9. Protocolul de rezoluție al adresei. Alocarea adreselor de rețea

Introducere

În unitatea anterioară am discutat despre protocolul IP; alegerea interfeței pe care trebuie retrimisă o datagramă se face analizând tabela de rutare. Rămâne însă de soluționat modul în care o datagrama IP este livrată unui gazde sau unui ruter din acea rețea. Datagramele IP folosesc adrese IP (logice) însă hardware-ul interfeței de rețea foloseşte adrese MAC (fizice) care au o cu totul altă structură. Pentru a putea încapsula o datagramă IP într-un cadru de nivel legătură de date este deci nevoie de un protocol care să translateze adresele logice în adrese fizice.

Adresele IP trebuie să fie unice şi să reflecte structura rețelei. Aşa cum am menționat în unitatea anterioară adresele codifică o porțiune de rețea, care este unică pentru toate gazdele de pe un segment şi o porțiune de gazdă. Astfel nu este posibil ca aceste adrese să fie înscrise în hardware-ul interfeței de rețea aşa cum se întâmplă cu adresele fizice. Adresele IP, măştile de rețea precum şi adresa IP a primului ruter trebuie deci să fie configurabile din software; configurarea se poate face manual sau folosind un protocol dedicat.

Obiective

După parcurgerea acestei unități de învățare studenții vor fi capabili:

- ✓ Să descrie necesitatea protocolului de rezoluție al adresei
- ✓ Să explice funcționarea ARP
- ✓ Să aloce blocuri de adrese IP conform specificațiilor
- ✓ Să descrie funcționarea DHCP

Durată medie de studiu individual

Durata medie de studiu individual : 2 ore

9.1. Protocolul de rezoluție al adresei

9.1.1. Necesitatea ARP

Pornind la de la topologia de rețea din Figura 9.1 să presupunem că o stație gazdă doreşte să transmită un mesaj de nivel aplicație către o altă stație gazdă aflată în aceeaşi rețea. La nivel aplicație identificarea stației gazdă destinație se face de regulă folosind numele de gazdă al acesteia (de exemplu *statia1.kb2.iesc.unitbv.ro*). La sursă mesajul de nivel aplicație este furnizat nivelului transport cu instrucţiunea de al livra aplicației destinație identificată prin adresa IP si un număr de port. Translatarea numelui de gazdă în adresă IP se face folosind sistemul numelor de domenii (DNS). Segmentul de nivel transport este apoi încapsulat într-o datagrama în al cărei antet se înscriu adresa IP sursă şi adresa IP destinație. Următorul pas este încapsularea datagramei într-un cadru de nivel legătură de date (spre exemplu Ethernet). Antetul cadrelor Ethernet conține de asemenea o adresă MAC sursă şi o adresă MAC destinație. Adresa MAC sursă este adresa stației care a generat cadrul; această informație este cunoscută. Adresa MAC destinație este adresa MAC a interfeței de rețea care trebuie să recepționeze acest cadru, adresă necunoscută în acest context (Figura 9.2). În astfel de cazuri se apelează la un protocol dedicat care cunoscând adresa IP poate determina adresa MAC. Protocolul care îndeplineşte această sarcină se numeşte Protocolul de Rezoluție al Adresei(eng. Address Resolution Protocol, ARP, RFC 826) el fiind conținut în stiva TCP/IP.

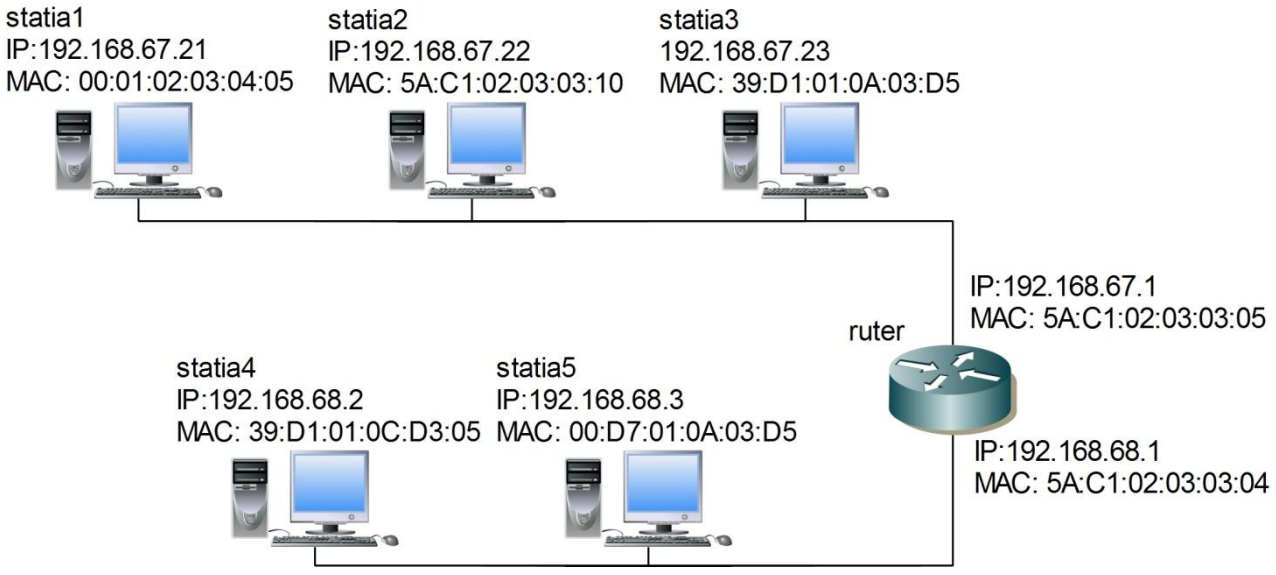

Figura 9.1 Interfețe de rețea cu adrese logice şi adrese fizice

Menționăm că există şi posibilitatea creării manuale a unui fişier static prin care se specifică corespondența dintre adresele IP şi adresele de nivel doi, însă pentru rețele mari sau rețele cu gazde mobile actualizarea fişierelor este o acțiune consumatoare de timp şi care poate genera

erori. Astfel de mecanisme au fost folosite în trecut înainte de apariția protocolului ARP sau în rețele în care transmiterea unor cadre de difuzare este considerată costisitoare.

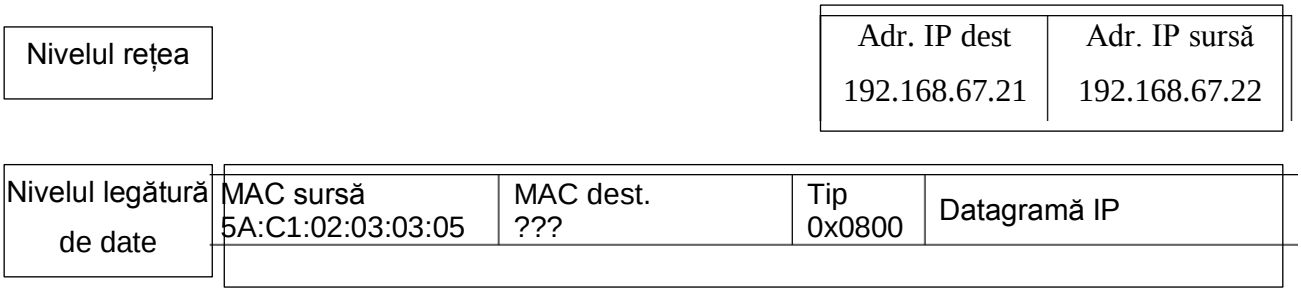

Figura 9.2 Încapsularea datagramelor IP în cadre Ethernet

9.1.2. Funcționarea ARP

ARP se bazează pe construirea şi menținerea unei tabele ARP. O tabelă ARP are rolul de a oferi o corespondență între adresele IP şi adresele MAC. Tabela este construită dinamic fiind stocată în memoria RAM. Există şi mecanisme pentru adăugarea sau ştergea manuală a unei intrări din tabelă, însă acestea sunt rar folosite.

Tabel 9.1 Tabelă ARP

Adresă IP	**Adresă MAC**	**Timp**
192.168.67.21	00:01:02:03:04:05	15:30
IP:192.168.67.1	5A:C1:02:03:03:05	15:32

9.1.3. Comunicația între stații aflate în aceeaşi rețea

Folosind rețeaua din Figura 9.1 să considerăm că toate stațiile, inclusiv ruterul au fost tocmai pornite, astfel încât tabelele ARP nu conțin nici o intrare. Presupunem că statia2 doreşte să comunice cu statia1, cunoscând doar adresa IP a acesteia. La nivelul rețea datele sosite de la nivelul superior vor fi încapsulate, se va adăuga un antet specific (antetul IPv4) ce va conține în câmpul adresă destinație 192.168.67.21 iar în câmpul adresă sursă 192.168.67.22. Pentru a putea încapsula datagrama într-un cadru, adresa IP destinație va fi căutată în tabela ARP şi nefiind găsită se va crea un cadru special (cerere ARP) ce va fi difuzat în rețea. Mai exact acest cadru va avea în câmpul destinație adresa de difuzare la nivel legătură de date FF:FF:FF: FF:FF:FF iar în câmpul sursă adresa MAC a stației 2 (5A:C1:02:03:03:05). Formatul (sintaxa) unui pachet ARP este prezentat mai jos:

Tip hardware		Tip protocol
Lungime hardware	Lungime protocol	Operație
Adresă hardware sursă		
Adresă protocol sursă		
Adresă hardware țintă		
Adresă protocol țintă		

Figura 9.3 Structura pachetelor ARP

Semnificația câmpurilor este următoarea:

Tip hardware (16 biți) specifică tipul interfeței de rețea utilizate (pentru Ethernet valoarea este 0x0001)

Tip protocol (16 biți) specifică protocol de nivel rețea utilizat (pentru IP valoarea este 0x0800)

Lungime hardware (8 biți) specifică lungimea adreselor de nivel doi (pentru adrese EUI- 48 bit valoarea este de 6 octeți). Informația ar putea fi determinată şi din câmpul Tip hardware.

Lungime protocol (8 biți) specifică lungimea adreselor de nivel doi (pentru adrese IPv4 valoarea este de 4 octeți). Informația ar putea fi determinată şi din câmpul Tip protocol.

Operație (16 biți) specifică tipul operației efectuate. Valorile sunt 1 pentru cerere şi 2 pentru răspuns.

Adresă hardware sursă, Adresă hardware țintă specifică adresa fizică a nodului care a generat cadrul şi adresa nodului care trebuie să recepționeze cadrul. Întrucât la transmiterea unui pachet ARP de cerere adresa hardware țintă nu e cunoscută acest câmp se completează cu zerouri.

Adresă protocol sursă, Adresă protocol țintă specifică adresa logică a interfeței care a generat cadrul şi adresa logică a interfeței care trebuie să recepționeze cadrul.

Se poate uşor observa ca anumite informații nu sunt absolut necesare pentru funcționarea protocolului (spre exemplu Lungime hardware poate fi determinată din Tip hardware, Lungime protocol poate fi determinată din Tip protocol, Adresă hardware ţintă e completată cu zerouri în pachetele de cerere etc.), însă ele au fost incluse pentru monitorizare, depanare şi asigurarea unei structuri unitare a pachetelor ARP. Deşi actualmente ARP-ul se foloseşte aproape exclusiv pentru

aflarea adresei MAC de tip EUI-48 cunoscând adresa IPv4, protocolul poate funcționa şi cu alte tipuri de adrese sau protocoale. Menționăm că pentru aflarea adresei MAC pornind de la adresa IPv6 se foloseşte protocolul NDP (Neighbour Discovery Protocol, RFC 2461) care este componentă a ICMPv6 şi nu ARP.

Trimiterea unui pachet ARP

1.Stația sursă caută în tabela ARP adresa de nivel doi a destinatarului datagramei IP

2. Dacă adresa de nivel do nu este găsită stația difuzează (folosind adresa de difuzare de nivel doi) un pachet ARP prin intermediul căruia solicită adresa de nivel doi a stației specificată prin adresa IP.

3. Pachetul ARP este încapsulat într-un cadru Ethernet având tipul 0x0806

4. Pentru a nu inunda rețeaua cu pachete ARP stațiile îşi limitează numărul de cereri ARP pentru un anumit interval de timp.

5. Dacă stația destinație recepționează cererea aceasta trimite un răspuns ce conține adresa solicitată direct la destinatar (unicast).

Recepționarea pachetelor ARP

1. Toate stațiile din rețeaua LAN identifică cadrele Ethernet având tipul 0x0806 ca fiind pachete ARP şi le transmit modului ARP pentru procesare.

2. O stație care recepționează un pachet ARP verifică dacă adresa stației care a transmis mesajul este deja în tabelă. Dacă da, atunci informația este actualizată. Această acțiune se execută plecând de la premisă că dacă o adresă a fost necesară în trecut ea va fi necesară şi în viitor. În caz contrar pachetul este ignorat, considerându-se că risipă de memorie şi de timp de procesor pentru a extrage fiecare adresă întrucât majoritatea gazdelor nu comunică cu toți vecinii din rețea.

3. Dacă pachetul ARP reprezintă un răspuns atunci informația este adăugată în tabelă.

4. Dacă mesajul reprezintă o cerere pentru stația care l-a recepționat (se determină prin examinarea adresei IP țintă) atunci stația respectivă va furniza un răspuns. De asemenea gazda va actualiza tabela ARP cu informația primită în cerere. Această acțiune se execută plecând de la premisă că dacă o stație are nevoie de adresa noastră atunci şi noi vom avea nevoie de acea adresă întrucât comunicația este de regulă bidirecțională.

După o anumită perioadă de timp intrările din tabelă expiră aceasta fiind înlăturate. În acest fel se limitează creşterea dimensiunii tabelei şi se rezolvă problema modificării adreselor.

9.1.4. Comunicația între stații aflate în rețele diferite

Protocolul de rezoluție al adresei se bazează pe difuzări la nivel legătură de date. Ruterele însă nu retrimit cadrele de difuzare. În consecință prin folosirea protocolului ARP pot fi aflate doar adresele gazdelor de pe acelaşi segment de rețea. De fapt, în cazul în care gazda corespondentă se află în altă rețea nici nu este nevoie de cunoaşterea adresei de nivel doi a acesteia ci doar de cunoaşterea adresei de nivel doi a primului ruter din cale. Există două modalități prin care gazdele pot afla adresa fizică a primului ruter: *default gateway* (rom. Poarta implicită) şi *proxy ARP*.

Default gateway

Default gateway reprezintă ruterul căruia i se trimit toate datagramele care sunt destinate unor adrese aflate în afara rețelei curent. În cazul folosirii *default gateway* stațiile trebuie să dețină ca informație de configurare adresa IP a primului ruter. Primul pas în procesul de rezoluție al adresei este determinarea dacă adresa destinație se află pe acelaşi segment de rețea. Pentru aceasta se aplică (ŞI pe biți) masca de rețea adresei IP proprii iar apoi se aplică masca de rețea adresei IP destinație. Dacă rezultatele celor două aplicări nu coincid înseamnă că adresa IP destinație se află în altă rețea şi deci cadrul trebuie să aibă ca destinație adresa interfeței ruterului. Cunoscând adresa IP a interfeței ruterului adresa de nivel doi se poate determina folosind o cerere ARP.

Ca exemplu să considerăm ca stația gazdă 192.168.67.21 doreşte să transmită o datagramă stației 192.168.68.23. Aplicăm mai întâi masca de rețea celor două adrese:

192.168. 67.21 &		192.168. 68.23 &
255.255.255.0		255.255.255.0
192.168. 67.0	≠	192.168. 68.0

Întrucât cele două rezultate sunt diferite însemnă că destinația se află pe alt segment de rețea iar cadrul trebui să aibă ca adresă destinație 5A:C1:02:03:03:05. Această adresă se determină simplu printr-o cerere ARP având ca adresă de protocol țintă 192.168.67.1

Proxy ARP

În cazul *proxy ARP* stațiile nu verifică dacă destinația se află sau nu în aceeaşi rețea. Ele pur şi simplu transmit cererile ARP. În cazul în care destinația se află pe alt segment de rețea cadrul ce conține pachetul ARP nu are cum să ajungă întrucât ruterele nu propagă cadrele de difuzare. În schimb ruterul va răspunde cu adresa proprie la toate cererile ARP destinate unor

adrese din afara rețelei. În consecinţă cadrele ce conțin datagrame de date destinate unor stații externe vor avea ca adresă destinație tot adresa fizică a ruterului.

Ca exemplu să considerăm ca stația gazdă 192.168.67.21 doreşte să transmită o datagramă stației 192.168.68.23. Stația1 va transmite o cerere ARP având ca adresă protocol țintă 192.168.68.23. Această cerere va fi recepţionată de toate stațiile de pe segmentul de rețea, inclusiv de interfață ruterului. Ruterul va analiza cererea şi folosind tabela de rutare, va concluziona ca adresa protocol destinație se află pe alt segment de rețea, condiții în care va răspunde el însuşi cerii cu propria adresa MAC.

Comparație între proxy arp şi default gateway

În cazul *proxy ARP* gazdele transmit cereri ARP ca şi cum toate destinațiile s-ar afla în rețeaua locală; la unele din aceste cereri le va răspunde ruterul. Dacă o stație comunică cu alte trei gazde aflate în rețele diferite, stația sursă va emite trei cereri ARP (câte una pentru fiecare stație). Cererile vor fi interceptate de ruter care le va şi soluționa; aceasta duce la o creştere a traficului precum şi a dimensiunii tabelei ARP la fiecare stație (toate adresele IP din afara rețelei vor avea asociată în tabelă adresa MAC a ruterului). În cazul *default gateway* stația sursă verifică apartenența adreselor destinație la rețeaua proprie şi în cazul în care aceste adrese fac parte din altă rețea, stația sursă nu va emite cereri ARP direct către ele ci va folosi adresa MAC a ruterului implicit (aceasta trebuie determinată o singură dată).

Dacă analizăm cele două protocoale, concluzia este că dacă stațiile comunică preponderent în interiorul rețelei atunci *proxy ARP* este mai avantajos întrucât se elimină testul suplimentar de apartenență al adresei. În cazul în care domină traficul extern atunci proxy ARP va emite câte o cerere pentru fiecare destinație. La momentul de față se foloseşte cel mai frecvent metoda *default gateway*.

9.2. Alocarea adreselor de rețea

Pentru obținerea unui bloc de adrese care să fie utilizat într-o subrețea a unei organizații, administratorul rețelei ar trebui să contacteze mai întâi furnizorul de servicii Internet care deține deja un bloc mai mare de adrese. Spre exemplu să presupunem că furnizorul deține blocul de adrese 25.55.0.0/16 care poate fi divizat folosind principiile măştilor de subrețea cu lungime variabilă. În exemplu nostru considerăm că există adrese libere începând cu 25.55.16.16 (adresele din intervalul 25.55.0.0-25.55.16.15 au fost deja alocate). Furnizorul de servicii Internet trebuie să aloce adrese pentru patru organizații client (A, B, C, D) care solicită 1000, 500, 2000 şi respectiv 4000 de adrese. Pentru cazul nostru adresele trebuie alocate strict în această ordine şi într-un mod

cât mai eficient (intervalele ramase libere să fie cât mai mici). Primul pas este determinarea numărului de biți de stație pentru fiecare organizație. Apoi putem determina măştile de rețea.

Organizația	Număr de gazde (număr maxim de adrese)	Biți gazdă/ Biți rețea	Masca de rețea	Increment (octet 2 LSB)
A	1000 ($1024=2^{10}$)	10/22	255.255.252.0 /22	4
B	500 ($512=2^{9}$)	9/23	255.255.254.0 /23	8
C	2000 ($2048=2^{11}$)	11/21	255.255.248.0 /21	2
D	4000 ($4096=2^{12}$)	12/20	255.255.240.0 /20	16

Pornind de la rețeaua A scriem primele subrețele începând cu 25.55.0.0 şi efectuăm alocarea. Pot fi agregate (grupate) doar rețelele care diferă prin acelaşi număr de biți; numărul de subrețele agregate trebuie să fie putere a lui 2. O rețea poate fi divizată într-un număr de subrețele putere a lui 2.

Nr.crt.	Rețea	Stare		
0	25.55.0.0/22	Utilizată		
1	25.55.4.0/22	Utilizată		
2	25.55.8.0/22	Utilizată		
3	25.55.12.0/22	Utilizată		
4	25.55.16.0/22	Utilizată parțial		
5	25.55.20.0/22	Se alocă pentru A		
6	25.55.24.0/22	Se împarte în două	25.55.24.0/23	Se alocă pentru B
7			25.55.26.0/23	Rămâne liberă
8	25.55.28.0/22			Rămâne liberă
9	25.55.32.0/22	Se grupează	25.55.28.0/21	Se alocă pentru C
10	25.55.36.0/22			
11	25.55.40.0/22			Rămâne liberă
12	25.55.44.0/22	Se grupează	25.55.44.0/20	Se alocă pentru D
13	25.55.48.0/22			
14	25.55.52.0/22			
15	25.55.56.0/22			
17	25.55.64.0/22			

La rândul său furnizorul de servicii trebuie şi el să obțină blocul de adrese. La nivel global există o autoritate care se ocupă cu alocarea blocurilor de adrese IP: Internet Corporation for

Assigned Names and Numbers (ICANN). Pentru a descentraliza procedura de alocare ICANN a delegat atribuțiile unor autorități regionale. În Europa atribuirile se fac prin RIPE (fr. Réseaux IP Européens).

9.2.1. Protocolul dinamic de configurare a gazdei

După ce o organizație a obținut un bloc de adrese, se poate trece la asignarea de adrese pentru interfețele ruterelor şi gazdelor. De regulă interfețele ruterelor sunt configurate manual de către administratorul de rețea. Configurarea gazdelor se poate face atât manual cât şi prin intermediul protocolului DHCP (Dynamic Host Configuration Protocol). În cazul configurării manuale administratorul scrie într-un fişier adresa IP, masca de rețea, adresa ruterului (default gateway) şi eventuale alte informații. O astfel de soluție nu este practică pentru rețelele mari (gazdele nu sunt accesibile de la distanța decât după ce au fost configurate) şi nici în cazul în care stațiile se mută frecvent dintr-o rețea în alta.

DHCP este un protocol bazat pe modelul client-server folosit de către stații pentru a obține informaţiile necesare funcționării stivei TCP/IP de la un server, în mod automat fără intervenția administratorului de rețea. DHCP poate fi configurat astfel încât o stație să obțină mereu aceeaşi adresă IP sau poate fi configurat să ofere adrese temporare, ce diferă de la o conectare la alta.

Funcționarea DHCP

Atunci când o gazdă având clientul DHCP activat este conectată la rețea, aceasta va trimite un pachet de difuzare prin care solicită informații serverului DHCP. Serverul administrează un interval de adrese IP, precum şi celelalte informații. La recepționarea unui astfel de pachet serverul va asigna o adresă pe care o va comunica solicitantului împreună cu restul informațiilor. Funcționarea protocolului este ilustrată în Figura 9.4. Semnificația mesajelor este următoarea:

DISCOVERY – clientul transmite un pachet de difuzare pentru identificarea serverelor DHCP disponibile, prin care solicită alocarea unei adrese.

OFFER – atunci când un server recepționează o cerere de la un client formulează o ofertă pe care i-o transmite. Într-o rețea pot exista mai multe servere DHCP.

REQUEST – atunci când clientul a primit o oferta, acesta trebuie să înştiinţeze celelalte servere că a acceptat una din oferte. Clientul trimite un pachet de difuzare prin care specifică adresa serverului a cărui ofertă a fost acceptată. La recepția acestui pachet celelalte servere vor anula oferta (anulează rezervarea adresei). La un pachet DISCOVERY pot răspunde oricâte servere însă clientul poate accepta o singură ofertă per interfață.

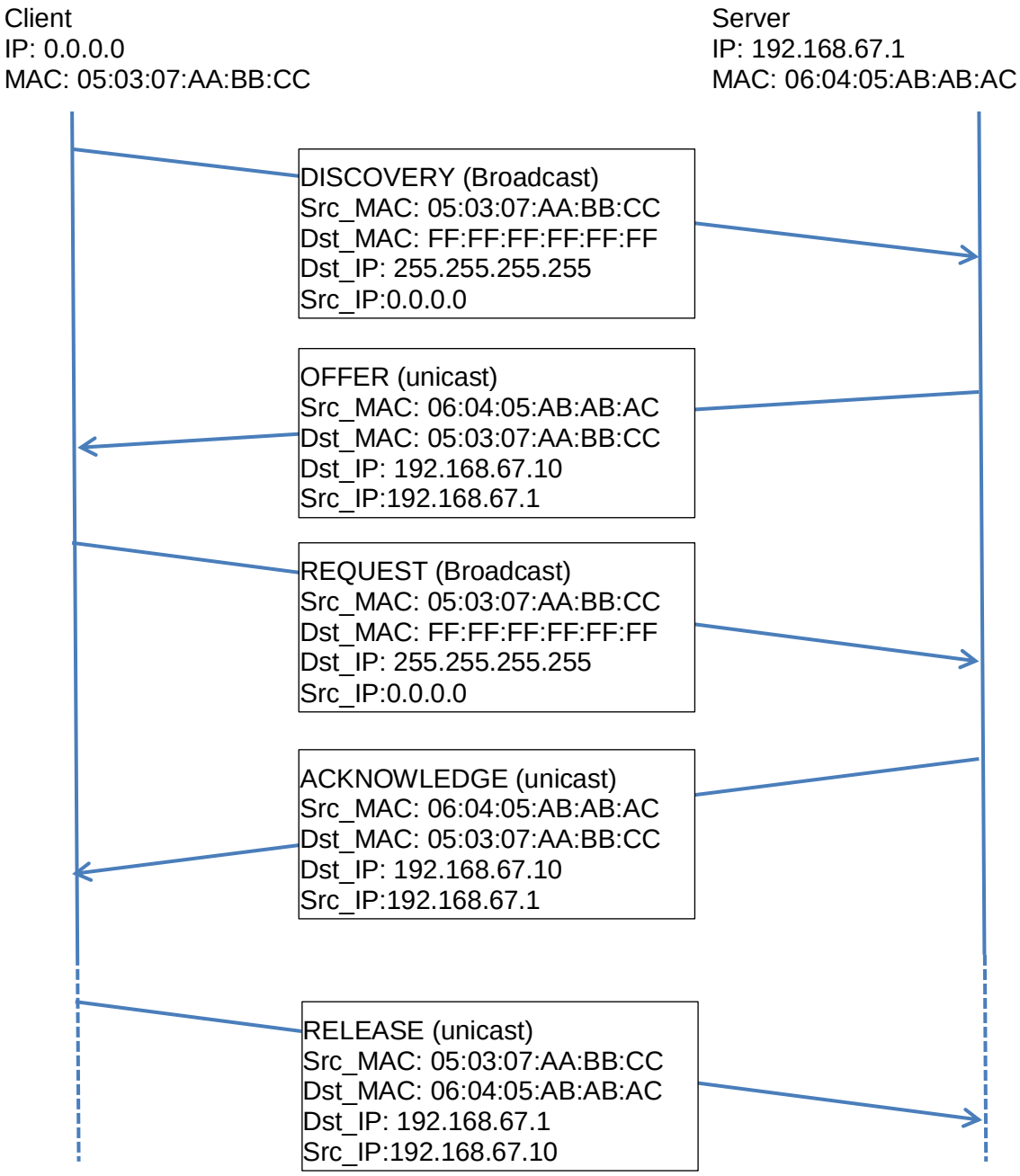

Figura 9.4 Pachete DHCP schimbate între server şi client

ACKNOWLEDGEMENT – indică sfârşitul procesului de asignare, rezervarea devenind definitivă.

RELEASE – clientul trimite o cerere serverului DHCP prin care cedează informațiile de configurare şi renunța la adresa IP. Întrucât de regulă se poate şti momentul în care utilizatorul detaşează dispozitivul de la rețea, protocolul nu impune trimiterea unui pachet RELEASE, ci doar recomandă.

O problemă care apare cu atribuirea automată a adreselor IP dintr-o rezervă comună este cât de mult ar trebui alocată o adresă IP. Dacă o gazdă părăseşte rețeaua şi nu anunță serverul serverul DHCP, acea adresă va fi indisponibilă permanent. Am putea impune gazdelor obligativitatea notificării serverului la părăsirea rețelei însă acest lucru nu este întotdeauna realizabil (sper exemplu blocarea sistemului de operare, întreruperea alimentării cu energie, părăsirea ariei de acoperire radio de către o gazdă mobilă). După o perioadă de timp vor fi pierdute multe adrese. Pentru a preveni aceasta, atribuirea adresei IP se face pentru o perioadă fixă de timp, tehnică numită închiriere. Durata de închiriere este specificată în pachetul OFFER. Chiar înainte ca perioada de închiriere să expire, gazda trebuie să solicite serverului reînnoirea adresei Dacă nu reuşeşte să facă cererea sau dacă cererea este respinsă, gazda nu va mai putea folosi adresa IP care îi fusese dată mai devreme. Adresele al căror interval de închiriere a expirat pot fi reutilizate de către server, pentru alte alocări.

Rezumat

Protocolul ARP are ca scop distribuirea dinamică a informaţiilor necesare construirii unei tabele ce asigură translatarea unei adrese IPv4 într-o adresă IEEE–48 bit; protocolul este bazat pe transmiterea de difuzării la nivel legătură de date. ARP este un mecanism care permite utilizarea adreselor logice unice global peste rețele având scheme de adresare fizică diferite.

Protocolul DHCP este de tip *plug-and-play* având o utilitate incontestabilă, alternativa fiind configurarea manuală a parametrilor necesari funcționării IP-ului. De asemenea DHCP ilustrează un aspect important al scalării: scalarea managementului rețelei. Permițând administratorului de rețea să configureze un interval de adrese IP per rețea în locul unei adrese per gazdă, DHCP simplifică semnificativ administrarea unei rețele. Pentru descoperirea serverului DHCP se folosesc cadre de difuzare.

Bibliografie

James F. Kurose, Keith W. Ross, *Computer Networking - A Top-Down Approach*, 5/E, Pearson Education, 2010

Andrew S. Tanenbaum, David J. Wetherall, *Computer Networks*, 5/E, Prentice Hall, 2011

Larry L. Peterson, Bruce S. Davie, *Computer Networks – a systems approach* 5/E, Elsevier , 2012

William Stallings, *Data and computer communications*, 9/E, Pearson Education, 2011