Δίκτυα υπολογιστών

Εργαστηριακή άσκηση 1 (Αναλυτής Πρωτοκόλλων Wireshark)

Τσάκωνας Παναγιώτης (03119610) Ομάδα: 3

Ακαδημαϊκό Έτος: 2022-2023

Διεύθυνση IP: 147.102.237.128	**Διεύθυνση MAC:** fc:e2:6c:02:ce:3f

Άσκηση 1: Βρείτε την κάρτα δικτύου

1.1) Είμαι σε ΛΣ MacOS και δεν μπορώ να την βρω, το μόνο που εμφανίζεται είναι το en0.
1.2) Ασύρματη σύνδεση (Wi-Fi).
1.3) 144 Mbps
1.4) MAC-address: fc:e2:6c:02:ce:3f
1.5) IPv4: 147.102.237.128
1.6) IPv6: fe80:c0ff:fe98:81a5
1.7) DNS address: 147.102.224.243
1.8) Default gateway: 147.102.236.200

Άσκηση 2: Ρυθμίσεις και στατιστικά

2.1) Με χρήση της εντολής `hostname` στο command line εμφανίζεται το ακόλουθο Host name: Panagiotiss-Macbook-Air-2.
2.2) Χρησιμοποιώντας την εντολή `ifconfig` δεν εμφανίζεται το όνομα της κάρτας δικτύου, καθότι είμαι σε ΛΣ MacOS, το μόνο εμφανίζεται το en0.
2.3) Χρησιμοποιώντας την εντολή `ifconfig` η MAC-address είναι: fc:e2:6c:02:ce:3f.
2.4) Χρησιμοποιώντας την εντολή `networkQuality` η σύνδεση στο διαδίκτυο είναι η ακόλουθη: 318.1 Mbps (Download) και 55.9 Mbps (Upload).
2.5) Χρησιμοποιώντας την εντολή `ifconfig` η IPv4 είναι: 147.102.237.128
2.6) Η μάσκα υποδικτύου είναι: 0xfffffc00.
  i) Χρησιμοποιώντας την εντολή `ifconfig` βρίσκουμε ότι το μέγεθος σε bit του τμήματος δικτύου της διεύθυνσης IPv4 του υπολογιστή μου είναι 22 bit.
  ii) Χρησιμοποιώντας την εντολή `ifconfig` βρίσκουμε την ακόλουθη διεύθυνση υποδικτύου: 147.102.236
2.7) Χρησιμοποιώντας την εντολή `ifconfig` βρίσκουμε την ακόλουθη IPv6: fe80::19:ceda:59e9:b423
2.8) Χρησιμοποιώντας την εντολή `netstat -nr` βρίσκουμε την ακόλουθη προκαθορισμένη πύλη: 147.102.236.200
2.9) Χρησιμοποιώντας την εντολή `scutil --dns | grep 'nameserver\[[0-9]*\]` βρίσκουμε την ακόλουθη διεύθυνση του DNS server: 147.102.224.243
2.10) Χρησιμοποιώντας την εντολή `ipconfig getpacket en0` βρίσκουμε την ακόλουθη διεύθυνση IPv4 του εξυπηρετητή DHCP: 147.102.236.230

2.11) Χρησιμοποιώντας την εντολή `sudo netstat -I en0 -b` βρίσκουμε ότι ο αριθμός των πλαισίων που έστειλε 125494379 και έλαβε 95308991 αντίστοιχα η κάρτα δικτύου είναι οι παραπάνω και η αντιστοιχία τους σε bytes είναι: 172259378422 (απεσταλμένα) και 12353745621 (ληφθέντα).

2.12) Χρησιμοποιώντας την εντολή `sudo netstat -s -s -p ip` βρίσκουμε ότι ο αριθμός πακέτων IPv4 που έστειλε και έλαβε η κάρτα δικτύου του υπολογιστή είναι: 110119142 και 92594640 αντίστοιχα.

2.13) Χρησιμοποιώντας την εντολή `sudo netstat -a | grep ESTABLISHED` βρίσκω ότι ο αριθμός των εγκατεστημένων (established) συνδέσεων TCP του υπολογιστή μου με άλλους υπολογιστές είναι 2.

2.14) Χρησιμοποιώντας την εντολή `sudo netstat -a | grep ESTABLISHED` βρίσκουμε ότι για δύο από τις παραπάνω συνδέσεις TCP, οι θύρες πηγής και προορισμού είναι οι εξής:

- Θύρα πηγής: 58063 και θύρα προορισμού: 5228
- Θύρα πηγής: 49214 και θύρα προορισμού: 5223

Άσκηση 3: Αναλυτής Πρωτοκόλλων Wireshark

3.1) Τα πρωτόκολλα που εμφανίζονται για την διεύθυνση 147.102.40.15 είναι μόνο TCP και HTTP.

3.2) Η διεύθυνση MAC του υπολογιστή μου σε δεκαεξαδική μορφή είναι: fc:e2:6c:02:ce:3f , όπως φαίνεται και παρακάτω:

```
Ethernet II, Src: Apple_02:ce:3f (fc:e2:6c:02:ce:3f),
```

3.3) Ο κατασκευαστής της κάρτας δικτύου είναι η Apple.

```
Ethernet II, Src: Apple_02:ce:3f (fc:e2:6c:02:ce:3f),
```

3.4) Η διεύθυνση IPv4 του υπολογιστή μου είναι η: 147.102.203.155

```
Internet Protocol Version 4, Src: 147.102.203.155, Dst: 147.102.40.15
```

3.5) Η διεύθυνση IPv4 του http://edu-dy.cn.ntua.gr είναι η: 147.102.40.15

3.6) Η σύνταξη του φίλτρου που εμφανίζεται στο πεδίο του φίλτρου απεικόνισης είναι: tcp.stream eq 5

3.7)

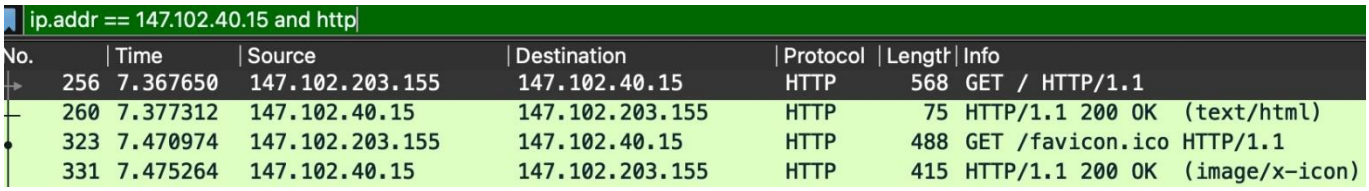
i) Ο τύπος του εξυπηρετητή ιστού που φιλοξενεί τη σελίδα που επισκέφθηκα είναι ο server Apache/2.2.22

ii) Ο τίτλος και το αντίστοιχο HTML tag της σελίδας που επισκέφθηκα είναι: <title>CN Lab1</title>

iii)Ο τίτλος εμφανίζεται στο παράθυρο που άνοιξε μετά το follow TCP Stream και είναι το ακόλουθο:

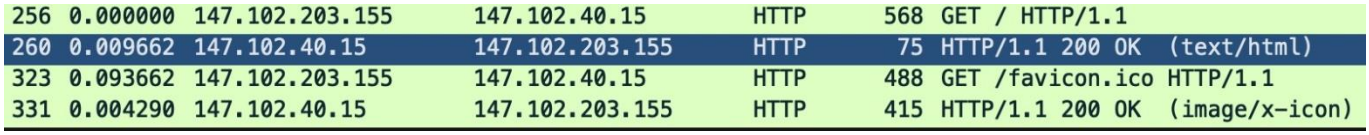
```
HTTP/1.1 200 OK
Date: Sun, 09 Oct 2022 20:33:09 GMT
Server: Apache/2.2.22 (FreeBSD) mod_ssl/2.2.22 OpenSSL/0.9.8zh-freebsd DAV/2
Last-Modified: Sat, 08 Oct 2022 23:57:10 GMT
ETag: "172914-9e-5ea8eaf3fc180"
Accept-Ranges: bytes
Content-Length: 158
Cache-Control: max-age=84600, public
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

<html>
   <head>
      <title>CN Lab1</title>
   </head>
   <body>
         <h1>It works!</h1>
         <h2>Computer Networks 2022-23</h2>
         <h3>Lab 1</h3>
   </body>
</html>
```

3.8) Η σύνταξή του φίλτρου ώστε να εμφανίζονται μόνο τα πρωτόκολλα HTTP είναι η ακόλουθη:



3.9) Στάλθηκαν 2 μηνύματα HTTP και αντίστοιχα λήφθηκαν 2.

3.10) Ο χρόνος που πέρασε από τη στιγμή που στάλθηκε το πρώτο αίτημα GET μέχρι να ληφθεί η απόκριση 200 OK είναι 0.009662s.

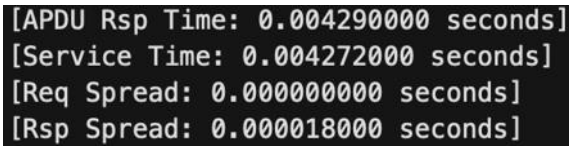


3.11) Χρειάστηκαν 8 πακέτα για την ολοκλήρωση της μετάδοσης και ακολουθούν και οι αύξοντες αριθμοί τους.

3.12) Το φίλτρο που χρησιμοποίησα για να εμφανίσω μόνο τα τεμάχια TCP είναι: `ip.addr == 147.102.40.15 and tcp and !http`.

3.13) Ο χρόνος που πέρασε για να ληφθεί το 1ο εξ αυτών είναι: (First TCP - HTTP GET favicon) = 0.004272s . Ο χρόνος που πέρασε για να ολοκληρωθεί και η μετάδοση των επόμενων είναι: (Last TCP - First TCP) = 0.000018s . Ο συνολικός χρόνος απόκρισης στο αίτημα GET είναι: (HTTP 200 OK favicon - HTTP GET favicon) = 0.00429s .

3.14) Οι χρόνοι με την χρήση του `TRANSUM RTE Data` είναι οι παρακάτω:



Παρατηρώ ότι το APDU Rsp Time είναι ίδιο με τον συνολικό χρόνο που χρειάστηκε από το HTTP GET favicon μέχρι το HTTP 200 OK favicon. Το Service Time είναι ο χρόνος που χρειάστηκε ο Server να αποκριθεί στο αίτημά HTTP GET favicon και το Rsp Spread είναι ο χρόνος που χρειάστηκαν όλα τα τεμάχια TCP για να ολοκληρωθούν.

3.15) Το φίλτρο που χρησιμοποίησα για να εμφανίσω μόνο τα μηνύματα HTTP που έστειλε ο υπολογιστής μου είναι: `ip.src == 147.102.203.155 and http` .