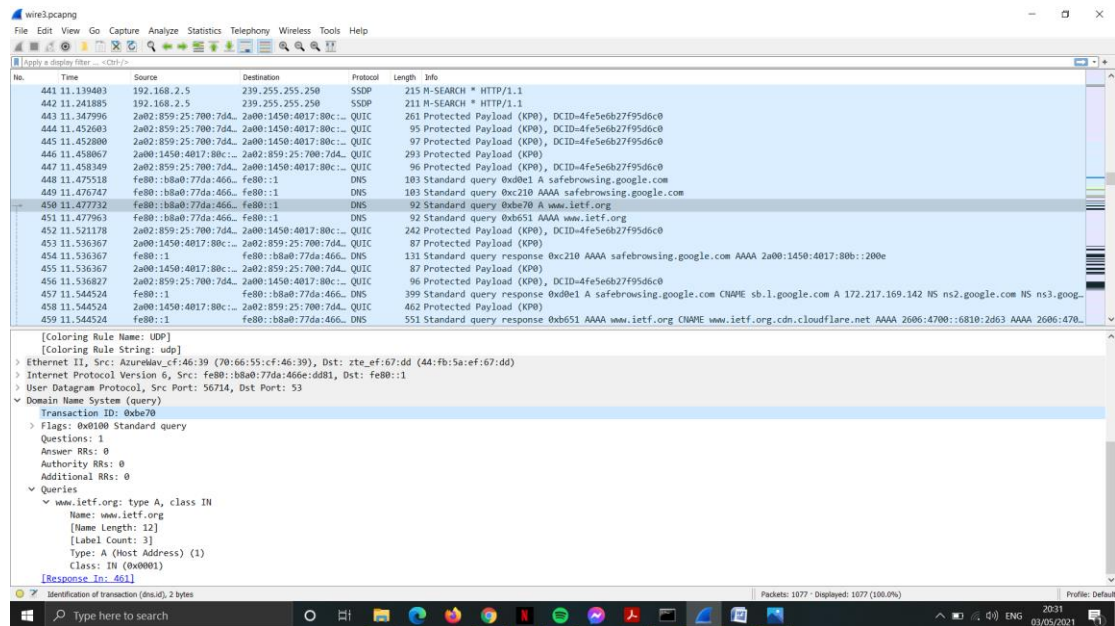


# ΔΙΚΤΥΑ ΠΡΩΤΗ ΕΡΓΑΣΤΗΡΙΑΚΗ

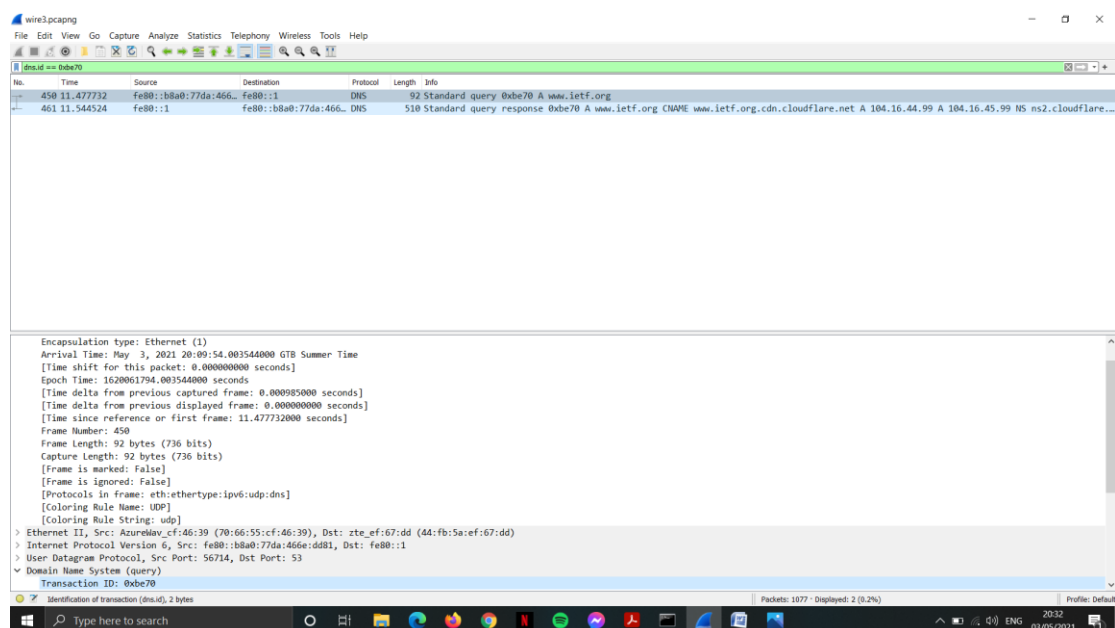
## Α' ΜΕΡΟΣ:

### 1. Μετάβαση σε ietf

Τα DNS πακέτα μεταξύ ερώτησης και απόκρισης



Τα δύο πακέτα που ερώτησης και απόκρισης



2. Στο πρώτο πεδίο έχουμε το χρόνο

Το πρωτόκολλο που χρησιμοποιείται για τη μεταφορά των πακέτων είναι το **User Datagram Protocol (UDP)**.

3. Το destination port ερώτησης είναι 53.

4. Το destination port απόκρισης είναι 53872.

5. Το μήνυμα ερώτησης βρίσκεται στη διεύθυνση fe80: :b8a0:77da:466e:dd81.

Μετά την εκτέλεση της ipconfig προκύπτει ότι η διεύθυνση του τοπικού DNS διακομιστή είναι: fe80: : b8a0:77da:466e:dd81%21

Παρατηρούμε ότι οι διευθύνσεις είναι ίδιες.

6. Στο frame 451, ο τύπος μηνύματος DNS ερώτησης (query) είναι standard query type: AAAA και δεν περιέχει καμία απάντηση.

7. Στο frame 459 βρίσκεται το μήνυμα απόκρισης, στο οποίο εμπεριέχονται 3 απαντήσεις, οι οποίες φαίνονται παρακάτω:

```
Class: IN (0x0001)
  v Answers
    v www.ietf.org: type CNAME, class IN, cname www.ietf.org.cdn.cloudflare.net
      Name: www.ietf.org
      Type: CNAME (Canonical NAME for an alias) (5)
      Class: IN (0x0001)
      Time to live: 1104 (18 minutes, 24 seconds)
      Data length: 33
      CNAME: www.ietf.org.cdn.cloudflare.net
    v www.ietf.org.cdn.cLOUDFLArE.net: type AAAA, class IN, addr 2606:4700::6810:2d63
      Name: www.ietf.org.cdn.cLOUDFLArE.net
      Type: AAAA (IPv6 Address) (28)
      Class: IN (0x0001)
      Time to live: 9 (9 seconds)
      Data length: 16
      AAAA Address: 2606:4700::6810:2d63
    v www.ietf.org.cdn.cLOUDFLArE.net: type AAAA, class IN, addr 2606:4700::6810:2c63
      Name: www.ietf.org.cdn.cLOUDFLArE.net
      Type: AAAA (IPv6 Address) (28)
      Class: IN (0x0001)
      Time to live: 9 (9 seconds)
      Data length: 16
      AAAA Address: 2606:4700::6810:2c63
  > Authoritative nameservers
```

8. Στο frame 464 βρίσκεται το επόμενο TCP SYN πακέτο και έχουμε:

Source Address: 2a02:859:25:700:7d4f:3c5c:767e:d83

9.

No.	Time	Source	Destination	Protocol	Length	Info
4 3.988859		fe80::b8a0:77da:466e::	fe80::1	DNS	94	Standard query 0x6d14 A www.google.com
5 3.989108		fe80::b8a0:77da:466e::	fe80::1	DNS	94	Standard query 0x3fd7 AAAA www.google.com
6 4.003437		fe80::1	fe80::b8a0:77da:466e::	DNS	358	Standard query response 0x6d14 A www.google.com A 142.250.187.100 NS ns2.google.com NS ns4.google.com NS ns1.google.com NS ns3.google.com
7 4.003437		fe80::1	fe80::b8a0:77da:466e::	DNS	370	Standard query response 0x3fd7 AAAA www.google.com AAAA 2a00:1450:4017:80e::2004 NS ns2.google.com NS ns4.google.com NS ns3.google.com
278 10.880974		fe80::b8a0:77da:466e::	fe80::1	DNS	103	Standard query 0xb37b A safebrowsing.google.com
279 10.881127		fe80::b8a0:77da:466e::	fe80::1	DNS	103	Standard query 0x7fd0 AAAA safebrowsing.google.com
280 10.882667		fe80::b8a0:77da:466e::	fe80::1	DNS	99	Standard query 0x340a A www.ceid.upatras.gr
281 10.882876		fe80::b8a0:77da:466e::	fe80::1	DNS	99	Standard query 0x8fd8 AAAA www.ceid.upatras.gr
283 10.896622		fe80::1	fe80::b8a0:77da:466e::	DNS	399	Standard query response 0xb37b A safebrowsing.google.com CNAME sb.l.google.com A 142.250.187.142 NS ns4.google.com NS ns2.google.com
284 10.896622		fe80::1	fe80::b8a0:77da:466e::	DNS	411	Standard query response 0x7fd0 AAAA safebrowsing.google.com CNAME sb.l.google.com AAAA 2a00:1450:4017:80e::200e NS ns1.google.com
286 10.903156		fe80::1	fe80::b8a0:77da:466e::	DNS	215	Standard query response 0x340a A www.ceid.upatras.gr CNAME web.ceid.upatras.gr A 150.140.141.173 NS F00.upnet.gr NS NIC.upatras.gr
287 10.904002		fe80::1	fe80::b8a0:77da:466e::	DNS	161	Standard query response 0x8fd8 AAAA www.ceid.upatras.gr CNAME web.ceid.upatras.gr SOA NIC.upatras.gr
355 11.879632		fe80::b8a0:77da:466e::	fe80::1	DNS	103	Standard query 0x8fd8 A maxcdn.bootstrapcdn.com
356 11.879751		fe80::b8a0:77da:466e::	fe80::1	DNS	103	Standard query 0xbdb5 AAAA maxcdn.bootstrapcdn.com
358 11.883195		fe80::b8a0:77da:466e::	fe80::1	DNS	99	Standard query 0xc1b4 A maps.googleapis.com
359 11.883347		fe80::b8a0:77da:466e::	fe80::1	DNS	99	Standard query 0xee3 AAAA maps.googleapis.com
367 11.893905		fe80::1	fe80::b8a0:77da:466e::	DNS	455	Standard query response 0x8fd8 A maxcdn.bootstrapcdn.com A 104.18.11.207 A 104.18.10.207 NS keenan.ns.cloudflare.com NS brenda.ns.cloudflare.com
374 11.894454		fe80::1	fe80::b8a0:77da:466e::	DNS	479	Standard query response 0xbdb5 AAAA maxcdn.bootstrapcdn.com AAAA 2606:4700::6812:acf AAAA 2606:4700::6812:bef NS brenda.ns.cloudflare.com
> Frame 280: 99 bytes on wire (792 bits), 99 bytes captured (792 bits) on interface \Device\NPF_{DAB3ABAS-235C-49E7-8311-79347392A084}, id 0						
Ethernet II, Src: AzureWav.cf:46:39 (78:66:55:cf:46:39), Dst: zte_ef:67:dd (44:fb:5a:ef:67:dd)						
> Destination: zte_ef:67:dd (44:fb:5a:ef:67:dd)						
> Source: AzureWav.cf:46:39 (78:66:55:cf:46:39)						
Type: IPv6 (0x86dd)						
Internet Protocol Version 6, Src: fe80::b8a0:77da:466e:dd81, Dst: fe80::1						
0110 .... = Version: 6						
> .... 0000 0000 ..... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)						
.... .... 1111 1110 0000 1101 0010 = Flow Label: 0xfe0a2						
Payload Length: 45						
Next Header: UDP (17)						
Hop Limit: 64						
Source Address: fe80::b8a0:77da:466e:dd81						
Destination Address: fe80::1						
> User Datagram Protocol, Src Port: 49686, Dst Port: 53						
> Domain Name System (query)						

Destination Port (query): 53

No.	Time	Source	Destination	Protocol	Length	Info
4 3.988859		fe80::b8a0:77da:466e::	fe80::1	DNS	94	Standard query 0x6d14 A www.google.com
5 3.989108		fe80::b8a0:77da:466e::	fe80::1	DNS	94	Standard query 0x3fd7 AAAA www.google.com
6 4.003437		fe80::1	fe80::b8a0:77da:466e::	DNS	358	Standard query response 0x6d14 A www.google.com A 142.250.187.100 NS ns2.google.com NS ns4.google.com NS ns1.google.com NS ns3.google.com
7 4.003437		fe80::1	fe80::b8a0:77da:466e::	DNS	370	Standard query response 0x3fd7 AAAA www.google.com AAAA 2a00:1450:4017:80e::2004 NS ns2.google.com NS ns4.google.com NS ns3.google.com
278 10.880974		fe80::b8a0:77da:466e::	fe80::1	DNS	103	Standard query 0xb37b A safebrowsing.google.com
279 10.881127		fe80::b8a0:77da:466e::	fe80::1	DNS	103	Standard query 0x7fd0 AAAA safebrowsing.google.com
280 10.882667		fe80::b8a0:77da:466e::	fe80::1	DNS	99	Standard query 0x340a A www.ceid.upatras.gr
281 10.882876		fe80::b8a0:77da:466e::	fe80::1	DNS	99	Standard query 0x8fd8 AAAA www.ceid.upatras.gr
283 10.896622		fe80::1	fe80::b8a0:77da:466e::	DNS	399	Standard query response 0xb37b A safebrowsing.google.com CNAME sb.l.google.com A 142.250.187.142 NS ns4.google.com NS ns2.google.com
284 10.896622		fe80::1	fe80::b8a0:77da:466e::	DNS	411	Standard query response 0x7fd0 AAAA safebrowsing.google.com CNAME sb.l.google.com AAAA 2a00:1450:4017:80e::200e NS ns1.google.com
286 10.903156		fe80::1	fe80::b8a0:77da:466e::	DNS	215	Standard query response 0x340a A www.ceid.upatras.gr CNAME web.ceid.upatras.gr A 150.140.141.173 NS F00.upnet.gr NS NIC.upatras.gr
287 10.904002		fe80::1	fe80::b8a0:77da:466e::	DNS	161	Standard query response 0x8fd8 AAAA www.ceid.upatras.gr CNAME web.ceid.upatras.gr SOA NIC.upatras.gr
355 11.879632		fe80::b8a0:77da:466e::	fe80::1	DNS	103	Standard query 0x8fd8 A maxcdn.bootstrapcdn.com
356 11.879751		fe80::b8a0:77da:466e::	fe80::1	DNS	103	Standard query 0xbdb5 AAAA maxcdn.bootstrapcdn.com
358 11.883195		fe80::b8a0:77da:466e::	fe80::1	DNS	99	Standard query 0xc1b4 A maps.googleapis.com
359 11.883347		fe80::b8a0:77da:466e::	fe80::1	DNS	99	Standard query 0xee3 AAAA maps.googleapis.com
367 11.893905		fe80::1	fe80::b8a0:77da:466e::	DNS	455	Standard query response 0x8fd8 A maxcdn.bootstrapcdn.com A 104.18.11.207 A 104.18.10.207 NS keenan.ns.cloudflare.com NS brenda.ns.cloudflare.com
374 11.894454		fe80::1	fe80::b8a0:77da:466e::	DNS	479	Standard query response 0xbdb5 AAAA maxcdn.bootstrapcdn.com AAAA 2606:4700::6812:acf AAAA 2606:4700::6812:bef NS brenda.ns.cloudflare.com
> Frame 286: 215 bytes on wire (1720 bits), 215 bytes captured (1720 bits) on interface \Device\NPF_{DAB3ABAS-235C-49E7-8311-79347392A084}, id 0						
Ethernet II, Src: zte_ef:67:dd (44:fb:5a:ef:67:dd), Dst: AzureWav.cf:46:39 (78:66:55:cf:46:39)						
Internet Protocol Version 6, Src: fe80::1, Dst: fe80::b8a0:77da:466e:dd81						
User Datagram Protocol, Src Port: 53, Dst Port: 49686						
Source Port: 53						
Destination Port: 49686						
Length: 161						
Checksum: 0x7057 [unverified]						
[Checksum Status: Unverified]						
[Stream index: 5]						
> [Timestamps]						
UDP payload (153 bytes)						
> Domain Name System (response)						

Source Port (response): 53

10.

Source Address (query, πρώτο screenshot ερωτήματος 9): fe80::b8a0:77da:466e:dd81

Που είναι ίδια με τη διεύθυνση του προεπιλεγμένου τοπικού διακομιστή DNS.

11.

Το μήνυμα ερώτησης είναι Standard Query και δεν περιέχει κάποια απάντηση.

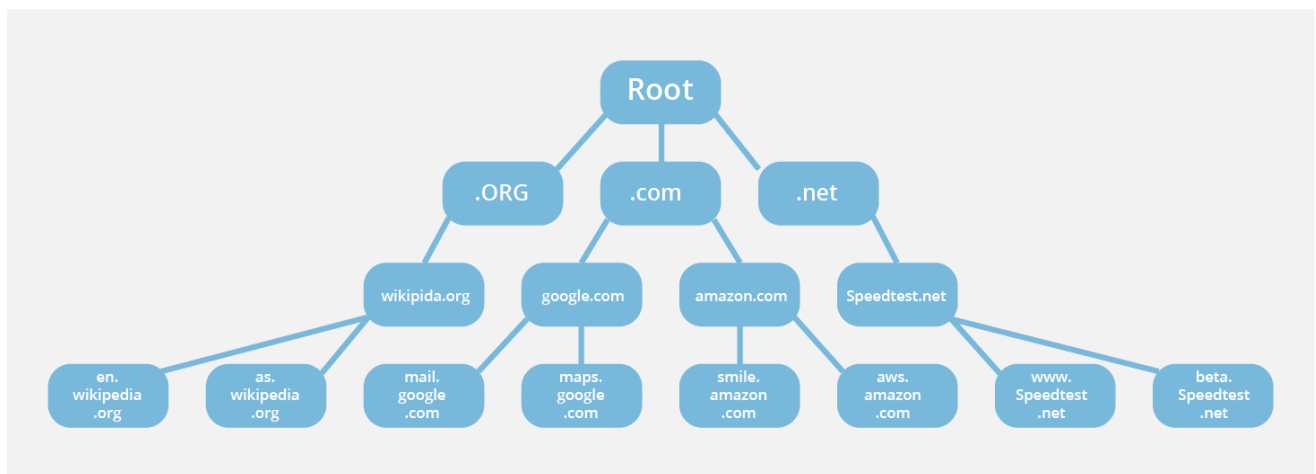
12.

Το μήνυμα απάντησης περιέχει 2 απαντήσεις, που φαίνονται παρακάτω:

```
> Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 2
Authority RRs: 2
Additional RRs: 2
> Queries
▼ Answers
  ▼ www.ceid.upatras.gr: type CNAME, class IN, cname web.ceid.upatras.gr
    Name: www.ceid.upatras.gr
    Type: CNAME (Canonical NAME for an alias) (5)
    Class: IN (0x0001)
    Time to live: 10800 (3 hours)
    Data length: 6
    CNAME: web.ceid.upatras.gr
  ▼ web.ceid.upatras.gr: type A, class IN, addr 150.140.141.173
    Name: web.ceid.upatras.gr
    Type: A (Host Address) (1)
    Class: IN (0x0001)
    Time to live: 6538 (1 hour, 48 minutes, 58 seconds)
    Data length: 4
    Address: 150.140.141.173
```

13.

Ιεραρχία DNS



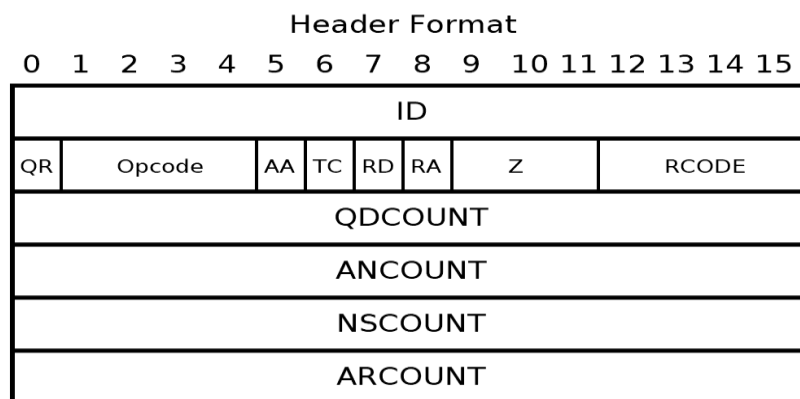
A. Το recursive resolver είναι η πρώτη στάση σε ένα ερώτημα DNS και λειτουργεί σαν ενδιάμεσος μεταξύ πελάτη και DNS name server.

B. Οι root name servers είναι DNS name servers, λειτουργούν στο root zone και απαντάνε κατευθείαν σε αιτήματα για αρχεία που βρίσκονται στο root zone κι επίσης μπορεί να παραπέμπουν άλλα αιτήματα στον κατάλληλο Top Level Domain (TLD) server.

Γ. Ο TLD name server διατηρεί πληροφορίες για όλα τα domain names που μοιράζονται κάποιο κοινό domain extension, όπως τα .com, .net κλπ. (Η δεύτερη σειρά στο διάγραμμα)

Δ. Ένας authoritative name server διατηρεί τα DNS records (A, CNAME, PTR κλπ) για έναν συγκεκριμένο τομέα/διεύθυνση.

#### 14.



ID: Ένα 16-μπιτο αναγνωριστικό που εκχωρείται από το πρόγραμμα που γεννά οποιουδήποτε είδους ερωτήσεις. Το αναγνωριστικό αυτό αντιγράφεται στην αντίστοιχη απάντηση και μπορεί να χρησιμοποιηθεί από τον αιτούντα για να ταιριάξει τις απαντήσεις με τα εκκρεμή ερωτήματα.

QR: Ένας τομέας με 1 bit που συγκεκριμενοποιεί αν το μήνυμα είναι ερώτηση (0) ή απάντηση (1).

OPCODE: Ένας τομέας με 4 bit που συγκεκριμενοποιεί το είδος της ερώτησης στο μήνυμα (πχ standard query -> 0).

AA - Authoritative Answer: 1 bit που είναι χρήσιμο μόνο στις απαντήσεις, και δηλώνει ότι ο responding name server είναι εξουσιοδοτημένος για το domain name στο κομμάτι της ερώτησης.

TC – TurnCation: καθορίζει ότι αυτό το μήνυμα έχει περικοπεί.

RD – Recursion Desired: bit που κατευθύνει τον εξυπηρετητή να αναζητήσει την ερώτηση αναδρομικά.

RA – Recursion Available: αυτό το bit γίνεται set ή clear σε μία απάντηση, και δείχνει αν η αναδρομική υποστήριξη ερώτησης είναι διαθέσιμη στο name server.

Z: κατοχυρωμένο για μελλοντική χρήση.

RCODE – Response Code: τομέας 4 bit τίθεται ως κομμάτι των απαντήσεων. Οι τιμές του έχουν την εξής αντιστοίχιση.

0 -> κανένα σφάλμα

1 -> format error: ο name server δεν κατάφερε να ερμηνεύσει το ερώτημα

2 -> server failure: ο name server δεν κατάφερε να επεξεργαστεί το ερώτημα εξαιτίας ενός προβλήματος του ιδίου.

3 -> name error: έχει σημασία μόνο στις απαντήσεις από έναν authoritative name server, αυτός ο κώδικας σηματοδοτεί ότι το domain name που αναφέρθηκε στο ερώτημα δεν υπάρχει.

4 -> not implemented: ο name server δεν υποστηρίζει το ζητούμενο είδος ερωτήματος.

5 -> refused: ο name server αρνείται να εκτελέσει τη συγκεκριμένη διεργασία για λόγους πολιτικής (policy reasons).

Κι ακολουθούν τα data.

## 15.

Πακέτο:

48 F8 B3 26 DF 49 BA BA BA BA BA BA 08 00 45 00 00 38 66 BD 00 00 80 11

02 0C C0 A8 01 34 08 08 08 D5 39 00 35 00 24 44 8F 00 03 01 00 00 01 00 00

00 00 00 00 06 67 6F 6F 67 6C 65 03 63 6F 6D 00 00 01 00 01

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
48	F8	B3	26	DF	49	BA	BA	BA	BA	BA	BA	BA	08	00	45
00	00	38	66	BD	00	00	80	11	02	0C	C0	A8	01	34	08
08	08	D5	39	00	35	00	24	44	8F	00	03	01	00	00	01
00	00	00	00	00	00	06	67	6F	6F	67	6C	65	03	63	6F
6D	00	00	01	00	01										

ba:ba:ba:ba:ba:ba → Cisco-Li\_26:df:49 0xba08 Ethernet II

1 πρωτόκολλο στο πακέτο:

Ethernet

## 16.

Πακέτο:

BA BA BA BA BA BA 48 F8 B3 26 DF 49 08 00 45 08 00 E8 B2 EF 00 00 37 11 FE 21 08 08 08 08  
C0 A8 01 34 00 35 D5 39 00 D4 28 A2 00 03 81 80 00 01 00 0B 00 00 00 00 06 67 6F 6F 67 6C  
65 03 63 6F 6D 00 00 01 00 01 C0 0C 00 01 00 01 00 00 00 04 00 04 4A 7D EC 23 C0 0C 00 01  
00 01 00 00 00 04 00 04 4A 7D EC 25 C0 0C 00 01 00 01 00 00 00 04 00 04 4A 7D EC 27 C0 0C  
00 01 00 01 00 00 00 04 00 04 4A 7D EC 20 C0 0C 00 01 00 01 00 00 00 04 00 04 4A 7D EC 28  
C0 0C 00 01 00 01 00 00 00 04 00 04 4A 7D EC 21 C0 0C 00 01 00 01 00 00 00 04 04 4A 7D EC  
29 C0 0C 00 01 00 01 00 00 00 04 00 04 4A 7D EC 22 C0 0C 00 01 00 01 00 00 00 04 00 04 4A  
7D EC 24 C0 0C 00 01 00 01 00 00 00 04 00 04 4A 7D EC 2E C0 0C 00 01 00 01 00 00 00 04 00  
04 4A 7D EC 26

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
BA	BA	BA	BA	BA	BA	48	F8	B3	26	DF	49	08	00	45	08
00	E8	B2	EF	00	00	37	11	FE	21	08	08	08	08	C0	A8
01	34	00	35	D5	39	00	D4	28	A2	00	03	81	80	00	01
00	0B	00	00	00	00	06	67	6F	6F	67	6C	65	03	63	6F
6D	00	00	01	00	01	C0	0C	00	01	00	01	00	00	00	04
00	04	4A	7D	EC	23	C0	0C	00	01	00	01	00	00	00	04
00	04	4A	7D	EC	25	C0	0C	00	01	00	01	00	00	00	04
00	04	4A	7D	EC	27	C0	0C	00	01	00	01	00	00	00	04
00	04	4A	7D	EC	20	C0	0C	00	01	00	01	00	00	00	04
00	04	4A	7D	EC	28	C0	0C	00	01	00	01	00	00	00	04
00	04	4A	7D	EC	21	C0	0C	00	01	00	01	00	00	00	04
04	4A	7D	EC	29	C0	0C	00	01	00	01	00	00	00	04	00
04	4A	7D	EC	22	C0	0C	00	01	00	01	00	00	00	04	00
04	4A	7D	EC	24	C0	0C	00	01	00	01	00	00	00	04	00
04	4A	7D	EC	2E	C0	0C	00	01	00	01	00	00	00	04	00
04	4A	7D	EC	26											

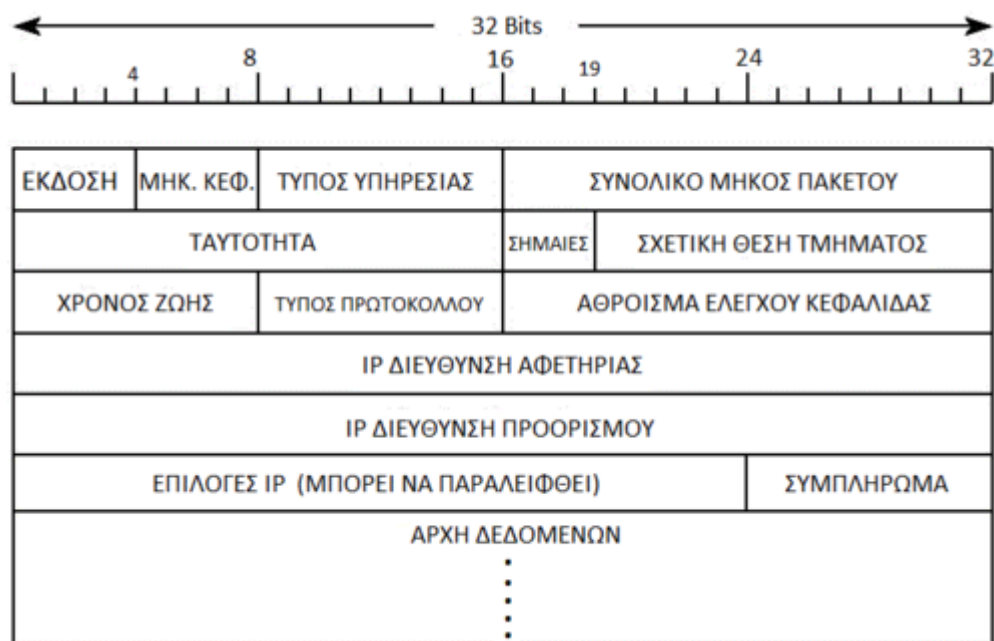
8.8.8.8 → 192.168.1.52 DNS Standard query response 0x0003 A google.com A 74.125.236.35  
A 74.125.236.37 A 74.125.236.39 A 74.125.236.32 A 74.125.236.40 A 74.125.236.33 A  
125.236.41.192

4 πρωτόκολλα στο πακέτο:

- a. Ethernet
- b. IPv4
- c. UDP
- d. DNS

## Β' ΜΕΡΟΣ

1.



**Έκδοση:** η τρέχουσα έκδοση IP

**Μήκος Κεφαλαίου:** ο αριθμός 32-bit λέξεων που αποτελούν την επικεφαλίδα

**Τύπος Υπηρεσίας (Differentiated Services Code Point – DSCP):** ορίζει ένα σεν από κλάσεις υπηρεσίας.

**Συνολικό Μήκος Πακέτου:** μετρίεται σε bytes. Είναι το συνολικό μέγεθος του πακέτου (επικεφαλίδα + δεδομένα)

**Ταυτότητα:** Ένας αριθμός 16-bit που μαζί με τη διεύθυνση του αποστολέα προσδιορίζει μοναδικά κάθε πακέτο.

**Σημείες:** : Είναι μια ακολουθία από τρία bits (R, DF, MF), το R δε χρησιμοποιείται, το DF καθορίζει αν θα κατακερματιστεί αυτό το διάγραμμα και το MF αν ακολουθούν κι άλλα τμήματα του κατακερματισμένου διαγράμματος.

**Σχετική Θέση Τμήματος:** Μετρίεται σε πολλαπλάσια των 8 byte (64-bit). Το πεδίο διαθέτει 13bits άρα η μέγιστη τιμή του είναι  $2^{13}=8.192$ . Πρόκειται για έναν αριθμό που προσδιορίζει τη θέση του πακέτου μέσα στο αρχικό διάγραμμα (εφόσον έγινε fragmentation). Η τιμή του τίθεται από τον δρομολογητή που έκανε τον κατακερματισμό του και είναι η απόσταση του πακέτου από την αρχή του αρχικού διαγράμματος.

**Χρόνος Ζωής:** : Προσδιορίζει το χρόνο ζωής του διαγράμματος. Μετρίεται σε αριθμό αλμάτων μέσω δρομολογητών. Η αρχική του τιμή τίθεται από το πρωτόκολλο ανωτέρου επιπέδου που δημιουργεί το διάγραμμα. Η μέγιστη δυνατή αρχική τιμή είναι 255. Σε κάθε



διέλευση του πακέτου από δρομολογητή ο αριθμός μειώνεται κατά ένα. Όταν γίνει 0 το διάγραμμα καταστρέφεται γιατί θεωρείται ότι έχει μπει σε μια διαδικασία ατέρμονου ταξιδιού μέσα στο δίκτυο χωρίς να βρίσκει τον προορισμό του.

**Πρωτόκολλο:** : Δείχνει ποιο είναι το πρωτόκολλο επιπέδου μεταφοράς που χρησιμοποιείται.

**Άθροισμα Ελέγχου Κεφαλίδας:** Χρησιμοποιείται για τον έλεγχο της ορθής μετάδοσης της επικεφαλίδας κι όχι ολόκληρου του πακέτου. Στην πραγματικότητα αναγνωρίζει τα σφάλματα που προέρχονται κατά την επεξεργασία των πακέτων μέσα στις συσκευές ενός δικτύου όπου δεν προστατεύονται από το έλεγχο σφαλμάτων. Υπολογίζεται ως το συμπλήρωμα ως προς 1 , του αθροίσματος των ως προς 1 συμπληρωμάτων όλων των 16-bit λέξεων της επικεφαλίδας. Αν ο δέκτης διαπιστώσει κάποια ασυμφωνία της επικεφαλίδας με το άθροισμα ελέγχου κεφαλίδας απορρίπτει το διάγραμμα.

**IP Διεύθυνση Αφετηρίας:** : Η IP διεύθυνση του αρχικού αποστολέα του πακέτου.

**IP Διεύθυνση Προορισμού:** : Η IP διεύθυνση του τελικού παραλήπτη του πακέτου.

**Επιλογές IP:** Η χρήση του αφορά σε διαγνωστικούς και διαχειριστικούς ελέγχους όπως η καταγραφή της διαδρομής, κατευθυνόμενη δρομολόγηση, ασφάλεια κ.α. Αν δεν χρησιμοποιείται ολόκληρο συμπληρώνεται με μηδενικά.

**00 A0 92 48 72 45 00 00 0C 05 C3 58 08 00 4 5 00 00 29 DB FB 40 00 FE 06 7D CB 81 6E 1E 1A  
81 6E 02 11 0203 00 50 6A 86 7B 57 B6 B6 B0 20 50 10 24 00 17 c4 00 00 02 54 41 4D 49 4C  
D7 87 6C A4**

**1.1** Διεύθυνση Αφετηρίας: 129.110.30.26

Διεύθυνση Προορισμού: 129.110.2.17

**1.2** 20 bytes

**1.3**

**1.4** TCP θύρα αποστολέα: 515

TCP θύρα δέκτη: 80

**1.5** Header Checksum: 0x7dcb

### 2.α.1.

```
C:\Users\asus m513ia>tracert -d 83.212.8.210
Tracing route to 83.212.8.210 over a maximum of 30 hops

  1    5 ms    2 ms    2 ms  192.168.2.1
  2   12 ms   13 ms   12 ms  62.38.0.170
  3   15 ms  109 ms   11 ms  62.38.97.93
  4   14 ms   90 ms   12 ms  62.38.37.89
  5   13 ms   99 ms   12 ms  62.38.97.150
  6   13 ms  102 ms   97 ms  62.38.93.221
  7    *      *      *    Request timed out.
  8    *      *      *    Request timed out.
  9    *      *      *    Request timed out.
 10   *      *      *    Request timed out.
 11   *      *      *    Request timed out.
 12   *      *      *    Request timed out.
 13   *      *      *    Request timed out.
 14   *      *      *    Request timed out.
 15   *      *      *    Request timed out.
 16   *      *      *    Request timed out.
 17   *      *      *    Request timed out.
 18   *      *      *    Request timed out.
 19   *      *      *    Request timed out.
 20   *      *      *    Request timed out.
 21   *      *      *    Request timed out.
 22   *      *      *    Request timed out.
 23   *      *      *    Request timed out.
 24   *      *      *    Request timed out.
 25   *      *      *    Request timed out.
 26   *      *      *    Request timed out.
 27   *      *      *    Request timed out.
 28   *      *      *    Request timed out.
 29   *      *      *    Request timed out.
 30   *      *      *    Request timed out.

Trace complete.
```

Εκτελούμε την εντολή `tracert -d 83.212.8.210` και λαμβάνουμε αυτό το αποτέλεσμα.

```
Command Prompt - tracert 83.212.8.210
Microsoft Windows [Version 10.0.19042.928]
(c) Microsoft Corporation. All rights reserved.

C:\Users\asus m513ia>tracert 83.212.8.210
Tracing route to 83.212.8.210 over a maximum of 30 hops

  1    2 ms    2 ms    2 ms  csp1.zte.com.cn [192.168.2.1]
  2   11 ms   10 ms   11 ms  loopback2004.med01.dsl.hol.gr [62.38.0.170]
  3   18 ms   11 ms   12 ms  tengigaeth00-03-00-09.med00.ccr.hol.gr [62.38.97.93]
  4   11 ms   11 ms   13 ms  62.38.37.89
  5   11 ms   12 ms   11 ms  62.38.97.150
  6   12 ms   12 ms   12 ms  62.38.93.221
  7    *      *      *    Request timed out.
  8    *      *      *    Request timed out.
  9    *      *      *    Request timed out.
 10   *      *      *    Request timed out.
 11   *      *      *    Request timed out.
```

Ξαναεκτελούμε την εντολή αυτή τη φορά χωρίς το `-d` αυτή τη φορά και το αποτέλεσμα που λαμβάνουμε βρίσκεται στη δεύτερη εικόνα.

Παρατηρούμε ότι στην πρώτη περίπτωση η επιπλέον παράμετρος βοηθάει στο να μην εμφανίζονται τα ονόματα των κεντρικών υπολογιστών, αποκρύπτει ουσιαστικά μερικές πληροφορίες κάνοντας πιο απλό το αποτέλεσμα δίνοντας μας μόνο τις IP διευθύνσεις.

### 2.α.2. Βήματα:

1. Ανοίγουμε το wireshark.

2. Πατάμε `ctrl+k` και στο πεδίο capture filter γράφουμε `ether host + MAC address μας`.

\* Τη MAC address μπορούμε να τη βρούμε ανοίγοντας το command prompt και εκτελώντας την εντολή `getmac -v`.

### 2.α.3.

icmp						
No.	Time	Source	Destination	Protocol	Length	Info
277	27.628267	192.168.2.5	83.212.8.210	ICMP	106	Echo (ping) request id=0x0001, seq=537/6402, ttl=1 (no response found!)
278	28.567881	192.168.2.1	192.168.2.5	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
279	28.570199	192.168.2.5	83.212.8.210	ICMP	106	Echo (ping) request id=0x0001, seq=538/6658, ttl=1 (no response found!)
280	28.674584	192.168.2.1	192.168.2.5	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
281	28.676124	192.168.2.5	83.212.8.210	ICMP	106	Echo (ping) request id=0x0001, seq=539/6914, ttl=1 (no response found!)
282	28.695349	192.168.2.1	192.168.2.5	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
283	29.693168	192.168.2.5	83.212.8.210	ICMP	106	Echo (ping) request id=0x0001, seq=540/7170, ttl=2 (no response found!)
284	29.705196	62.38.0.170	192.168.2.5	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
285	29.706340	192.168.2.5	83.212.8.210	ICMP	106	Echo (ping) request id=0x0001, seq=541/7426, ttl=2 (no response found!)
286	29.801675	62.38.0.170	192.168.2.5	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
287	29.804125	192.168.2.5	83.212.8.210	ICMP	106	Echo (ping) request id=0x0001, seq=542/7682, ttl=2 (no response found!)
288	29.816004	62.38.0.170	192.168.2.5	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
289	30.814385	192.168.2.5	83.212.8.210	ICMP	106	Echo (ping) request id=0x0001, seq=543/7938, ttl=3 (no response found!)
290	30.827314	62.38.97.93	192.168.2.5	ICMP	182	Time-to-live exceeded (Time to live exceeded in transit)
291	30.828532	192.168.2.5	83.212.8.210	ICMP	106	Echo (ping) request id=0x0001, seq=544/8194, ttl=3 (no response found!)
292	30.841117	62.38.97.93	192.168.2.5	ICMP	182	Time-to-live exceeded (Time to live exceeded in transit)
293	30.845579	192.168.2.5	83.212.8.210	ICMP	106	Echo (ping) request id=0x0001, seq=545/8450, ttl=3 (no response found!)
294	30.858502	62.38.97.93	192.168.2.5	ICMP	182	Time-to-live exceeded (Time to live exceeded in transit)

> Frame 277: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface \Device\NPF\_{DA03ABA5-235C-49E7-8311-79347392AD84}, id 0

> Ethernet II, Src: AzureWav\_cf:46:39 (70:66:55:cf:46:39), Dst: zte\_ef:67:dd (44:fb:5a:ef:67:dd)

> Internet Protocol Version 4, Src: 192.168.2.5, Dst: 83.212.8.210

> Internet Control Message Protocol

### 2.α.4. Διεύθυνση του υπολογιστή:

0100 .... = Version: 4	
.... 0101 = Header Length: 20 bytes (5)	
> Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)	
Total Length: 120	
Identification: 0x7882 (30850)	
> Flags: 0x00	
Fragment Offset: 0	
Time to Live: 64	
Protocol: ICMP (1)	
Header Checksum: 0x7bec [validation disabled]	
[Header checksum status: Unverified]	
Source Address: 192.168.2.1	
Destination Address: 192.168.2.5	
> Internet Control Message Protocol	

0010	00 78 78 82 00 00 40 01	7b ec c0 a8 02 01	c0 a8	..xx...@. { . . . .
0020	02 05 0b 00 f4 ff 00 00	00 00 45 00 00 5c 2e 3b		.....E.. \.;
0030	00 00 01 01 6c 13 c0 a8	02 05 53 d4 08 d2 08 00		....1... .S....
0040	f5 5b 00 01 02 a3 00 00	00 00 00 00 00 00 00 00		...[.....
0050	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00		.....
0060	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00		.....
0070	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00		.....
0080	00 00 00 00 00 00 00 00			.....

Source Address (ip.src), 4 bytes

### 2.α.5.

> Time to Live: 1	
Protocol: ICMP (1)	
Header Checksum: 0x6c13 [validation disabled]	
[Header checksum status: Unverified]	
Source Address: 192.168.2.5	
Destination Address: 83.212.8.210	
> Internet Control Message Protocol	

0000	44 fb 5a ef 67 dd 70 66	55 cf 46 39 08 00 45 00	D.Z.g.pf U.F9..E.
0010	00 5c 2e 3b 00 00 01 01	6c 13 c0 a8 02 05 53 d4	.. \. ; . . 1 . . . . S .
0020	08 d2 08 00 f5 5b 00 01	02 a3 00 00 00 00 00 00	.....[. ....
0030	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	.....
0040	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	.....
0050	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	.....
0060	00 00 00 00 00 00 00 00	00 00	.....

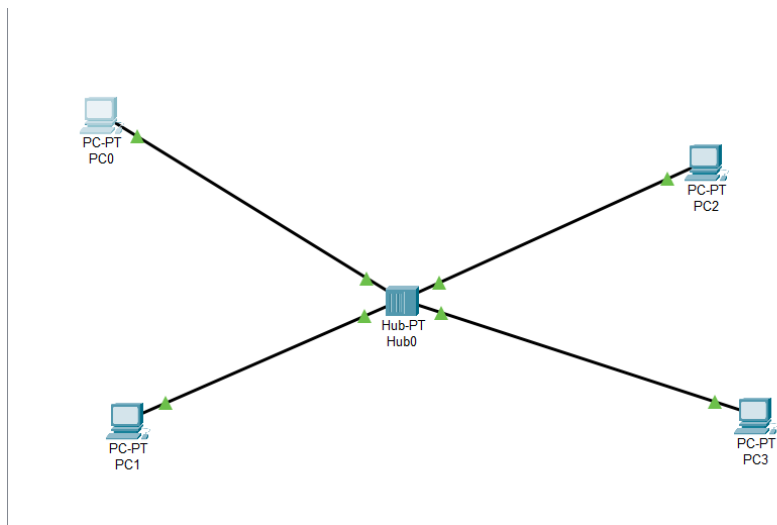
**2.α.6.** 20 bytes.

**2.α.7.** 64 bytes.

**2.α.8.** Απ' το πακέτο γνωρίζουμε ότι το μέγεθος του είναι 92 bytes. Και γνωρίζουμε ότι:

Μέγεθος πακέτου = επικεφαλίδα + δεδομένα

### Γ' ΜΕΡΟΣ:



**11.1** Στο τοπικό interface του PC0.

Κάνοντας ping την IP διεύθυνση του PC0 αναμένουμε αποτέλεσμα για το αν οι ρυθμίσεις του δικτύου είναι σωστές.

PC0

```
Physical  Config  Desktop  Programming  Attributes
Command Prompt

Packet Tracer PC Command Line 1.0
C:\>Ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=19ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time=7ms TTL=128
Reply from 192.168.1.1: bytes=32 time=8ms TTL=128

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 19ms, Average = 8ms

C:\>
```

## 11.2 Ναι

Λαμβάνουμε αποτέλεσμα για τη δεύτερη διεύθυνση που μας δείχνει ότι υπάρχει σύνδεση μεταξύ των υπολογιστών και άμεση διαθεσιμότητα.

```
C:\> Ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

## 11.3 Ναι

Η ίδια εντολή εκτελείται και παρέχει τα ίδια αποτελέσματα.

## Δ' ΜΕΡΟΣ:

1. Telnet 10.10.10.2 -> είσοδος στο S1 (user EXEC mode)
2. S1>en -> privileged EXEC mode
3. S1#copy running-config startup-config -> αποθήκευση τρέχουσας κατάστασης
4. S1#show running-config -> εμφάνισης τρέχουσας κατάστασης -> ο κωδικός είναι σε μορφή κειμένου (φανερός)
5. S1#conf ter -> είσοδος στο configuration terminal
6. S1(config)#service password-encryption -> ενεργοποίηση λειτουργίας κρυπτογράφησης κωδικού
7. S1(config)#exit -> έξοδος από configuration terminal
8. S1#show running-config
9. S1#copy running-config startup-config
10. S1#conf ter
11. S1(config)#ip domain-name netacad.pda -> διαμόρφωση ονόματος τομέα
12. S1(config)#crypt key generate rsa -> δημιουργία κλειδίων ασφαλείας

13. S1(config)#username up1067409 password 1067409 -> δημιουργία του user up1067409
14. S1(config)#username administrator secret Cisco -> δημιουργία dmin
15. S1(config)#line vty 0 15
16. S1(config)#login local -> απαιτείται username και password για το login
17. S1(config)#transport input ssh -> επιτρέπεται μόνο SSH για απομακρυσμένη πρόσβαση
18. S1(config)#exit
19. S1#exit
20. S1>exit
21. Telnet 10.10.10.2 -> αποτυχία
22. SSH -l administrator 10.10.10.2
23. S1> enable
24. S1# copy running-config startup-config

Μητροπούλου Αικατερίνα AM: 1067409