



ΔΙΚΤΥΑ ΕΠΙΚΟΙΝΩΝΙΩΝ

2^η Εργασία με χρήση του λογισμικού WireShark

ΑΡΙΣΤΕΙΔΗΣ ΧΡΟΝΟΠΟΥΛΟΣ P3160194

ΕΡΩΤΗΣΕΙΣ: 1. Για IPv4: UDP = 1655

TCP = 3036

Topic / Item	Count
▼ IP Protocol Types	4701
UDP	1655
TCP	3036

Για IPv6: UDP = 0

TCP = 0

2. Τα διαφορετικά endpoint με τα οποία υπάρχει επικοινωνία σε επίπεδο ethernet είναι τα εξής:

- 01:00:5e:00:00:01
- 01:00:5e:00:00:fb
- 01:00:5e:00:00:fc
- 01:00:5e:7f:ff:fa
- 10:50:72:28:b3:20
- 40:b0:76:de:0d:49
- b4:2e:99:cb:df:69
- ff:ff:ff:ff:ff:ff

Αντιστοιχούν στις συσκευές με τις οποίες επικοινωνεί ο server.

3. Τα endpoints με τα οποία υπάρχει επικοινωνία σε επίπεδο IP είναι τα εξής:

Ethernet · 8	IPv4 · 42	IPv6
--------------	-----------	------

42 για IPv4 και 0 για IPv6.

35.186.224.25
35.186.224.47
52.113.199.107
52.113.205.249
52.114.77.33
64.233.184.188
79.110.86.107
79.110.86.147
93.184.220.29
93.184.220.66
104.244.42.8
140.82.114.26
142.250.184.131
142.250.184.138
142.250.184.142
157.240.9.23
157.240.9.35
162.125.19.130
172.67.75.39
172.217.17.174
172.217.17.227
172.217.17.234
172.217.169.99
172.217.169.110
172.217.169.118
172.217.169.142
172.217.169.195
185.199.108.154
192.0.73.2
192.168.2.1
192.168.2.4
192.168.2.5
192.168.2.255
195.201.241.83
216.58.206.173
216.58.212.1
216.58.214.132
216.58.214.142
224.0.0.1
224.0.0.251
224.0.0.252
239.255.255.250

Αυτά τα endpoints δεν ταυτίζονται με τα endpoints σε επίπεδο ethernet διότι τα endpoints του ethernet αναφέρονται σε MAC ενώ αυτά σε IP.

4. Τα ports που χρησιμοποιήθηκαν από τον υπολογιστή μου προς τον DNS server είναι τα εξής:

SOURCE PORT	DESTINATION
65462	53
57956	
59802	
55492	
65443	
57686	
61881	
57579	
55338	
60785	
64069	
56400	
...	

Τα ports που χρησιμοποιήθηκαν από το DNS server προς τον υπολογιστή μου είναι τα εξής:

SOURCE PORT	DESTINATION
53	65462
	57956
	59802
	55492
	65443
	57686
	61881
	57579
	55338
	60785
	64069

	56400 ...
--	--------------

5. Αν είναι ερώτημα το καταλαβαίνουμε πρώτα απ' όλα από το (query) που βρίσκεται σε παρένθεση στο dns. Επίσης το dst port είναι 53 και το src είναι η IP διεύθυνση μας.

```
> Internet Protocol Version 4, Src: 192.168.2.4, Dst: 192.168.2.1
> User Datagram Protocol, Src Port: 57579, Dst Port: 53
▼ Domain Name System (query)
```

Αν είναι απάντηση σε ερώτημα το καταλαβαίνουμε από το (response) που βρίσκεται σε παρένθεση στο dns. Επίσης το src port είναι 53 και το destination είναι η IP διεύθυνση μας.

```
> Internet Protocol Version 4, Src: 192.168.2.1, Dst: 192.168.2.4
> User Datagram Protocol, Src Port: 53, Dst Port: 57579
▼ Domain Name System (response)
```

Το πακέτο ερώτησης με το πακέτο απάντησης συνδέονται μέσω του src port και dst port αντιστοίχα.

6. Υπάρχει σημαία και πας λέει ότι δεν είναι authoritative.

```
▼ Flags: 0x8180 Standard query response, No error
```

```
Authoritative: Server is not an authority for domain
```

7. Το www.book4book.gr είναι canonical name. Η IP διεύθυνση που αντιστοιχεί στο www.book4book.gr είναι 195.201.241.83

```
C:\Users\arhsxro>tracert www.book4book.gr

Tracing route to book4book.gr [195.201.241.83]
over a maximum of 30 hops:
```

8. Αυτά τα 3 βήματα είναι τα εξής:

- **SYN:** Ο client θέλει να εγκαθιδρύσει σύνδεση με τον servers και του στέλνει ένα segment με SYN. Το SYN δηλώνει με ποιόν αριθμό ξεκινάνε τα segments του. Με την αποστολή αυτή δηλώνει ότι είναι πολύ πιθανό να ξεκινήσει επικοινωνία με τον server.
- **SYN,ACK:** Ο server απαντάει στο αίτημα του client με ένα σέτ από SYN-ACK signal bits. Το ACK δηλώνει την απάντηση στο segment που ο χρήστης έστειλε και το SYN δηλώνει τον αριθμό με τον οποίο ο server θα ξεκινάει τα segments του.
- **ACK:** Ο client τώρα αναγνωρίζει το response από τον server και πλέον εγκαθιδρύεται μια secure σύνδεση μεταξύ τους για μεταφορά data.

33	3.056817	192.168.2.4	52.113.199.107	TCP	66 63356 → 443 [SYN] Seq=0
34	3.130271	52.113.199.107	192.168.2.4	TCP	66 443 → 63356 [SYN, ACK] S
35	3.130361	192.168.2.4	52.113.199.107	TCP	54 63356 → 443 [ACK] Seq=1

9. GET

SOURCE PORT	DESTINATION PORT
63360	80
63361	
63362	
63363	
...	

HTTP

SOURCE PORT	DESTINATION PORT
80	63360
	63361
	63362
	63363
	...

Παρατηρούμε ότι ο client χρησιμοποιεί τα ports 63360 .. ενώ ο server το 80.Ο client στέλνει αίτημα μέσω αυτών και λαμβάνει response επίσης.Αντίστοιχα ο server στέλνει response και λαμβάνει αίτηματα μέσω του 80.

Το HTTP χρησιμοποιεί TCP πρωτόκολλο επιπέδου μεταφοράς.Πρωτού ο client ανταλλάξει request/response μηνύματα με τον server πρέπει να εγκαθιδρύσει ένα TCP connection.

10.Ο browser έστειλε αρκετά HTTP GET requests.Τα μηνύματα αυτά στάλθηκαν στο www.book4book με IP διεύθυνση:195.201.241.83

512	16.671698	192.168.2.4	195.201.241.83	HTTP	507	GET /wp-content/plugins/the-events-calendar/resources/events.css HTTP/1.1
572	16.721484	192.168.2.4	195.201.241.83	HTTP	509	GET /wp-content/plugins/smart-youtube//themes/theme10/colorbox.css HTTP/1.1
576	16.741176	192.168.2.4	195.201.241.83	HTTP	529	GET /wp-content/plugins/jquery-vertical-accordion-menu/skin.php?widget_id=3&skin=clean HTTP/1.1
581	16.750885	192.168.2.4	195.201.241.83	HTTP	553	GET /wp-content/themes/custom-community-pro/_inc/css/reset.css HTTP/1.1
587	16.754615	192.168.2.4	195.201.241.83	HTTP	498	GET /wp-content/plugins/sitepress-multilingual-cms/res/js/sitepress.js HTTP/1.1
600	16.772788	192.168.2.4	195.201.241.83	HTTP	474	GET /wp-includes/js/jquery/jquery.js?ver=1.7.1 HTTP/1.1
931	17.139609	192.168.2.4	195.201.241.83	HTTP	542	GET /wp-content/plugins/sitepress-multilingual-cms/res/flags/el.png HTTP/1.1
964	17.148838	192.168.2.4	195.201.241.83	HTTP	542	GET /wp-content/plugins/sitepress-multilingual-cms/res/flags/en.png HTTP/1.1
965	17.149855	192.168.2.4	195.201.241.83	HTTP	513	GET /wp-content/uploads/2014/06/cy.gif HTTP/1.1
966	17.149991	192.168.2.4	195.201.241.83	HTTP	542	GET /wp-content/plugins/sitepress-multilingual-cms/res/flags/lk.png HTTP/1.1
967	17.150587	192.168.2.4	195.201.241.83	HTTP	522	GET /wp-content/uploads/2012/05/searchthing.png HTTP/1.1
1052	17.260616	192.168.2.4	195.201.241.83	HTTP	484	GET /none HTTP/1.1
1053	17.260845	192.168.2.4	195.201.241.83	HTTP	524	GET /wp-content/uploads/2012/05/book4bookmenu.png HTTP/1.1

11. Η έκδοση που τρέχει ο browser είναι:HTTP/1.1

```
✓ Hypertext Transfer Protocol
> GET / HTTP/1.1\r\n
```

Η έκδοση που τρέχει ο server είναι:HTTP/1.1

```
✓ Hypertext Transfer Protocol
> HTTP/1.1 200 OK\r\n
```

Το λογισμικό web server που τρέχει ο server για το site είναι:Apache

```
Server: Apache\r\n
```