
* Payload Length (Lungime date)- 16 biți - Acest câmp specifică lungimea câmpului de date, măsurată în octeţi.
* Next Header (Următorul antet) – 8 biți - Reprezintă un pointer către (următorul eventual) antet opţional; fiecare extensie include un câmp Următorul antet, care localizează următoarea extensie; câmpul Următorul antet din ultima extensie localizează datele utile;
* Hop Limit (Limită de hop-uri) - 8 biți - Are rol asemănător câmpului TTL din antetul pachetului IPv4; elimină necesitatea ca routerele să calculeze timpul de stocare a unui pachet;
* Câmpurile de adrese – câte 128 biți fiecare - Conţin adresele de reţea (IPv6) a sistemului sursă şi a sistemului destinaţie. Aceste câmpuri nu sunt modificate la trecerea pachetelor prin routere.

**

**Fig 4. Diferențele dintre antetul IPv4 si antetul IPv6**

**2.3 ICMP pentru IPv6**

Un rol foarte important pentru folosirea stivei IPv6 îl deține protocolul ICMP. Cum am văzut mai devreme, structura pachetului IPv6 este asemănătoare cu cea pentru IPv4. Pachetele de tip ICMP sunt referențiate in antetul de nivel 3 prin valoarea 58 atribuită câmpului “Următorul antet”.



**Fig 5. Structura pachetului ICMP**

 Cele mai importante mesaje ICMP folosite pentru funcționarea corectă a protocolului IPv6 sunt:

* Mesaje de eroare :
	+ **Destination Unreachable –** Mesaj folosit atunci cand pachetul trimis nu poate ajunge la destinație
	+ **Time Exceeded** – Mesaj trimis atunci de către un router atunci când valoarea câmpului Hop Limit ajunge la 0.
* Mesaje de informare:
	+ **Echo Request –** Mesaj folosit pentru diagnosticarea rețelei
	+ **Echo reply –** Mesaj trimis ca răspuns la Echo Request.

**2.4 Interacțiunea Ipv6 cu nivelul legătură de date**

 Apariția IPv6 a produs o schimbare a protocoalelor la nivelul stivei OSI. Astfel, protocoalele implementate la nivelul 3 au fost înlocuite cu **Neighbor Discovery Protocol (NDP)**. NDP introduce funcții de tipul descoperire a următorului hop, descoperire router, detecție adrese duplicat, rezolvare adrese, descoperire parametri. Protocolul NDP se bazează pe cinci tipuri de mesaje ICMP:

* Router Solicitation (RS) – tip 133
* Router Advertisement (RA) – tip 134
* Neighbor Solicitation (NS) – tip 135
* Neighbor Advertisement (NA) – tip 136
* Route Redirection – tip 137

Majoritatea acestor mesaje pot fi trimise atât către o adresa unicast, cât și către o adresă multicast.

**Concluzii**

Mesajele ICMP sunt transmise ca datagrame si constau dintr-un antet IP care incapsuleaza date ICMP. Mesajele ICMP contin intregul antet IP al mesajului original sustinand astfel identificarea usoara a pachetului pierdut.

ICMP-ul a fost folosit pentru a executa atacul de tip serviciu- respins ( „ ping-ul mortii”), trimitand un pachet IP mai mare decat numarul de biti permis de protocolul IP

In Ipv6, ICMP-ul este foarte important, fiind o parte integrata, deoarece pe langa mesajele de baza pe care le furnizeaza si in Ipv4, IPv6 are mesaje ICMP noi. Functionalitatea ARP in IPv4 a fost inlocuita cu ICMP 135& 136 („Descoperirea vecinilor”) si ICMP 133& 134 („Descoperirea Routerelor”).

Fragmentarea in IPv6 este facuta doar la capete, nu pe traseul intermediar. Pentru a semnaliza ca un pachet are nevoie sa fie fragmentat, un ICMP de tipul 2, „Pachet prea mare” este trimis sursei care l-a emis dupa ce prima data este trimis si pierdut. De aceea, pachetele ICMP de tipul 2 au nevoie sa fie acceptate in retea, chiar si cu mesaje de la adrese externe, altfel fragmentarea va fi corupta.

Pentru IPv6 fragmentarea apare la 1280 de octeti, fiind o valoare considerabil mai mare, comparata cu 576 octeti, cat ar fi fost pentru IPv4, astfel evitandu-se fragmentari dese.

Pentru Ipv4, o parte din mesajele ICMP sunt permise de firewall. Regula generala este ca se permit mesajele ICMP din Internet intr-un DMZ, de un firewall si sunt respinse de catre dispozitivul pe care se afla firewallul. In schimb, ICMPv6 permite mesaje aditionale nu doar prin firewall-ul dispozitivului, dar si pentru mesajele trimise catre sau de la dispozitiv.

Mesajele ICMPv6 sunt vitale pentru functionarea corecta a IPv6 si pentru firewall-ul transparent trebuie sa fie capabile sa urmareasca mesajele ICMPv6 care parcurg vecinii, sa detecteze adresele duplicate, sa se autoconfigureze si sa aiba un management multicast, astfel reducandu-se atacurile IP-la-MAC.

**Bibliografie**

<https://www.afrinic.net/en/services/statistics/ipv4-resources>

<https://www.scribd.com/doc/180751273/31/Pachete-IPv4>

<http://andrei.clubcisco.ro/cursuri/f/f-sym/3rl/cursuri2012/RL_curs_04.pdf>

<http://www.runceanu.ro/adrian/wp-content/cursuri/retele2013/RC_C6_2013.pdf>

<http://documents.tips/documents/sistemul-de-adrese-ipv4-si-ipv6-dragan-d-cristian-bogdan.html>

<http://www.cs.cmu.edu/~mihaib/articles/internet/internet-html.html>

<http://vega.unitbv.ro/~zaharia/tdrcii/TDRC_II-06-IP.pdf>

<http://www.unibuc.ro/prof/niculae_c_m/telecom/internet_prot_ip.htm>

<http://wbt.unitbv.ro/web/moodle/file.php/1/Ghiduri/Retele_de_comunicatii_date.pdf>

<http://ittx.ro/author/mihai-dumitrascu/>

<http://www.inforetele.com/ccna/modelul-osi/>

http://gate.upm.ro/retele/ourse\_Labs/Lab/IPAddressing\_Subnet\_VLSM\_CIDR\_Subnet/Adresarea\_IP.pdf

http://www.retele-cibernetice.ro/IPv6.php

http://calin.comm.pub.ro/Didactice/ARI/Notite%20curs/Notite/par2\_2\_Niv%203%20-%20IPv6.pdf

http://ipv6.com/articles/general/IPv6-Header.htm

<http://www.one-it.ro/blog/ipv6-vs-ipv4-noua-generatie-de-adrese-internet-protocol/>

<http://ipv6.com/articles/general/IPv6-Header.htm>

http://searchnetworking.techtarget.com/definition/ICMP

http://www.seanconvery.com/v6-v4-threats.pdf