Lucrarea de laborator nr.6.
Protocolul IP

În acest laborator vom investiga protocolul IP concentrându-ne asupra datagramei IP. Vom analiza un trace de datagrame IP trimise şi recepţionate, folosind *traceroute*. Vom investiga diferitele câmpuri ale datagramei IP şi vom studia fragmentarea IP în detaliu.

Înainte de începerea acestui laborator, este indicat să revizuiţi informaţiile despre RFC 2151 de la [ftp://ftp.rfc-editor.org/in-notes/rfc2151.txt] şi cele despre RFC 791 de la [ftp://ftp.rfc-editor.org/in-notes/rfc791.txt].

Captura de pachete prin execuţia de *traceroute*.

Pentru a genera un trace al datagramelor IP vom folosi *traceroute* în scopul transmiterii de datagrame de diferite mărimi către aceeaşi destinaţie, *X*. Ştim că *traceroute* funcţionează trimiţând întâi una sau mai multe datagrame cu câmpurile TTL din header-ul IP setate la 1; apoi trimite o serie de una sau mai multe datagrame spre aceeaşi destinaţie cu TTL = 2; apoi trimite o serie de una sau mai multe datagrame spre aceeaşi destinaţie cu TTL = 3 ş.a.m.d. Ştim că un router trebuie să decrementeze TTL-ul (cu 1) din fiecare datagramă primită (de fapt RFC 791 spune ca router-ul trebuie să decrementeze TTL-ul cu *cel puţin* 1). Dacă TTL ajunge la 0, router-ul întoarce un mesaj *ICMP* (type 11 – *TTL-exceeded*) către transmiţător. În consecinţă, o datagramă cu TTL = 1 (trimisă de computerul care execută *traceroute*) va face router-ul, la distanţă de un hop de transmiţător să trimită un mesaj *ICMP TTL-exceeded* înapoi la transmiţător; datagrama trimisă cu TTL = 2 va face router-ul la distanţă de două hopuri de transmiţător să trimită un mesaj ICMP înapoi la transmiţător; datagrama trimisă cu TTL = 3 va face router-ul la distanţă de trei hopuri de transmiţător să trimită un mesaj ICMP înapoi la transmiţător ş.a.m.d. Astfel, computerul care execută *traceroute* poate afla identităţile routere-lor dintre el însuşi şi destinaţia *X* uitându-se la adresele IP sursă din datagramele care conţin mesaje *ICMP TTL-exceeded*.

***Traceroute* poate trimite datagrame de diferite lungimi.**

Windows. Programul *tracert* (folosit în laboratorul Wireshark ICMP) nu ne lasă să schimbăm mărimea mesajului *ICMP echo request (ping)* trimis de programul *tracert*. Un program mai bun pentru Windows este *pingplotter* disponibil freeware şi hardware la http://www.pingplotter.com. Instalaţi *pingplotter* şi testaţi-l făcând câteva trace-uri la site-urile voastre preferate. Mărimea mesajului ping poate fi setată în *pingplotter* selectând *Edit* → *Options* → *Packet Options* şi apoi completaţi câmpul *Packet Size*. Mărimea default a pachetului este 56b. După ce *pingplotter* a trimis o serie de pachete cu valori crescătoare TTL, va reîncepe procesul de trimitere cu TTL = 1, după ce aşteaptă timpul pentru *Trace Interval*. Valoarea lui *Trace Interval* şi numărul intervalurilor poate fi setată explicit în *pingplotter*.

Linux/Unix. Cu comanda *traceroute* din Unix, mărimea datagramei UDP trimisă spre destinaţie poate fi setată explicit indicând numărul de octeţi din datagramă; această valoare este scrisă în linia de comandă *traceroute* imediat după numele sau adresa destinaţiei. De exemplu, pentru a trimite datagrame *traceroute* de 2000b spre "www.unitbv.ro", comanda este:

%traceroute www.unitbv.ro 2000

În continuare, activaţi Wireshark şi porniţi captura; apoi apăsaţi *OK* la ecranul "Wireshark Packet Capture Options" (nu trebuie sa selectaţi vreo opţiune aici).

Dacă folosiţi Windows, porniţi *pingplotter* şi scrieţi numele unei destinaţii în "Address to Trace Window". Scrieţi 3 la "# of times to Trace" ca să nu adunaţi prea multe date. Selectaţi *Edit* → *Advanced Options* → *Packet Options* şi scrieţi "56" la câmpul *Packet Size* şi apăsaţi *OK*. Apoi apăsaţi butonul "Trace". Ar trebui să vedeţi ceva asemănător cu imaginea din Figura 14:

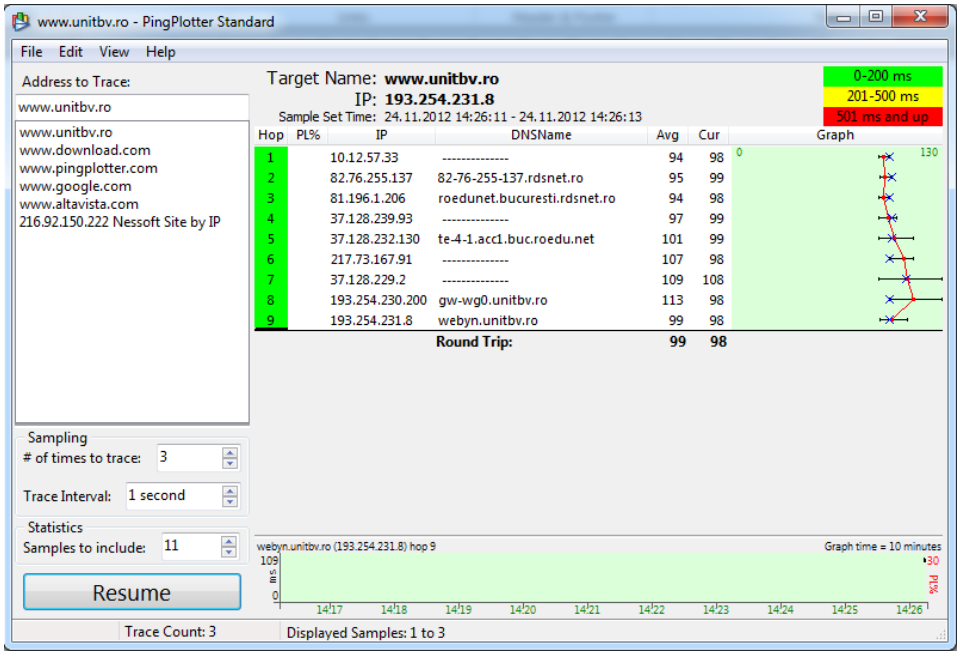

Figura 14 - Transmiterea datagramelor de diferite lungimi

Trimiteţi apoi un set de datagrame de o lungime mai mare, selectând *Edit → Advanced Options → Packet Options* şi introduceţi valoarea 2000 în câmpul *Packet Size* şi apăsaţi *OK*. Apoi apăsaţi *Resume*.

Acum trimiteţi un set de datagrame de lungime mai mare selectând *Edit → Advanced Options → Packet Options* şi introduceţi valoarea de 3500 în câmpul *Packet Size* şi apăsaţi *OK*. Apoi apăsaţi *Resume*.

Opriţi trace-ul Wireshark.

Dacă folosiţi Unix, introduceţi trei comenzi *traceroute*, una cu o lungime de 56b, alta de 2000b şi una de 3500b.
Opriţi trace-ul Wireshark.

Dacă nu va merge Wireshark puteţi descărca arhiva de pe CD şi extrage fişierul *ip-ethereal-trace-1* pe care să-l folosiţi pentru a vă ajuta la întrebările de mai jos.

O privire asupra trace-ului.

În trace-ul dvs. ar trebui să puteţi vedea seriile de *ICMP Echo Request* (dacă folosiţi Windows) sau segmentul UDP (dacă folosiţi Unix) trimise de computerul dvs. şi mesajele *ICMP TTL-exceeded* returnate de computerul dvs. prin routerele intermediare. La întrebările de mai jos vom presupune că folosiţi Windows-ul, întrebările corespunzătoare pentru Unix ar trebui să fie clare. Este recomandat să arătaţi un printout (*File → Print, Selected packet only, Packet summary line* şi selectaţi detaliul de pachete minim de care aveţi nevoie pentru a răspunde) al pachetelor din trace-ul pe care l-aţi folosit, pentru a răspunde la întrebări.

1. Selectaţi primul mesaj *ICMP Echo Request* trimis de computerul dvs. şi extindeţi partea de Internet Protocol a pachetului. Care este adresa IP a computerului dvs. ?
2. Care este valoarea câmpului “upper layer protocol” în header-ul pachetului IP?
3. Câţi octeţi sunt în header-ul IP? Câţi octeţi sunt în payload-ul datagramei IP? Justificaţi răspunsul.
4. Această datagrama IP a fost fragmentată? Justificaţi răspunsul.

Acum, sortaţi pachetele după adresa IP sursă, făcând click pe header-ul coloanei *Source*; ar trebui să apară o săgeată îndreptată în jos. Selectaţi primul mesaj *ICMP Echo Request* trimis de computerul dvs, şi extindeţi porţiunea Internet Protocol din fereastra “details of selected packet header”. În fereastra “listing of captured packets” ar trebui să vedeţi toate mesajele *ICMP* ulterioare (poate cu alte pachete printre ele, trimise de alte protocoale care rulează pe computerul dvs.) sub acest prim mesaj *ICMP*.

5. Care câmpuri din datagrama IP se schimbă întotdeauna de la o datagramă la următoarea, în această serie de mesaje *ICMP*?
6. Care câmpuri rămân constante? Care câmpuri *trebuie* să rămână constante? Care câmpuri trebuie să se schimbe? De ce?
7. Descrieţi modelul pe care-l vedeți în valorile din câmpul *Identification* al datagramei IP.

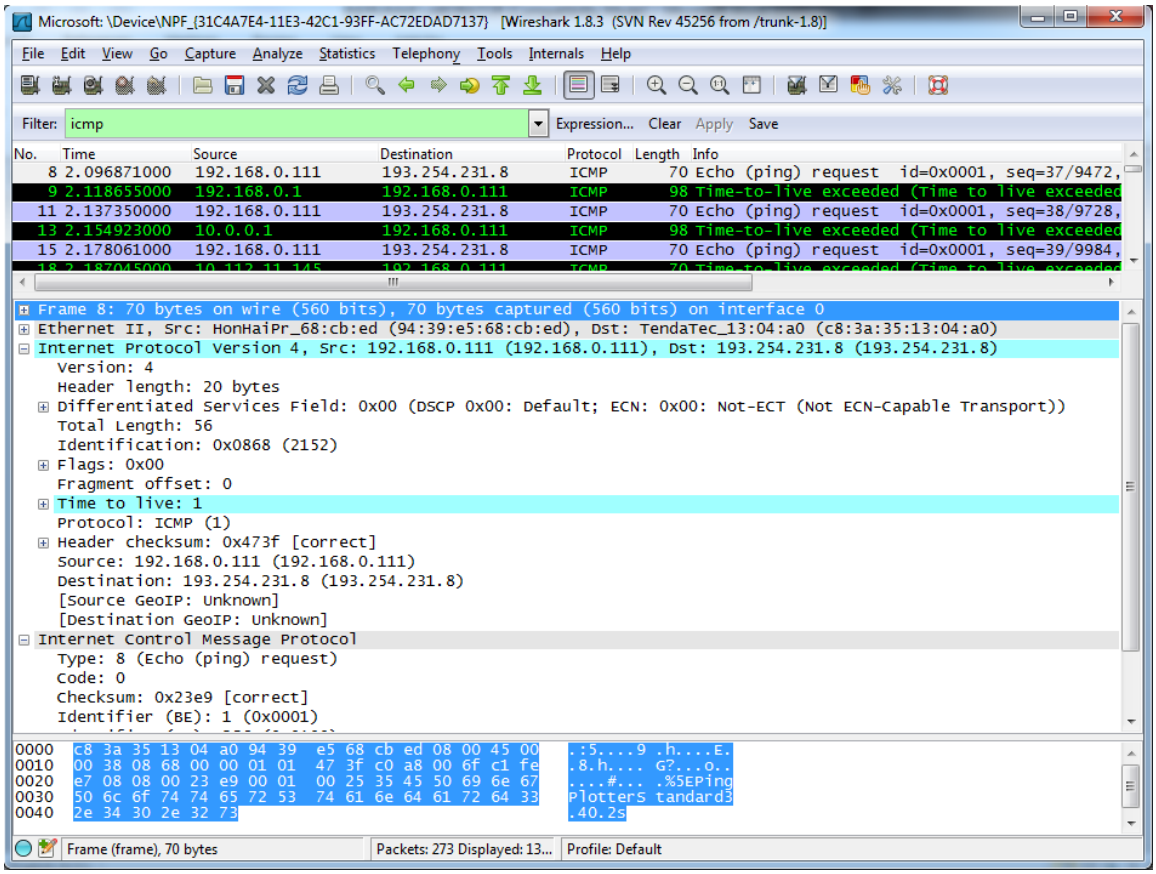

Figura 15 - Identificarea câmpurilor din datagrama IP

Apoi (cu pachetele încă sortate după adresa sursă), găsiţi seria de replici *ICMP TTL-exceeded* trimise la computerul dvs. de către cel mai apropiat router.

8. Care este valoarea din câmpurile *Identification* şi *TTL*?
9. Rămân aceste valori neschimbate pentru toate replicile *ICMP TTL-exceeded* trimise la computerul dvs. de la cel mai apropiat router? De ce?

Fragmentarea

Sortaţi iarăşi lista pachetelor după timp, făcând click pe coloana *Time*.

10. Găsiţi primul mesaj *ICMP Echo Request* care a fost trimis de către computerul dvs. după ce aţi schimbat *Packet Size* la 2000 în *pingplotter*. A fost acel mesaj fragmentat de-a lungul mai multor datagrame IP? (Notă: dacă pachetul dvs. nu a fost fragmentat, folosiţi fişierul *ip-ethereal-trace-1* din arhiva *wireshark-traces.zip*).
11. Tipăriţi primul fragment al datagramei IP fragmentate. Ce informaţie din header-ul IP indică faptul că datagrama a fost fragmentată? Ce informaţie din header-ul IP indică dacă acesta este primul sau ultimul fragment? Cât de lungă este această datagramă IP?
12. Tipăriţi al doilea fragment al datagramei. Ce informaţie din header-ul IP indică faptul că acesta nu este primul fragment? Există mai multe fragmente? Justificaţi răspunsul.
13. Care câmpuri se schimbă în header-ul IP între primul şi al doilea fragment?

Acum găsiţi primul mesaj *ICMP Echo Request* care a fost trimis de computerul dvs. după ce aţi schimbat *Packet Size* la 3500 în *pingplotter*.

14. Câte fragmente au fost create din datagrama originală?
15. Ce câmpuri s-au schimbat în header-ul IP de la un fragment la altul?

Cuprins