

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ
ΥΠΟΛΟΓΙΣΤΩΝ
ΡΟΗ Δ - ΔΙΚΤΥΑ ΥΠΟΛΟΓΙΣΤΩΝ (COMPUTER NETWORKS)

ΓΕΩΡΓΑΚΟΠΟΥΛΟΣ ΓΕΩΡΓΙΟΣ 03120827

ΑΝΑΦΟΡΑ 1ΗΣ ΕΡΓΑΣΤΗΡΙΑΚΗΣ ΑΣΚΗΣΗΣ

Λογισμικό: Linux Ubuntu 20.04

Όνομα PC: glaptop

Διεύθυνση IP: 192.168.2.8

Διεύθυνση MAC: 70:9c:d1:03:b0:15

ΑΣΚΗΣΗ 1: Βρείτε την κάρτα δικτύου.

Σχόλια - Παρατηρήσεις:

1. Η 1η άσκηση έγινε στον προσωπικό μου υπολογιστή με σύνδεση στο οικιακό wifi.
2. Στο λειτουργικό σύστημα που χρησιμοποιώ , δεν υπάρχει καποιο γραφικό περιβάλλον που να φαίνεται η κάρτα δικτύου, για να αντλήσω τις πληροφορίες από εκεί, όπως γίνεται στα windows. Επομένως όλες οι πληροφορίες βρέθηκαν με χρήση του terminal.

1.1 Network adapter name: wlp0s20f3

* Χρησιμοποιώντας την εντολή ifconfig

1.2 Είδος σύνδεσης: Wifi

* Χρησιμοποιώντας την εντολή nmcli

1.3 Ταχύτητα Σύνδεσης: 98.05 Mbps

* Χρησιμοποιώντας την εντολή speedtest-cli

1.4 Διεύθυνση υπο-στρώματος MAC: 70:9c:d1:03:b0:15

* Χρησιμοποιώντας την εντολή ifconfig

1.5 Διεύθυνση IPv4: 192.168.2.8

1.6 Διεύθυνση IPv6: 2a02:85f:ece1:ee00:e2af:774f:d1ac:28bc/64

1.7 Διεύθυνση DNS εξυπηρετητή: Current DNS Server: 2a02:858::8888

* Χρησιμοποιώντας την εντολή resolvectl status

1.8 Διεύθυνση προκαθορισμένης πύλης: 192.168.2.1

* Χρησιμοποιώντας την εντολή route -n

ΑΣΚΗΣΗ 2: Ρυθμίσεις και Στατιστικά

Σχόλια:

1. Η 2η ασκηση εγινε στον προσωπικό μου υπολογιστή με συνδεση στο wifi του πολυτεχνείου (eduroam).

2.1 Ονομα του υπολογιστή: glaptop

* Χρησιμοποιώντας την εντολή hostname

2.2 Ονόματα καρτων δικτύου: wlp0s20f3

* Χρησιμοποιώντας την εντολή ifconfig

2.3 Διεύθυνση υπο-στρώματος MAC: ether 70:9c:d1:03:b0:15

* Χρησιμοποιώντας την εντολή ifconfig

2.4 Ταχύτητα Συνδεσης: txqueuelen 1000. Αρα 1000 Mbps. Αρα 1 Gbps

* Χρησιμοποιώντας την εντολή ifconfig

2.5 Διεύθυνση IPv4: inet 147.102.239.218

* Χρησιμοποιώντας την εντολή ifconfig

2.6 Μάσκα Υποδικτύου: netmask 255.255.252.0

* Χρησιμοποιώντας την εντολή ifconfig

i) Το μήκος προθέματος δικτυου ειναι το πληθος των ασσων στο subnet mask. Επομενως $8+8+6=22$.

ii) Η διευθυνση υποδικτυου ειναι το λογικο AND της διευθυνσης IPv4 και της netmask, εκφρασμενες σε bit. Αρα 147.102.236.0

2.7 Διεύθυνση IPv6: inet6 fe80::c10a:ffa:fe29:4d09

* Χρησιμοποιώντας την εντολή ifconfig

2.8 Διεύθυνση προκαθορισμένης πύλης: 147.102.236.200

* Χρησιμοποιώντας την εντολή route -n

2.9 Διεύθυνση DNS εξυπηρετητή: Current DNS Server: 147.102.224.243

* Χρησιμοποιώντας την εντολή resolvectl status

2.10 Βρισκουμε το /var/lib/dhcp/dhclient.leases το οποιο ομως ειναι αδειο Τρεξαμε το `sudo dhclient -d -nw wlp0s20f3`

Βγαζει: DHCPOFFER of 147.102.239.103 from 147.102.236.230

Αρα διευθυνση εξυπηρετητή DHCP: 147.102.236.230

2.11 Αριθμός Πλαισίων Ethernet και πλήθος byte που εστειλε και έλαβε η καρτα δικτύου:

RX: bytes packets errors dropped missed mcast

167247449 317307 0 23 0 0

TX: bytes packets errors dropped carrier collsns

14616243 58483 0 0 0 0

* Χρησιμοποιώντας την εντολή `ip -s link show wlp0s20f3`

2.12 Αριθμός πακέτων IPv4:

298153 total packets received

64569 requests sent out

* Χρησιμοποιώντας την εντολή `netstat -s4`

2.13 Αριθμός εγκατεστημένων συνδέσεων TCP: 8

* Χρησιμοποιώντας την εντολή `netstat -ant|grep ESTABLISHED | wc -l`

2.14 Θυρες πηγής και προορισμού:

147.102.239.218:47244 35.201.100.119:443
147.102.239.218:54922 108.177.126.188:5228

* Χρησιμοποιώντας την εντολή netstat -ant|grep ESTABLISHED

ΑΣΚΗΣΗ 3: Αναλυτής Πρωτοκόλλων Wireshark

Σχόλια:

2. Η 3η άσκηση έγινε στον προσωπικό μου υπολογιστή με σύνδεση στο wifi του πολυτεχνείου (eduroam).
3. Η καταγραφή έγινε διαφορετική μέρα με την άσκηση 2.

3.1 Εφαρμόζοντας το φίλτρο απεικόνισης ip.addr == 147.102.40.15 βλέπουμε όλα τα πακέτα που ανταλλάχθηκαν με τον εξυπηρετητή ιστού της σελίδας edu-dy.cn.ntua.gr.

Τα διαφορετικά πρωτόκολλα που εμφανίζονται είναι: HTTP, TCP, TLSv1

GET

```
Frame 278: 894 bytes on wire (7152 bits), 894 bytes captured (7152 bits) on interface wlp0s20f3, id 0  
Ethernet II, Src: IntelCor_03:b0:15 (70:9c:d1:03:b0:15), Dst: Cisco_d0:d9:1d (08:ec:f5:d0:d9:1d)  
Internet Protocol Version 4, Src: 147.102.200.52, Dst: 147.102.40.15  
Transmission Control Protocol, Src Port: 46970, Dst Port: 80, Seq: 1, Ack: 1, Len: 828  
Hypertext Transfer Protocol
```

200 OK

```
Frame 281: 599 bytes on wire (4792 bits), 599 bytes captured (4792 bits) on interface wlp0s20f3, id 0  
Ethernet II, Src: Cisco_d0:d9:1d (08:ec:f5:d0:d9:1d), Dst: IntelCor_03:b0:15 (70:9c:d1:03:b0:15)  
Internet Protocol Version 4, Src: 147.102.40.15, Dst: 147.102.200.52  
Transmission Control Protocol, Src Port: 80, Dst Port: 46970, Seq: 1, Ack: 829, Len: 533  
Hypertext Transfer Protocol  
Line-based text data: text/html (10 lines)
```

3.2 Διευθυνση MAC: 70:9c:d1:03:b0:15

3.3 Τα bit του κατασκευαστή είναι τα πρώτα 3 bytes εκτός του 1ου και του 2ου bit. Προκύπτει ότι ο κατασκευαστής είναι η Intel Corp

3.4 Διευθυνση IPv4: 147.102.200.52

* Η καταγραφή έγινε διαφορετική μέρα με την άσκηση 2, για αυτό έχουμε διαφορετικές διευθύνσεις IPv4.

3.5 Διευθυνση IPv4 του edu-dy.cn.ntua.gr: 147.102.40.15

The screenshot shows the Wireshark interface with a packet capture of a GET request and a 200 OK response. The packet list on the left shows frames 327 and 328. The packet details pane on the right shows the structure of the HTTP request and response, including headers like Host, User-Agent, Accept, and cookies.

No.	Time	Source	Destination	Protocol	Length	Info
327	4.264855465	147.102.200.52	147.102.40.15	TCP	66	46970 → 80 [ACK] Seq=16
328	4.264890632	147.102.40.15	147.102.200.52	HTTP	4083	HTTP/1.1 200 OK (image)
329	4.264890626	147.102.40.15	147.102.200.52	TCP	66	80 → 46970 [ACK] Seq=53
324	4.262407883	147.102.200.52	147.102.40.15	HTTP	840	GET /favicon.ico HTTP/1
282	4.139799502	147.102.200.52	147.102.40.15	TCP	66	46970 → 80 [ACK] Seq=82
281	4.139773178	147.102.40.15	147.102.200.52	HTTP	599	HTTP/1.1 200 OK (text/
280	4.139103376	147.102.40.15	147.102.200.52	TCP	66	80 → 46970 [ACK] Seq=1
278	4.136091706	147.102.200.52	147.102.40.15	HTTP	894	GET / HTTP/1.1
249	4.119976414	147.102.200.52	147.102.40.15	TCP	66	46970 → 80 [ACK] Seq=1
245	4.119879197	147.102.40.15	147.102.200.52	TCP	74	80 → 46970 [SYN, ACK] S
243	4.118228801	147.102.200.52	147.102.40.15	TCP	74	46970 → 80 [SYN] Seq=0

GET / HTTP/1.1
Host: edu-dy.cn.ntua.gr
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/117.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: el-GR,el;q=0.9
Cookie: _ga_P1H85FV7M1=GS1.1.1684823816.1.1.1684823844.0.0.0; _ga_DB55ZNXH=GS1.2.1692025059.1.1.1692025061.0.0.0; _ga_XNYYPKSG03=GS1.1.1694196126.1.0.1694196134.0.0.0; _ga_DZ8LQ4EHBC=GS1.1.1695250051.4.0.1695250051.0.0.0; _ga=GAI.2.336243303.1677595549; _ga_11YT0PZY6X=GS1.2.1696170658.1.0.1696170658.0.0.0; _gid=GA1.2.939464379.1696511330; _gat=1; _ga_BQ6WS9N7TV=GS1.2.1696511330.24.1.1696511411.0.0.0

HTTP/1.1 200 OK
Date: Wed, 27 Sep 2023 09:35:39 GMT
Server: Apache/2.2.22 (FreeBSD) mod_ssl/2.2.22 OpenSSL/0.9.8zh-freebsd DAV/2
Last-Modified: Wed, 20 Sep 2023 05:59:09 GMT
ETag: "172914-9e-605c412e52540"
Accept-Ranges: bytes

3.6 Σύνταξη του φίλτρου: tcp.stream eq 4

3.7 i) Τυπος εξυπηρετητή ιστού: erver: Apache/2.2.22 (FreeBSD)

ii) Τίτλος και HTML tag: <title>CN Lab1</title>

iii) Πανω στην αντιστοιχη καρτέλα.

3.8 Κατάλληλο φίλτρο: (ip.addr == 147.102.40.15)&&(http)

(ip.addr == 147.102.40.15)&&(http)						
No.	Time	Source	Destination	Protocol	Length	Info
326	4.264800632	147.102.40.15	147.102.200.52	HTTP	4083	HTTP/1.1 200 OK (image/
324	4.262407883	147.102.200.52	147.102.40.15	HTTP	840	GET /favicon.ico HTTP/1.1
281	4.139773178	147.102.40.15	147.102.200.52	HTTP	599	HTTP/1.1 200 OK (text/
278	4.136091706	147.102.200.52	147.102.40.15	HTTP	894	GET / HTTP/1.1

3.9 Στάλθηκαν 2 http μηνύματα και λήφθηκαν 2 http μηνύματα

3.10 Από την ακόλουθη φωτογραφία, έχοντας αλλάξει το view, παρατηρούμε ότι από την στιγμή που στάλθηκε το πρώτο αίτημα GET μεχρι να ληφθεί απόκριση του 200 OK πέρασαν 0.0037 sec

(ip.addr == 147.102.40.15)&&(http)						
No.	Time	Source	Destination	Protocol	Length	Info
326	0.002392749	147.102.40.15	147.102.200.52	HTTP	4083	HTTP/1.1 200 OK (image/x
324	0.122634705	147.102.200.52	147.102.40.15	HTTP	840	GET /favicon.ico HTTP/1.1
281	0.003681472	147.102.40.15	147.102.200.52	HTTP	599	HTTP/1.1 200 OK (text/ht
278	0.000000000	147.102.200.52	147.102.40.15	HTTP	894	GET / HTTP/1.1

3.11

282	0.000026324	147.102.200.52	147.102.40.15	TCP	66	46970 → 80 [ACK]
324	0.122608381	147.102.200.52	147.102.40.15	HTTP	840	GET /favicon.ico
325	0.002392343	147.102.40.15	147.102.200.52	TCP	66	80 → 46970 [ACK]
326	0.000000406	147.102.40.15	147.102.200.52	HTTP	4083	HTTP/1.1 200 OK
327	0.000054833	147.102.200.52	147.102.40.15	TCP	66	46970 → 80 [ACK]

Βλέπουμε ότι χρειάζεται 1 πακέτα για να ολοκληρωθεί η μετάδοση. Επομένως ειχε δημιουργηθεί πρόβλημα με την μνημη cache.

*Σχολιο:

Σε διαφορετικό λειτουργικο παρατηρώ ότι χρειάζεται μεγαλύτερο αριθμό πακέτων

82	0.046307	192.168.2.6	147.102.40.15	TCP	54	62797 → 80 [ACK] Seq=51
96	0.154992	192.168.2.6	147.102.40.15	HTTP	581	GET /favicon.ico HTTP/1.1
97	0.009164	147.102.40.15	192.168.2.6	TCP	590	80 → 62797 [ACK] Seq=51
98	0.000000	147.102.40.15	192.168.2.6	TCP	590	80 → 62797 [ACK] Seq=1
99	0.000153	192.168.2.6	147.102.40.15	TCP	54	62797 → 80 [ACK] Seq=1
100	0.000029	147.102.40.15	192.168.2.6	TCP	590	80 → 62797 [ACK] Seq=1
101	0.000000	147.102.40.15	192.168.2.6	TCP	590	80 → 62797 [ACK] Seq=2
102	0.000000	147.102.40.15	192.168.2.6	TCP	590	80 → 62797 [ACK] Seq=2
103	0.000061	192.168.2.6	147.102.40.15	TCP	54	62797 → 80 [ACK] Seq=1
104	0.000210	147.102.40.15	192.168.2.6	TCP	590	80 → 62797 [ACK] Seq=3
105	0.000000	147.102.40.15	192.168.2.6	TCP	590	80 → 62797 [ACK] Seq=3
106	0.000000	147.102.40.15	192.168.2.6	HTTP	319	HTTP/1.1 200 OK (image/
107	0.000069	192.168.2.6	147.102.40.15	TCP	54	62797 → 80 [ACK] Seq=1

Σε αυτή την περίπτωση, χρησιμοποιώντας τον 2ο προσωπικό μου υπολογιστή (Windows 10 , IPv4=192.168.2.6) βλέπω ότι χρειάζεται 8 πακέτα

3.12 Κατάλληλο φίλτρο:

(ip.addr == 147.102.40.15)&&(tcp)&&(!http)&&(!tls)

*Τα Επόμενα 2 ερωτήματα (3.13 και 3.14) θα γίνουν με βάση την καταγραφή από windows για περισσότερη σαφήνεια. Η άσκηση λύνεται σε όλα τα λειτουργικά.

3.13 Χρησιμοποιώντας το view “seconds since previous displayed packet” βλέπουμε ότι:

Χρονος μεχρι να ληφθεί το πρώτο εξ αυτών: 0.009164 sec

Χρονος από το 1ο μεχρι να ολοκληρωθεί η μετάδοση: 0.453 msec

(Συγκρινουμε τους χρόνους από το 1ο εως το τελευταio tcp segment)

Χρόνος για να ολοκληρωθεί η απόκριση στο αίτημα: 0.9617 msec

(Χρονος από το GET μεχρι το 200 OK)

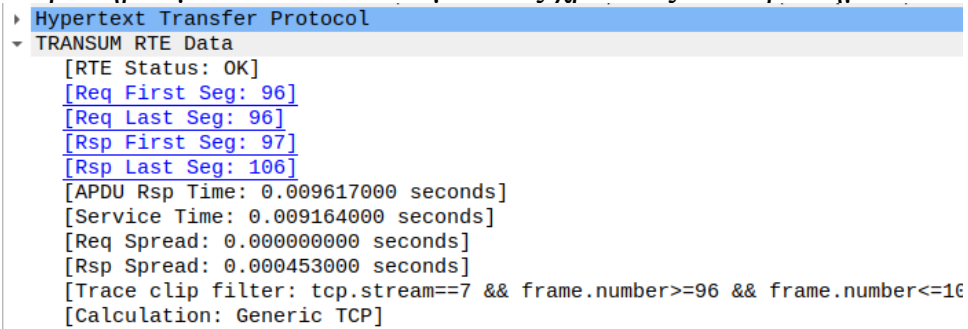
3.14 Οι χρόνοι από το TRANSUM είναι:

Service time: 0.009164 sec

Response Spread: 0.000453 sec

Application PDU Response time: 0.009617 sec

Παρατηρούμε ότι είναι ίδιοι με τους χρόνους στο ερώτημα 3.13



The screenshot shows the 'Hypertext Transfer Protocol' section expanded in Wireshark. Under 'TRANSUM RTE Data', the following information is displayed:

- [RTE Status: OK]
- [Req First Seg: 96]
- [Req Last Seg: 96]
- [Rsp First Seg: 97]
- [Rsp Last Seg: 106]
- [APDU Rsp Time: 0.009617000 seconds]
- [Service Time: 0.009164000 seconds]
- [Req Spread: 0.000000000 seconds]
- [Rsp Spread: 0.000453000 seconds]
- [Trace clip filter: tcp.stream==7 && frame.number>=96 && frame.number<=106]
- [Calculation: Generic TCP]

3.15 ip.src==(147.102.200.52)&&(http)