

Nivelul Rețea în Internet

Studenți:

SORESCU- MOREELS Raluca- Elena

VASILE Alin- Florentin

Grupa: 441A

Profesor coordonator:

Conf.Dr.Ing. Ștefan STĂNCESCU

Cuprins

Cuprins.....	2
1. Introducere.....	3
1.1. Istoria Internetworking-ului (Raluca Sorescu).....	3
1.2. Cum diferă rețelele și cum pot fi conectate (Alin Vasile)	5
1.2.1. Rețele locale (LAN- Local Area Network).....	5
1.2.2. Rețele de arii largi (WAN- Wide Area Network).....	6
1.2.3. Rețele Metropolitane (MAN- Metropolitan Area Network)	6
2. Programele de rețea (Rețele de Calculatoare) (Alin Vasile)	7
2.1. Ierarhiile de protocoale	7
2.2. Servicii orientate pe conexiuni și servicii fără conexiuni	8
2.3. Relația dintre servicii și protocoale	8
3. Protocoale de control în Internet și modul lor de funcționare (Raluca Sorescu).....	9
3.1. Protocolul Mesajelor de Control din Internet (ICMP- Internet Control Message Protocol) ...	9
3.2. Protocolul de rezoluție a adresei (ARP – Address Resolution Protocol)	11
3.3. Protocolul de rezoluție inversă a adresei (RARP – Reverse Address Resolution Protocol)...	13
4. Bibliografie	14

1. Introducere

Lucrarea de față își propune să prezinte o serie de aspecte atât teoretice, cât și practice, legate de nivelul rețea în Internet.

1.1. Istoria Internetworking-ului

Interworking-ul este o colecție de rețele individuale, conectate prin diferite dispozitive intermediare, precum routere sau dispozitive gateway. Această colecție funcționează ca o singură rețea și asigură comunicarea între rețele, folosind în principal, protocolul Internet Routing Protocol. Internetworking-ul este realizabil doar dacă rețelele conectate folosesc aceeași stivă de protocoale sau aceleași metodologii de comunicare.

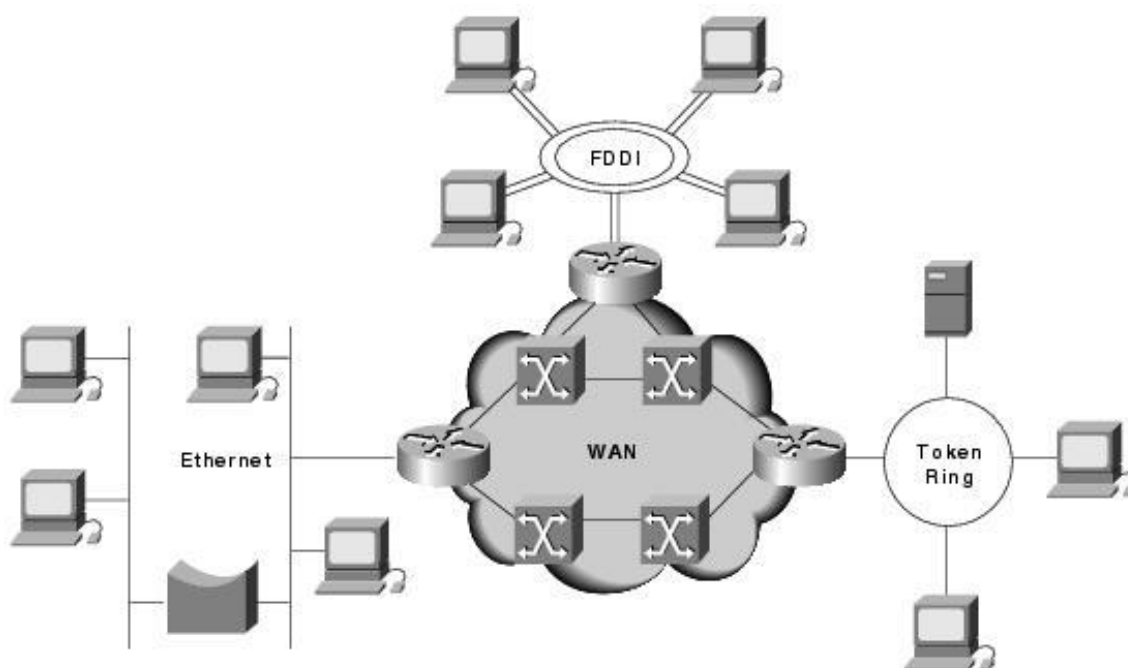


Figura 1. Exemplu de rețele interconectate - Internetworking¹

Dezvoltarea acestei colecții de rețele a început în 1969, atunci când s-a realizat o legătură între Universitatea California-Los Angeles și Institutul de Cercetare Stanford. Această legătură s-a realizat cu ajutorul unei rețele numită ARPANET- Advanced Research Projects Agency Network. Ulterior, aceasta a fost extinsă prin adăugarea a încă două noduri de rețea, unul la Universitatea California- Santa Barbara, iar celălalt la Universitatea Utah.

¹ http://docwiki.cisco.com/wiki/File:Technology_Handbook-01-2-01.jpg

Nouă ani mai târziu, colaborarea dintre firma de comunicații Tymnet și compania de servicii financiare și comunicații Western Union Internațional a făcut posibilă realizarea primei rețele de comutație de pachete la nivel internațional. Această rețea este cunoscută sub numele de IPSS- International Packet Switched Service și a avut o expansiune exponențială în Europa și SUA, astfel încât în anii 1990 aceasta a fost extinsă la nivel global. Astfel a apărut necesitatea unui protocol de rețea, deoarece era nevoie de un sistem de reguli și convenții pentru a fi asigurată comunicarea între dispozitivele atașate la rețea. Principalele neconcordanțe care puteau apărea sunt:

- Temporizarea;
- Formatul pachetelor;
- Inițierea și finalizarea transferului de date;
- Contorul pentru erori;

Protocolul principal pe care actualele rețele interconectate îl folosesc este IP-Internet Protocol. Aceste rețele sunt de trei tipuri:

- Intranet
- Extranet
- Internet

Primele două tipuri, Intranet și Extranet, nu sunt rețele care depind în mod direct de accesul la Internet. În cazul în care se dorește conexiunea acestora la Internet, atunci administratorii acestor rețele trebuie să asigure un nivel ridicat de securitate, pentru a putea preveni accesul neautorizat.

1.2. Cum diferă rețelele și cum pot fi conectate

În subcapitolul acesta vom prezenta pe scurt, caracteristicile principale ale rețelelor.

1.2.1. Rețele locale (LAN- Local Area Network)

Local Area Network este o rețea care acoperă o zonă geografică restrânsă, cum ar fi o clădire sau un campus restrâns. Aceasta utilizează o tehnologie de transmisie reprezentată de un singur cablu la care sunt atasate toate dispozitivele. În prezent, conform standardului IEEE 802.3 viteza de operare a LAN-urilor este de peste 400Gbit/s.²

Proprietăți LAN:

- Viteză mare de transfer
- De regulă, este administrată de o singură organizație sau individual
- Interconectează dispozitive pe o arie restrânsă

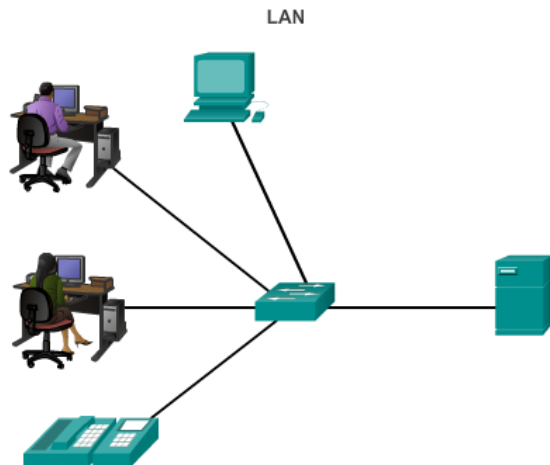


Figura 2. Exemplu rețea LAN³

Rețelele de calculatoare pot fi conectate prin diferite metode: prin fibră optică, Ethernet, Wireless LAN, HomePNA sau Power line.

² Un Gigabit este echivalentul a 10^9 biți, nu a 1,073,741,824 biți

³ Curs CCNA1

1.2.2. Rețele de arii largi (WAN- Wide Area Network)

Rețelele de tipul WAN acoperă zone geografice mari. Acestea asigură accesul la alte rețele locale, interconectate pe o zonă întinsă. De obicei, administrarea acestui tip de rețele este realizată cu ajutorul mai multor furnizori (SP - Service Provider sau ISP- Internet Service Provider).



Figura 3. Exeplu rețea WAN

1.2.3. Rețele Metropolitane (MAN- Metropolitan Area Network)

O rețea MAN este o versiune extinsă a LAN-urilor și utilizează în mod normal tehnologii similare acestora. În ceea ce privește întinderea MAN-urilor, putem spune că aceasta cuprinde în întinderea sa orașe întregi. (cf. IEEE802-2001)

Acestea oferă un transfer înalt de date și în general este administrată de un singur operator.

2. Programele de rețea (Rețele de Calculatoare)

2.1. Ierarhiile de protocoale

Pentru reducerea complexității programelor care trebuie să ruleze într-o rețea, s-a decis ca este necesară organizarea acestora sub forma unei ierarhii, această ierarhie purtând numele de stivă de protocoale. Această stivă este prezentată sub forma unor straturi, fiecare strat având rolul de a oferi diverse servicii stratului imediat superior. Pastrand structura de ierarhie cel mai bun mod de funcționare este acela în care fiecare strat superior nu trebuie să cunoască detalii despre implementarea structurilor din straturile inferioare. Într-o astfel de ierarhie, structura de pe un anumit nivel al unei mașini trebuie să comunice cu o structură de pe alta mașină situată obligatoriu la același nivel ierarhic. Între două niveluri consecutive în ierarhia de protocoale trebuie să existe o interfață care definește ce fel de servicii oferă nivelul inferior celui superior. Acesta este cel mai avantajos mod de organizare deoarece oferă fiabilitate și în cazul în care se aduc modificări pe unul dintre nivele. De asemenea, structura ierarhică permite modificarea unor elemente dintr-un nivel fără a necesita modificări multiple în cadrul celorlalte nivele cu o singură condiție, aceea de a exista între nivele o interfață foarte bine definită.

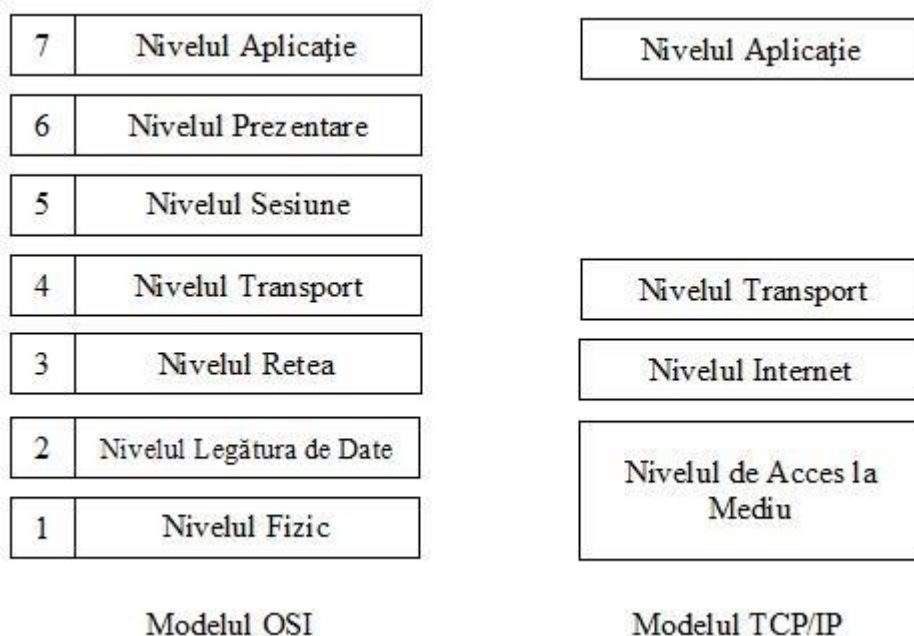


Figura 4. Stivele OSI și TCP/IP

2.2. Servicii orientate pe conexiuni și servicii fără conexiuni

Fiecare nivel din stiva OSI poate să ofere nivelului de deasupra două tipuri de servicii. Cele două servicii sunt împartite în două categorii: orientat pe conexiune și fără conexiune.

În ceea ce privește serviciul orientat pe conexiune se poate descrie foarte ușor ca fiind serviciul ce se bazează pe realizarea conexiunii între două părți componente ale sistemului și ulterior realizarea transferului de informații între cele două părți. În esență, conexiunea funcționează ca o teavă, emitorul introduce un obiect la unul din capete iar receptorul scoate obiectul la celălalt capăt.

Din punctul de vedere al serviciului fără conexiune, se poate spune că este modelul de bază al sistemului postal deoarece toate mesajele transmise conțin o adresă de destinație și fiecare mesaj circula în mod independent. Cu alte cuvinte nu este necesară realizarea unei conexiuni între cele două puncte finale pentru a realiza un transfer.

Ambele servicii sunt caracterizate printr-un factor de calitate. Serviciile cu conexiune au avantajul primirii tuturor informațiilor de la emitor dar au ca dezavantaj procesul de realizare a conexiunii, proces ce necesită mai mult timp. Pe de altă parte serviciul fără conexiune este mai rapid deoarece informațiile se transmit fără să se stabilească o conexiune anterioară dar nu există certitudinea că informațiile vor ajunge de fiecare dată la adresa dorită.

Ca și în viața reală, nivelul de rețea face anumite compromisuri. Dacă se dorește transmiterea unor fișiere în care este necesar ca fiecare octet transmis să ajungă în aceeași poziție la recepție atunci se utilizează un serviciu cu conexiune care va fi ceva mai lent dar sigur. Într-un sistem de mesagerie se poate implementa foarte ușor un serviciu fără conexiune, serviciu în care se dorește o transmitere a datelor cât mai rapidă cu riscurile aferente. Pentru serviciul fără conexiune s-au adus îmbunătățiri, s-a realizat un sistem timp cerere-răspuns în care emitorul transmite o cerere și așteaptă un răspuns. Cel mai frecvent sistem în care se folosește acest serviciu de tip cerere-răspuns este în cadrul sistemelor client-server.

2.3. Relația dintre servicii și protocoale

De cele mai multe ori serviciile și protocoalele sunt confundate chiar dacă sunt două concepte total distincte. Un serviciu definește operațiile pe care un nivel este pregătit să le realizeze dar nu oferă niciun fel de informații despre implementarea lor. De asemenea un serviciu este definit în contextul unei interfețe între două niveluri. Un protocol este un set de reguli ce are ca obiectiv specificarea felului în care se realizează transmiterea de pachete. Fiecare entitate folosește un protocol pentru a

definii serviciile. Fiecare nivel din stiva poate sa utilizeze orice fel de protocol cu conditia sa nu schimbe serviciul vazut din exterior.

3. Protocoale de control în Internet și modul lor de funcționare

Așa cum a fos prezentat și anterior, protocolul care se folosește pentru schimbul de date este IP-ul (Internet Protocol v4/v6) , însă pentru o mai bună funcționare a rețelei, au fost implementate și câteva protocoale de control, precum ICMP, ARP, RARP și BOOTP.

3.1. Protocolul Mesajelor de Control din Internet (ICMP- Internet Control Message Protocol)

Protocolul Mesajelor de Control din Internet este folosit pentru raportarea problemelor din rețea, semnalizare și diagnosticare. Acesta a apărut ca o îmbunătățire a protocolului Internet (IP), ce conține în interiorul pachetelor sale mesajele ICMP.

3.1.1. Structura segmentului ICMP

Toate pachetele trimise de ICMP dispun de un antet cu dimensiunea de 8 octeți, dar și de o secțiune de date cu o lungime variabilă. Acest antet începe imediat după antetul protocolului Ipc4 și are următoarea structură:

Offsets	Octet	0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Type								Code								Checksum															
4	32	Rest of Header																															

Figura 5. Structura Antetului ICMP⁴

Type - Tipul pachetului ICMP (8 biți)

Code - Subtipul pachetului ICMP; acesta variază în funcție de tipul ales anterior (8 biți)

Checksum- Suma de control se calculează pornind de la câmpurile antet, respectiv date și este resetată la 0 înainte de generare (16 biți)

Rest of Header – Restul antetului conține date bazate pe tipul, respectiv codul antetului ICMP (4 bytes)

⁴ https://en.wikipedia.org/wiki/Internet_Control_Message_Protocol

3.1.2. Principalele tipuri de mesaje ICMP

Tipul mesajului	Descrierea mesajului
Destinație inaccesibilă	Pachetul nu poate fi livrat
Timp depășit	Câmpul timp de viață a ajuns la 0
Problemă de parametru	Câmp invalid în antet
Oprire sursă	Pachet de șoc
Redirectare	Redirectare datagrama rețelei
Cerere de ecou	Întreabă o mașină dacă este activă
Răspuns ecou	Da, sunt activă
Cerere de amprentă de timp	La fel ca cererea de ecou, dar cu amprentă de timp
Răspuns cu amprentă de timp	La fel ca răspunsul ecou, dar cu amprentă de timp

Tabelul 1. Tipurile principale de mesaje ICMP

- Mesajul **„Destinație inaccesibilă”** (Destination unreachable) este generat de un ruter și are rolul de a informa gazda ca destinația nu poate fi localizată.
- Mesajul **„Timp depășit”** (Time exceeded) este generat de gateway și apare atunci când un pachet este eliminat datorită ajungerii contorului său la zero. În principu, acest mesaj apare în cazul unei aglomerări pe o anumită rută sau în cazul în care ceasul a fost inițializat cu o valoare prea mică.
- Mesajul **„Problemă de parametru”** (Parameter Problem: Bad IP header) este generat în mod automat ca un răspuns pentru o eroare neinclusă în câmpul niciunui alt mesaj ICMP. De obicei, acesta indică o eroare în programele IP ale gazdei emițătoare.
- Mesajul **„Oprire sursă”** (Source Quench) este folosit destul de rar, scopul său principal fiind de a limita traficul gazdelor care trimit prea multe pachete. Astfel, când o gazdă primea acest mesaj, era de așteptat să încetinească ritmul de transmisie, însă s-a observat ulterior faptul că acest tip de mesaj ICMP nu ajută foarte mult decongestia rețelei, ci mai mult o îngreuna.
- Mesajul **„Redirectare”** (Redirect) este generat de ruter și are ca scop principal informarea gazdei despre dirijarea greșită a unui pachet.
- Cele două mesaje **„Cerere de ecou”** (Echo Request) și **„Răspuns ecou”** (Echo Reply) se folosesc pentru verificarea accesibilității unei rute. Atunci când se recepționează mesajul ECHO, se va răspunde cu un mesaj RĂSPUNS ECHO.
- În ceea ce privește mesajele **„Cerere de amprentă de timp”** (Timestamp Request) și **„Răspuns cu amprentă de timp”** (Timestamp reply) sunt similare celor două mesaje expuse anterior, diferența majoră dintre ele fiind cele două contoare de timp, de sosire, respectiv de plecare a răspunsului, de care dispun cele din urmă.

3.2. Protocolul de rezoluție a adresei (ARP – Address Resolution Protocol)

Protocolul de rezoluție a adresei este un protocol extrem de important în infrastructura rețelei. Mai exact, acesta este folosit pentru a realiza o mapare dinamică a adresei IP (adresă de rețea) către cea MAC (adresă fizică).

ARP folosește mesaje simple și tocmai de aceea este extrem de folosit. Cele mai întâlnite metode de optimizare a ARP sunt:

Ca o primă metodă de optimizare, putem expune posibilitatea de păstrare a rezultatului, în urma fiecărei execuție a ARP, facilitând astfel comunicarea între două gazde. Data următoare când se va dori recontactarea unei mașini, corespondentul adresei va fi găsit local, fapt ce previne redifuzarea pachetelor de mapare.

O a doua optimizare se referă la difuzarea corespondenței de adrese la pornirea mașinii. Acest lucru este posibil cu ajutorul unui pachet ARP de căutare a propriei adrese IP. În cazul în care se va primi un răspuns, două mașini din rețea dețin aceeași adresă IP, fapt ce împiedică funcționarea noului sistem. Însă, noul sistem este cel care informează administratorul de sistem despre duplicarea adresei IP.

Cererea de ARP: PC1 difuzează o cerere ARP către toate stațiile din rețea.

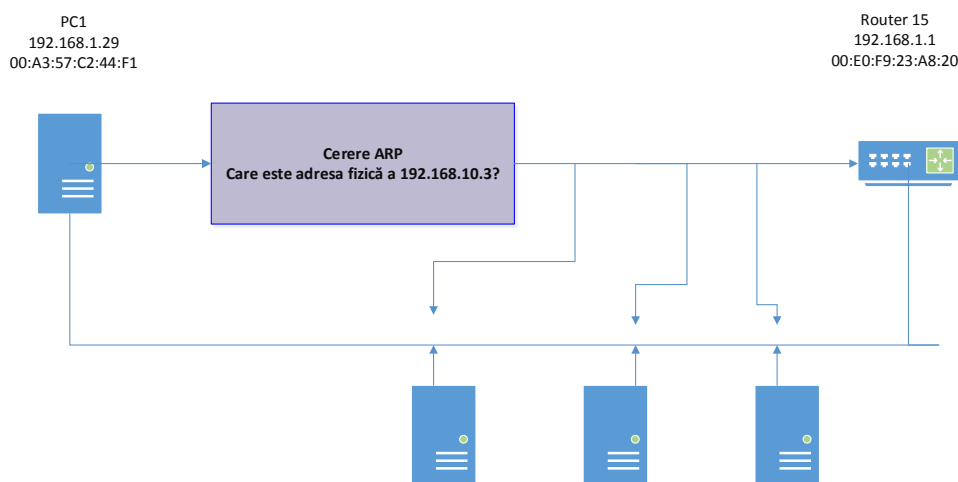


Figura 6. Cerere ARP

Răspunsul ARP: Ruterul 15 răspunde cu un răspuns de tip ARP, ce conține adresa fizică cerută.

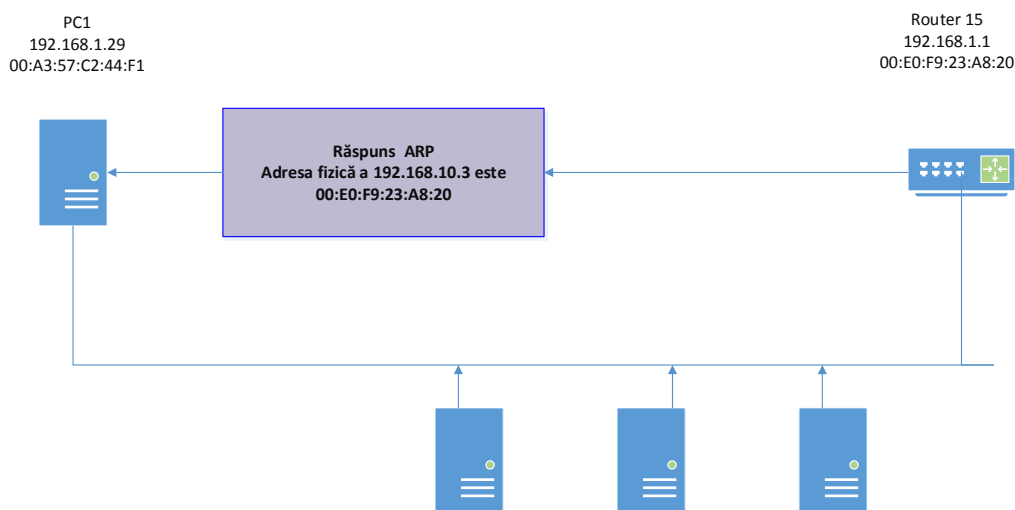


Figura 7. Răspuns ARP

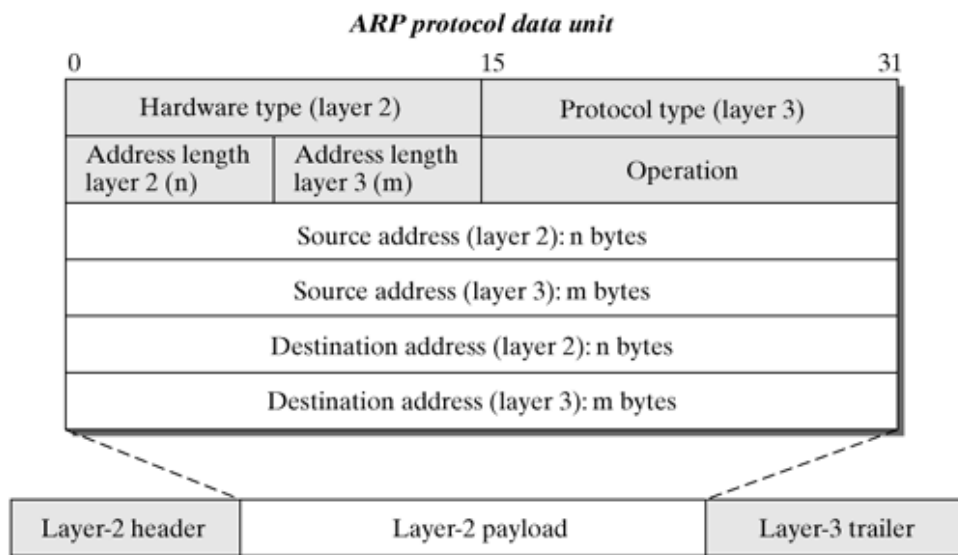


Figura 8. Formatul Pachetului ARP⁵

⁵ <http://flylib.com/books/3/475/1/html/2/images/0131777203/graphics/15fig02.gif>

În Figura 8, se poate observa structura pachetelor ARP. Foarte importante sunt adresele sursă și destinație.

Cerere ARP de la PC1:

- ❖ Adresa fizică a sursei: 00:A3:57:C2:44:F1
- ❖ Adresa IP a sursei: 192.168.1.29
- ❖ Adresa fizică a destinației: 00:00:00:00:00:00
- ❖ Adresa IP a destinației: 192.168.1.1

Răspuns ARP de la Ruter15:

- ❖ Adresa fizică a sursei: 00:E0:F9:23:A8:20
- ❖ Adresa IP a sursei: 192.168.1.1
- ❖ Adresa fizică a destinației: 00:A3:57:C2:44:F1
- ❖ Adresa IP a destinației: 192.168.1.29

3.3. Protocolul de rezoluție inversă a adresei (RARP – Reverse Address Resolution Protocol)

Acest protocol permite unei stații noi să difuzeze adresa sa fizică și să ceară adresa sa IP. În acest caz, serverul RARP caută adresa fizică primită în fișierele sale de configurare și trimite înapoi adresa IP corespunzătoare.

Un dezavantaj al acestui protocol este reprezentat de necesitatea unui server RARP în fiecare rețea.

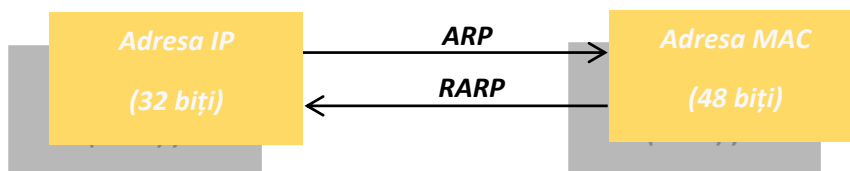


Figura 6. Relația între ARP și RARP

4. Bibliografie

1. http://www.runceanu.ro/adrian/wp-content/cursuri/retele2013/RC_C10_2013.pdf
2. https://sites.google.com/site/sfuicu/rc/rc_lab/wireshark/protocoale
3. http://gate.upm.ro/retele/DOCs-Course_Labs/Curs/Books/Tanenbaum-ComputerNetworks_ed4-RO.pdf
4. <http://www.networksorcery.com/enp/protocol/icmp.htm>
5. Curs Cisco CCNA1
6. https://en.wikipedia.org/wiki/IEEE_802.3
7. <http://www.competentedigitale.ro/it/it10.html>
8. <http://www.eugo.ro/Retele/index.php>