Lucrarea de laborator nr.9.
Protocoalele Ethernet şi ARP

În acest laborator vom studia protocoalele Ethernet şi ARP. Dacă doriţi să aprofundaţi, la ftp://ftp.rfc-editor.org/innotes/std/std37.txt găsiţi detalii ale protocolului ARP, care este folosit de un dispozitiv IP pentru a determina adresa IP a unei interfeţe remote, a cărei adresă Ethernet este cunoscută.

Captura şi analiza cadrelor Ethernet

Un cadru Ethernet are forma următoare:

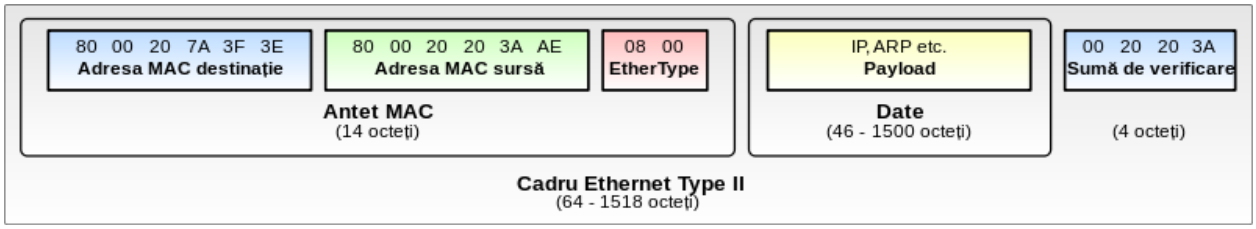

Figura 22 - Structura unui cadru Ethernet

- Mai întâi, goliţi cache-ul browser-ului dvs. Pentru Mozilla Firefox selectaţi *Tools* → *Clear Private Data* şi bifaţi 'Cache'. Pentru Internet Explorer, selectaţi *Tools* → *Internet Options* → *Delete Files*;
- Porniţi Wireshark;

- Intraţi la http://tc.unitbv.ro/rc/HTTP_3.html. Ar trebui ca browser-ul să vă afişeze Titlul I din Constituţia României.
- Opriţi captura Wireshark. Întâi, găsiţi „packet numbers" (coloana cea mai din stânga în fereastra de sus a Wireshark) a mesajului HTTP GET care a fost trimis de la computerul dvs, la serverul „tc.unitbv.ro" precum şi începutul mesajului răspuns HTTP trimis la computerul dvs de către server. Ar trebui să vedeţi un ecran asemănător cu imaginea din Figura 23 (unde pachetul 5 conţine mesajul HTTP GET)

(*Nota*: dacă nu va merge Wireshark, folosiţi fişierul *ethernet-trace-1* de pe CD)

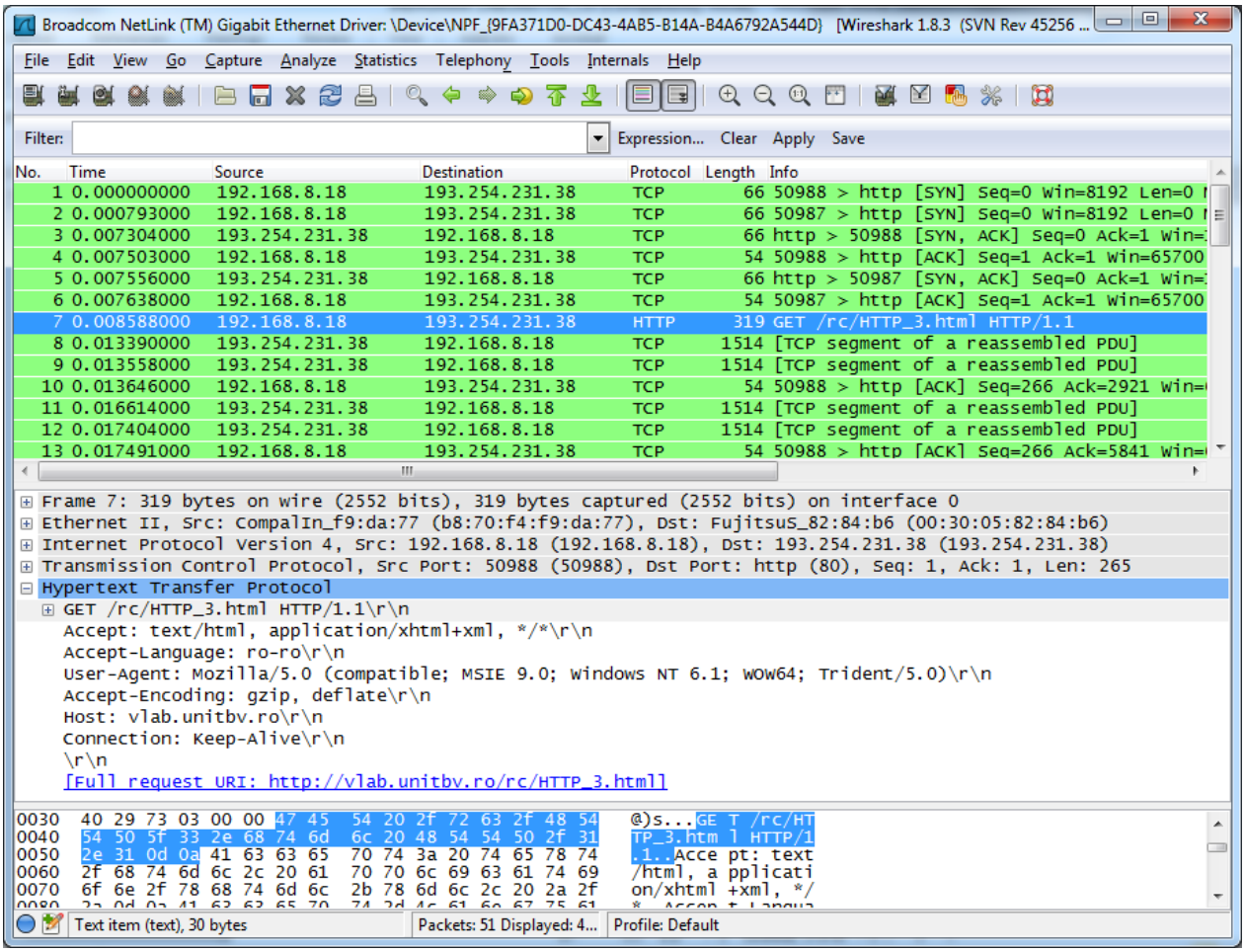

Figura 23 - Mesajele HTTP GET şi http de răspuns

După cum ştim, acest laborator se ocupă de Ethernet şi ARP, deci nu ne interesează IP sau protocoalele higher-layer. În consecinţă, vom schimba fereastra Wireshark "listing of captured packets" astfel încât să arate informaţii doar despre protocoale sub IP. Pentru aceasta, selectaţi *Analyze* → *Enabled Protocols*. Apoi, debifaţi IP şi apăsaţi *OK*. Acum ar trebui să vedeţi o fereastra Wireshark ca în Figura 24:

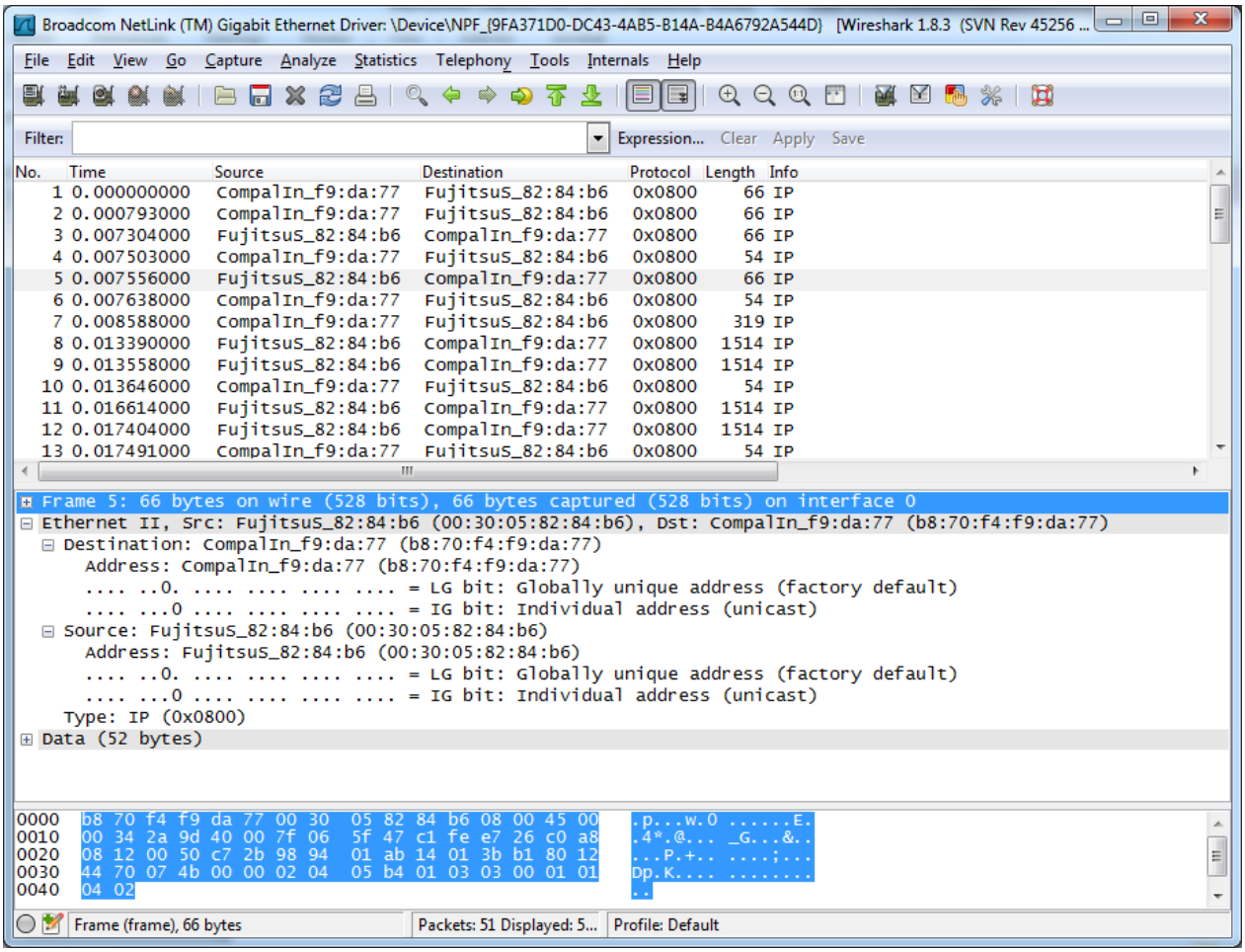

Figura 24 - Lista pachetelor cu afişarea protocoalelor “sub” IP

Pentru a răspunde la următoarele întrebări, va trebui să priviţi ferestrele “packet details” şi ‘packet contents’.

Selectaţi cadrul Ethernet care conţine mesajul HTTP GET. Ştim că mesajul HTTP GET este transportat într-un segment TCP, care este transportat într-o datagramă IP, care este transportată într-un cadru Ethernet. Extindeţi informaţia Ethernet II în fereastra ”packet details”. Reţineţi că, header-ul şi payload-ul cadrului Ethernet sunt afişate în fereastra „packet contents”.

Răspundeţi la următoarele întrebări, bazându-vă pe conţinutul cadrului Ethernet care prezintă mesajul HTTP GET. Oricând puteţi, este bine să vă justificaţi cu un printout al pachetelor din trace-ul folosit pentru a răspunde la întrebări: *File → Print*, alegeţi *Selected packet only,* apoi, *Packet summary line*, şi selectaţi detaliul minim al pachetului de care aveţi nevoie pentru a răspunde la întrebare.

1. Care este adresa Ethernet pe 48b a computerului dvs?
2. Care este adresa destinaţie pe 48b din cadrul Ethernet? Este aceasta adresa Ethernet pentru “tc.unitbv.ro”? (Indiciu: răspunsul este *nu*). Ce dispozitiv are această adresă ca adresă pentru Ethernet? Atenţie la această întrebare !!!

3. Scrieţi valoarea hexazecimală pentru câmpul de 2B “Frame-type”. Ce reprezintă în câmpul „flag” biţii a căror valoare este 0 (dar 1)?
4. Câţi octeţi de la începutul cadrului Ethernet apar până la simbolul “G” în ASCII, din “GET” în cadrul Ethernet?
5. Care este valoarea hexazecimală a câmpului CRC în acest cadru Ethernet?

Apoi, răspundeţi la următoarele întrebări, bazându-vă pe conţinutul cadrului Ethernet care conţine primul octet al mesajului de răspuns HTTP:

6. Care este valoarea adresei sursă Ethernet? Este aceasta adresa computerului dvs, sau a lui “tc.unitbv.ro” (Indiciu: răspunsul este *nu*). Ce dispozitiv are aceasta drept adresa sa Ethernet?
7. Care este valoarea adresei sursa Ethernet? Este această adresă Ethernet, adresa computerului dvs?
8. Scrieţi valoarea hexazecimală a câmpului de 2B “Frame type”’. În câmpul „flag”, ce înseamnă biţii a căror valoare este 0 (dar 1)?
9. Câţi octeţi de la începutul cadrului Ethernet apar până la simbolul ASCII “O”, din “OK” (de exemplu în HTTP response code), în acest cadru Ethernet?
10. Care este valoarea hexazecimală a câmpului CRC în acest cadru Ethernet?

ARP – Address Resolution Protocol

Protocolul de rezoluţie a adresei, este un protocol ce determină adresele numerice unice ale maşinilor din reţea.

Pentru ca două sisteme de calcul să poată comunica într-o reţea este necesară cunoaşterea atât a adresei MAC, cât şi a adresei IP. În cazul în care numai una dintre adrese este disponibilă se apelează la un protocol dedicat care pe baza acesteia va determina cealaltă adresă.

Stiva de protocoale TCP/IP conţine două protocoale de nivel reţea pentru a servi acest scop: ARP (Address Resolution Protocol) şi RARP (Reverse Address Resolution Protocol). ARP este protocolul ce va oferi adresa MAC a unui dispozitiv de reţea, dată fiind adresa sa IP. ARP se bazează pe construirea şi menţinerea unei tabele ARP. O tabelă ARP are rolul de a oferi o corespondenţă între adresele IP şi cele MAC. Acestea sunt construite dinamic şi sunt stocate în memoria RAM.

Deşi există mecanisme pentru adăugarea sau eliminarea unei intrări într-o tabelă ARP acestea sunt rareori folosite. Fiecare computer sau dispozitiv de reţea îşi păstrează propria sa tabelă ARP.

ARP Caching

Ştim că protocolul ARP păstrează un cache de perechi de translaţii de adrese IP-to-Ethernet (IP-to-Ethernet address translation pair) pe computerul dvs. Comanda *arp* (valabilă şi pentru MSDOS şi pentru Linux/Unix) este folosită pentru a vedea şi manipula conţinutul acestui

cache. Deoarece comanda *arp* şi protocolul ARP au acelaşi nume, a face o confuzie este uşor. Reţineţi însă ca sunt diferite – protocolul ARP defineşte formatul şi înţelesul mesajelor trimise şi recepţionate, şi defineşte acţiunile luate la transmisia şi recepţia mesajelor.

Să privim conţinutul cache-ului ARP pe computerul dvs:

-MS-DOS. Comanda *arp* se poate porni scriind *arp* sau *c:/windows/system32/arp* în Command Prompt

-Linux/Unix. Executabilul comenzii *arp* poate fi în diferite locuri. De obicei se găseşte în "/sbin/arp" (pentru Linux) şi „usr/etc/arp" (pentru variante de Unix)

Comanda *arp –a* afişează conţinutul cache-ului ARP de pe computerul dvs. Rulaţi *arp*.

11. Scrieţi conţinutul cache-ului ARP. Ce reprezintă valoarea fiecărei coloane?

Pentru a vă putea vedea computerul trimiţând şi primind mesaje ARP, trebuie să golim cache-ul ARP, deoarece, dacă nu am face acest lucru, computerul dvs este probabil să găsească un "IP-Ethernet address translation pair" în cache-ul lui şi în consecinţă, să nu trimită un mesaj ARP.

-MS-DOS. Comanda *arp –d* * va goli cache-ul ARP. *–d* indică ştergerea, iar * este wildcard pentru ştergerea întregii tabele;

-Linux/Unix. a*rp –d* * va goli cache-ul ARP. Este nevoie de privilegii de root pentru a putea rula această comandă.

În continuare executaţi următoarele acţiuni:

- Ştergeţi cache-ul ARP.
- Ştergeţi cache-ul browser-ului (pentru Netscape 7.0, *Edit → Preferences → Advanced → Cache* şi ştergeţi memoria şi cache-ul discului. Pentru Internet Explorer, *Tools → Internet Options → Delete Files*).
- Porniţi captura Wireshark.
- Intraţi la http://tc.unitbv.ro/rc/HTTP_3.html unde ar trebui să vedeţi din nou Constituţia României.
- Opriţi captura Wireshark. Din nou, nu ne interesează protocoale IP sau higher-layer, deci schimbaţi fereastra "listing of captured packets" astfel încât să afişeze informaţii doar despre protocoale sub IP: *Analyze → Enabled Protocols*. Apoi debifaţi IP şi selectaţi *OK*. Acum ar trebui să vedeţi ceva similar cu imaginea din Figura 25:
(*Notă*: dacă nu va merge Wireshark, folosiţi fişierul *ethernet-trace-1* de pe CD).

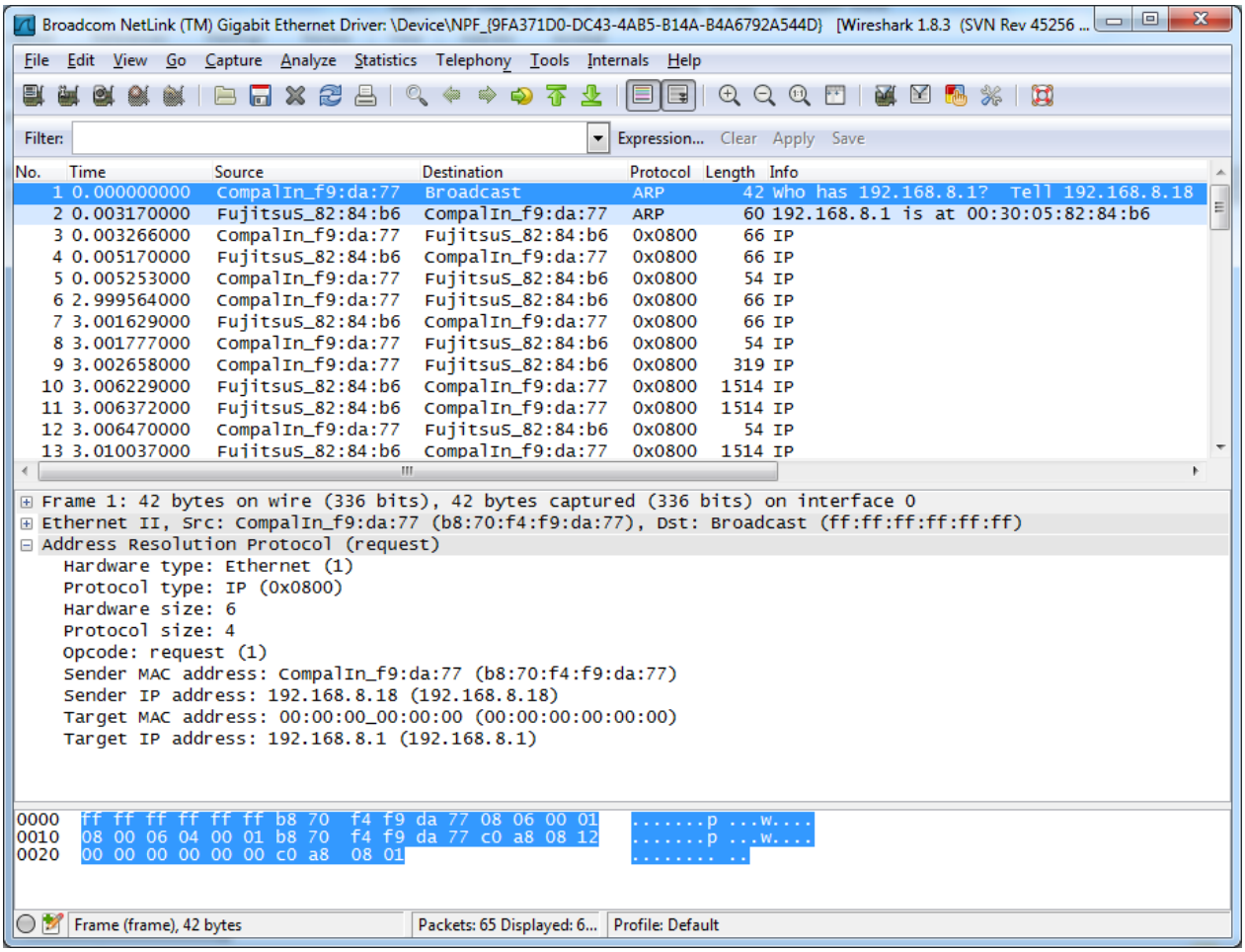

Figura 25 - Captura de pachete ce conţine mesaje ARP

În exemplul de mai sus, primele două cadre din trace, conţin mesaje ARP.

Răspundeţi la următoarele întrebări:

12. Care sunt valorile hexazecimale pentru adresele sursă şi destinaţie din cadrul Ethernet care conţine mesajul de cerere ARP?
13. Scrieţi valoarea hexazecimală pentru câmpul de 2B Ethernet Frame type. Ce reprezintă biţii a căror valoare este 1 ?
14. Descărcaţi specificaţiile ARP de la ftp://ftp.rfc-editor.org/innotes/std/std37.txt. Un alt studiu se afla şi la http://www.erg.abdn.ac.uk/users/gorry/course/inet-pages/arp.html

    a) Cu câți octeți începe câmpul ARP *opcode* de la începutul cadrului Ethernet?

    b) Care este valoarea câmpului *opcode* din porţiunea ARP-payload a cadrului Ethernet, prin care se face cererea ARP?

    c) Mesajul ARP conţine adresa IP a transmiţătorului?

d) Unde apare “întrebarea” – adresa Ethernet a computerului a cărui adresă IP corespunzătoare este interogată? - în cererea ARP?

15. Acum găsiţi replica ARP care a fost trimisă ca răspuns cererii ARP.

    a) Cu câți octeţi începe câmpul ARP *opcode* de la începutul cadrului Ethernet?

    b) Care este valoarea câmpului *opcode* din porţiunea ARP-payload a cadrului Ethernet, prin care se face răspunsul ARP?

    c) Unde, în mesajul ARP, apare “răspunsul” la cererea ARP precedentă – adresa IP a computerului care are adresa Ethernet a cărui adresă IP corespunzătoare este interogată?

16. Care sunt valorile hexazecimale pentru adresele sursă şi destinaţie din cadrul Ethernet care conţine mesajul „ARP reply”?

17. Deschideţi fişierul *ethernet-trace-1* de pe CD). Primele două pachete ARP din acest trace corespund unei cereri ARP trimisă de computerul pe care rulează Wireshark, şi replicii ARP trimisă către computerul cu Wireshark de către computerul cu “ARP-requested Ethernet address”. Dar mai există încă un computer în această reţea, după cum indică pachetul 6 – altă cerere ARP. De ce nu există o replică ARP (trimisă ca răspuns cererii ARP din pachetul 6) în trace?

Bonus

1. Comanda *arp:*

   Arp –s InetAddr EtherAddr

permite adăugarea manuală a unei linii (entry) în cache-ul ARP care transformă adresa IP *InetAddr* în adresa fizica *EtherAddr*. Ce s-ar întâmpla dacă, atunci când adăugaţi manual o linie, scrieţi corect adresa IP, dar adresa Ethernet o greşiţi?

2. Care este timpul default în care o linie (un entry) rămâne în cache-ul ARP până când va fi eliminată? Puteţi determina acest lucru empiric (monitorizând conţinutul cache-ului) sau căutând în documentaţia sistemului dvs de operare. Indicaţi felul în care aţi determinat această valoare.

Cuprins