

Στοιχεία Φοιτητή: Κωστορρίζος Δημήτριος

ΑΜ: 1054419

Έτος Σπουδών: 4ο

Απαντήσεις για το μέρος Α

Αποτέλεσμα Εντολής: nslookup www.ceid.upatras.gr

```
C:\Users\jimak>nslookup www.ceid.upatras.gr
Server:  speedport-entry-2i.ote.gr
Address:  fe80::1

Non-authoritative answer:
Name:    web.ceid.upatras.gr
Address: 150.140.141.173
Aliases: www.ceid.upatras.gr
```

Αποτέλεσμα Εντολής: ipconfig /all

```
C:\Users\jimak>ipconfig /all
```

Windows IP Configuration

```
Host Name . . . . . : LAPTOP-8LOKK1K1
Primary Dns Suffix . . . . . :
Node Type . . . . . : Mixed
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
```

Ethernet adapter Ethernet:

```
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : Realtek PCIe GbE Family Controller
Physical Address. . . . . : 50-7B-9D-94-61-9E
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
```

Wireless LAN adapter Τοπική σύνδεση* 2:

```
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #4
Physical Address. . . . . : E0-94-67-BD-0B-C4
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
```

Wireless LAN adapter Τοπική σύνδεση* 4:

```
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #5
Physical Address. . . . . : E2-94-67-BD-0B-C3
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
```

Ethernet adapter Ethernet 5:

```
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : TAP-Windows Adapter V9
Physical Address. . . . . : 00-FF-2C-81-32-52
DHCP Enabled. . . . . : Yes
```

Αποτέλεσμα Εντολής: ipconfig /displaydns

Windows IP Configuration

cm3-ams1.cm.steampowered.com

Record Name : cm3-ams1.cm.steampowered.com
Record Type : 1
Time To Live : 7329
Data Length : 4
Section : Answer
A (Host) Record . . . : 155.133.248.36

cm03-fra.cm.steampowered.com

Record Name : CM03-FRA.cm.steampowered.com
Record Type : 1
Time To Live : 7257
Data Length : 4
Section : Answer
A (Host) Record . . . : 162.254.197.42

mail.ceid.upatras.gr

Record Name : mail.ceid.upatras.gr
Record Type : 1
Time To Live : 8815
Data Length : 4
Section : Answer
A (Host) Record . . . : 150.140.141.143

cm1-vie1.cm.steampowered.com

Record Name : cm1-vie1.cm.steampowered.com
Record Type : 1

Time To Live : 7358
Data Length : 4
Section : Answer
A (Host) Record . . . : 146.66.155.100

eu-west595.discord.media

Record Name : eu-west595.discord.media
Record Type : 1
Time To Live : 150
Data Length : 4
Section : Answer
A (Host) Record . . . : 162.159.130.235

Record Name : eu-west595.discord.media
Record Type : 1
Time To Live : 150
Data Length : 4
Section : Answer
A (Host) Record . . . : 162.159.137.234

Record Name : eu-west595.discord.media
Record Type : 1
Time To Live : 150
Data Length : 4
Section : Answer
A (Host) Record . . . : 162.159.129.235

Record Name : eu-west595.discord.media
Record Type : 1
Time To Live : 150
Data Length : 4
Section : Answer
A (Host) Record . . . : 162.159.138.234

Record Name : eu-west595.discord.media
Record Type : 1
Time To Live : 150
Data Length : 4
Section : Answer
A (Host) Record . . . : 162.159.128.235

cm2-fra1.cm.steampowered.com

Record Name : cm2-fra1.cm.steampowered.com
Record Type : 1
Time To Live : 7313
Data Length : 4
Section : Answer
A (Host) Record . . . : 162.254.197.180

clientservices.googleapis.com

Record Name : clientservices.googleapis.com
Record Type : 28
Time To Live : 103
Data Length : 16
Section : Answer
AAAA Record : 2a00:1450:4001:808::2003

clientservices.googleapis.com

Record Name : clientservices.googleapis.com
Record Type : 1
Time To Live : 103
Data Length : 4
Section : Answer
A (Host) Record . . . : 172.217.23.131

cm4-sto1.cm.steampowered.com

Record Name : cm4-sto1.cm.steampowered.com
Record Type : 1
Time To Live : 7170
Data Length : 4
Section : Answer
A (Host) Record . . . : 162.254.198.133

cm1-ams1.cm.steampowered.com

Record Name : cm1-ams1.cm.steampowered.com
Record Type : 1
Time To Live : 7432
Data Length : 4
Section : Answer
A (Host) Record . . . : 155.133.248.34

geo.prod.do.dsp.mp.microsoft.com

Record Name : geo.prod.do.dsp.mp.microsoft.com
Record Type : 1
Time To Live : 1056
Data Length : 4
Section : Answer
A (Host) Record . . . : 13.78.187.58

cm4-fra1.cm.steampowered.com

Record Name : cm4-fra1.cm.steampowered.com
Record Type : 1
Time To Live : 2533
Data Length : 4
Section : Answer
A (Host) Record . . . : 162.254.197.181

crash.steampowered.com

Record Name : crash.steampowered.com
Record Type : 1
Time To Live : 8164
Data Length : 4
Section : Answer
A (Host) Record . . . : 208.64.203.173

Record Name : crash.steampowered.com
Record Type : 1
Time To Live : 8164
Data Length : 4
Section : Answer
A (Host) Record . . . : 208.64.203.140

mus.lenovo.com

Record Name : mus.lenovo.com
Record Type : 1
Time To Live : 3645
Data Length : 4
Section : Answer
A (Host) Record . . . : 54.215.241.186

cm1-sto1.cm.steampowered.com

Record Name : cm1-sto1.cm.steampowered.com
Record Type : 1
Time To Live : 7278
Data Length : 4
Section : Answer
A (Host) Record . . . : 162.254.198.130

clients4.google.com

Record Name : clients4.google.com
Record Type : 5
Time To Live : 97
Data Length : 8
Section : Answer
CNAME Record : clients.l.google.com

Record Name : clients.l.google.com
Record Type : 28
Time To Live : 97
Data Length : 16
Section : Answer
AAAA Record : 2a00:1450:4001:800::200e

clients4.google.com

Record Name : clients4.google.com
Record Type : 5
Time To Live : 98
Data Length : 8
Section : Answer
CNAME Record : clients.l.google.com

Record Name : clients.l.google.com
Record Type : 1
Time To Live : 98
Data Length : 4
Section : Answer
A (Host) Record : 172.217.18.110

cm1-par1.cm.steampowered.com

Record Name : cm1-par1.cm.steampowered.com


```

cm1-par1.cm.steampowered.com
-----
Record Name . . . . . : cm1-par1.cm.steampowered.com
Record Type . . . . . : 1
Time To Live . . . . . : 7692
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 185.25.182.76

cm2-par1.cm.steampowered.com
-----
Record Name . . . . . : cm2-par1.cm.steampowered.com
Record Type . . . . . : 1
Time To Live . . . . . : 7694
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 185.25.182.77

cm4-ams1.cm.steampowered.com
-----
Record Name . . . . . : cm4-ams1.cm.steampowered.com
Record Type . . . . . : 1
Time To Live . . . . . : 7200
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 155.133.248.37

```

Αποτέλεσμα Εντολής: ipconfig /flushdns

```

C:\Users\jimak>ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

```

1. Τα πακέτα DNS που ανταλλάχθηκαν είναι:

No.	Time	Source	Destination	Protocol	Length	Info
54	2.281360	192.168.1.10	193.92.150.3	DNS	72	Standard query
0x2be8 NS www.ietf.org						

No.	Time	Source	Destination	Protocol	Length	Info
56	2.336997	193.92.150.3	192.168.1.10	DNS	175	Standard query response 0x2be8 NS www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net SOA ns1.cloudflare.net

dns						
No.	Time	Source	Destination	Protocol	Length	Info
112	3.167198	192.168.1.10	193.92.150.3	DNS	72	Standard query 0x9388 NS www.ietf.org
118	3.221571	193.92.150.3	192.168.1.10	DNS	175	Standard query response 0x9388

2. Τα πεδία του μηνύματος είναι ως εξής:

- Time: Ο χρόνος ζωής του πακέτου
- Source: Η διεύθυνση IP του αποστολέα
- Destination: Η διεύθυνση IP του παραλήπτη
- Protocol: Το πρωτόκολλο που χρησιμοποιήθηκε
- Length: Το μήκος του πακέτου
- Info: Πληροφορίες για το πακέτο

Το είδος πρωτοκόλλου που χρησιμοποιήθηκε για το πακέτο είναι TCP.

3. Η θύρα προορισμού για το μήνυμα της ερώτησης DNS είναι η θύρα 53.

4. Η θύρα προέλευσης για το μήνυμα της απόκρισης DNS είναι η θύρα 53.

5. Το μήνυμα ερώτησης DNS εμφανίζεται στην διεύθυνση 192.168.1.6, η οποία ταυτίζεται με την IPv4 διεύθυνση του τοπικού διακομιστή DNS.

6. Το ερώτημα έχει "τύπο" DNS. Η απάντηση ωστόσο έχει "τύπο" CNAME. Το ερώτημα δεν περιέχει οποιεσδήποτε "απαντήσεις".

7. Το μήνυμα απόκρισης DNS περιέχει 2 απαντήσεις. Η κάθε απάντηση περιέχει τα εξής πεδία

- Όνομα
- Τύπος

- Κλάση
- Χρόνος Ζωής
- Μήκος Δεδομένων
- CNAME

8. Η διεύθυνση IP του πακέτου SYN αντιστοιχεί στην πρώτη διεύθυνση του μηνύματος απόκρισης DNS, πιο συγκεκριμένα η διεύθυνση IP είναι η 4.31.198.44.

9. Η θύρα προορισμού για το μήνυμα της ερώτησης DNS, όπως και η θύρα προέλευσης για το μήνυμα της απόκρισης DNS, είναι η θύρα 53.

12	1.144125	192.168.1.68	192.168.1.254	DNS	79 Standard ...
13	1.186310	192.168.1.254	192.168.1.68	DNS	141 Standard ...
17	1.308568	192.168.1.68	150.140.129.7	TCP	62 60555 → 1...
1	0.000000	46.177.71.186	192.168.1.68	UDP	132 58342 → 6...
2	0.000282	192.168.1.68	46.177.71.186	UDP	132 63283 → 5...
3	0.070747	46.177.71.186	192.168.1.68	UDP	132 58342 → 6...

> Frame 12: 79 bytes on wire (632 bits), 79 bytes captured (632 bits) on interface \Device\NPF_
 > Ethernet II, Src: Dell_04:7b:66 (84:7b:eb:04:7b:66), Dst: ThomsonT_ba:9f:ea (08:76:ff:ba:9f:e
 > Internet Protocol Version 4, Src: 192.168.1.68, Dst: 192.168.1.254
 > User Datagram Protocol, Src Port: 61861, Dst Port: 53
 > Domain Name System (query)

10. Το μήνυμα ερώτησης DNS εμφανίζεται στην διεύθυνση IP 192.168.1.254. Η διεύθυνση IP του προεπιλεγμένου διακομιστή DNS είναι η 193.92.3.110, οπότε οι δύο διευθύνσεις δεν ταυτίζονται.

11. Το ερώτημα DNS έχει τύπο AAAAA. Το ερώτημα περιέχει τις συγκεκριμένες “απαντήσεις”, από www.ceid.upatras.gr και από το authoritative nameservers.

12. Το μήνυμα απόκρισης DNS περιέχει 2 “απαντήσεις”. Οι απαντήσεις φαίνονται παρακάτω:

```

  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: 79035 (21 hours, 57 minutes, 15 seconds)
    Data length: 6
    CNAME: web.ceid.upatras.gr
  Authoritative nameservers
  ceid.upatras.gr: type SOA, class IN, mname NIC.upatras.gr
    Name: ceid.upatras.gr
    Type: SOA (Start Of a zone of Authority) (6)
    Class: IN (0x0001)
    Time to live: 77603 (21 hours, 33 minutes, 23 seconds)
    Data length: 32
    Primary name server: NIC.upatras.gr
    Responsible authority's mailbox: noc.upatras.gr
    Serial Number: 97759
    Refresh Interval: 21600 (6 hours)
    Retry Interval: 3600 (1 hour)
    Expire limit: 604800 (7 days)
    Minimum TTL: 86400 (1 day)

```

13. Recursive Resolver:

Ένα DNS (recursive resolver), έχει σχεδιαστεί για τη λήψη ερωτημάτων DNS και είναι το πρώτο βήμα σε ένα ερώτημα DNS. Ο αναδρομικός διακομιστής είναι σαν μεσάζων μεταξύ ενός πελάτη και ενός διακομιστή ονομάτων DNS. Όταν λαμβάνει ένα ερώτημα DNS, θα κοιτάξει πρώτα στην κρυφή μνήμη του για την απάντηση. Εάν δεν έχει την απάντηση στην κρυφή μνήμη του, θα στείλει το αίτημα σε έναν διακομιστή ονόματος ρίζας(root), έπειτα σε έναν διακομιστή ονομάτων TLD και τελικά θα ανακτήσει την απάντηση από τον επίσημο διακομιστή ονομάτων για το όνομα τομέα. Στη συνέχεια, η απάντηση θα επιστραφεί στον πελάτη διαδικτύου. Κατά τη διάρκεια αυτής της διαδικασίας, το recursive resolver θα αποθηκεύσει προσωρινά την απάντηση για το μήκος του TTL. Εάν ληφθεί ξανά το ίδιο ερώτημα, η διαδικασία υποβολής ερωτημάτων για τον εξουσιοδοτημένο διακομιστή ονόματος θα παραλειφθεί και θα επιστραφεί η απάντηση από την προσωρινή μνήμη.

Root Nameserver:

Ο DNS Root Server εξάγει τον τομέα του ανώτατου επιπέδου (TLD) από το ερώτημα του χρήστη. Ο διακομιστής root names αποκρίνεται κατευθύνοντας το recursive resolver σε έναν διακομιστή ονομάτων TLD, με βάση την επέκταση αυτού του τομέα (.com, .gr, .org κ.λπ.).

TLD Nameserver:

Ένας διακομιστής ονομάτων TLD διατηρεί πληροφορίες για όλα τα ονόματα τομέα που μοιράζονται μια κοινή επέκταση τομέα, όπως .com, .gr, .org κ.λπ.

Authoritative Nameservers:

Ένας εξουσιοδοτημένος διακομιστής ονόματος (Authoritative name server) παρέχει πρωτότυπες και οριστικές απαντήσεις σε ερωτήματα DNS. Δεν παρέχει προσωρινά

αποθηκευμένες απαντήσεις που ελήφθησαν από άλλο διακομιστή ονομάτων, αντίθετα, αποθηκεύει τις εγγραφές DNS στο σύστημά του και επιστρέφει μόνο απαντήσεις σε ερωτήματα σχετικά με ονόματα τομέα που είναι αποθηκευμένα στο σύστημα διαμόρφωσής του.

14. Τα πακέτα DNS έχουν:

Header

Question, η ερώτηση για τον name server

Answer, η απάντηση στην ερώτηση προς τον server

Authority

Additional

Η κεφαλίδα (**header**) περιγράφει τον τύπο του πακέτου και ποια πεδία περιέχονται στο πακέτο. Ακολουθώντας την κεφαλίδα είναι μια σειρά από ερωτήσεις, απαντήσεις, αρχεία εξουσιοδότησης και πρόσθετες εγγραφές.

Τα headers έχουν:

ID: Αναγνωριστικό 16-bit που εκχωρείται από το πρόγραμμα που δημιουργεί οποιοδήποτε είδος ερωτήματος. Αυτό το αναγνωριστικό αντιγράφει την αντίστοιχη απάντηση και μπορεί να χρησιμοποιηθεί από τον αιτούντα για να αντιστοιχίσει απαντήσεις σε εκκρεμή ερωτήματα

QR: Ένα πεδίο bit που καθορίζει εάν αυτό το μήνυμα είναι ερώτημα (0) ή απόκριση (1)

OPCODE: Ένα πεδίο τεσσάρων bit που καθορίζει το είδος του ερωτήματος σε αυτό το μήνυμα

AA: Μη εξουσιοδοτημένη απάντηση - αυτό το bit έχει νόημα μόνο στις απαντήσεις και καθορίζει ότι ο διακομιστής ονομάτων αποκρίσεων είναι μια αρχή για το εν λόγω όνομα τομέα.

TC: TrunCation - καθορίζει ότι αυτό το μήνυμα είχε υποστεί περικοπή

RD: Recursion Desired - αυτό το bit κατευθύνει το διακομιστή ονομάτων για να συνεχίσει το ερώτημα αναδρομικά

RA: Διαθέσιμη αναδρομή - αυτή η ρύθμιση έχει οριστεί ή εκκαθαριστεί σε μια απόκριση και υποδηλώνει εάν η υποστήριξη αναδρομικής αναζήτησης είναι διαθέσιμη στο διακομιστή ονομάτων. Η αναδρομική υποστήριξη ερωτημάτων είναι προαιρετική

RCODE: Κωδικός απόκρισης - αυτό το πεδίο 4-bit έχει οριστεί ως μέρος των απαντήσεων

QDCOUNT: ένας μη προσημασμένος ακέραιος αριθμός 16-bit που καθορίζει τον αριθμό των καταχωρήσεων στην ενότητα ερωτήσεων

ANCOUNT: ένας μη προσημασμένος ακέραιος αριθμός 16-bit που καθορίζει τον αριθμό των εγγραφών πόρων στην ενότητα απαντήσεων

ARCOUNT: ένας μη προσημασμένος ακέραιος αριθμός 16-bit που καθορίζει τον αριθμό των εγγραφών πόρων στην ενότητα πρόσθετων εγγραφών

Τα DNS ερωτήματα έχουν:

QNAME: Ένα όνομα τομέα που αντιπροσωπεύεται ως μια ακολουθία ετικετών, όπου κάθε ετικέτα αποτελείται από ένα longoctet ακολουθούμενο από αυτόν τον αριθμό οκτάδων. Το όνομα τομέα τερματίζεται με μηδενικό μήκος για την μηδενική ετικέτα της ρίζας

QTYPE: Ένας κωδικός δύο οκτάδων που καθορίζει τον τύπο του ερωτήματος

QCLASS: Ένας κωδικός δύο οκτάδων που καθορίζει την κλάση του ερωτήματος

Οι DNS απαντήσεις έχουν:

Name: Το όνομα τομέα που υποβλήθηκε σε ερώτηση, με την ίδια μορφή με το QNAME στις ερωτήσεις.

Type: δύο οκτάδες που περιέχουν έναν από τους κωδικούς τύπου. Αυτό το πεδίο καθορίζει την έννοια των δεδομένων στο πεδίο RDATA

Class: Δύο οκτάδες που καθορίζουν την κλάση των δεδομένων στο πεδίο RDATA

TTL: Ο αριθμός των δευτερολέπτων των αποτελεσμάτων μπορεί να αποθηκευτεί προσωρινά.

RLENGTH: Το μήκος του πεδίου RDATA

RDATA: Τα δεδομένα της απόκρισης. Η μορφή εξαρτάται από το πεδίο TYPE: εάν για παράδειγμα το TYPE is 0x0001 for A records, τότε αυτή είναι η διεύθυνση IP (4 οκτάδες). Εάν ο τύπος is 0x0005 for CNAMEs, τότε αυτό είναι το όνομα του ψευδωνύμου.

15. Το πακέτο πρόκειται για μία DNS ερώτηση. Το domain του οποίου ζητείται η IP είναι το ο gaia.cs.umass.edu

16. Το πακέτο πρόκειται για μία DNS ερώτηση.

Απαντήσεις για το μέρος Β

Μετά την πλήρη ανάλυση των δεκαεξαδικών πεδίων του frame δεδομένων:

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 02 03 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

Ethernet:

Destination: 00 A0 92 48 72 45

Source: 00 00 0C 05 C3 58

Type: 08 00

Internet Protocol:

Version: 4

Header length: 5

Differentiated Services Field: 00

Total length: 00 29

Identification: DB FB

Flags: 40 00

0... = Reserved bit: Not set

.1.. = Don't fragment: Set

..0. = More fragments: Not set

...0 0000 0000 0000 = Fragment offset: 0

Time to live: FE

Protocol: 06

Header checksum: 7D CB

Source: 81 6E 1E 1A

Destination: 81 6E 02 11

Transmission Control Protocol:

Source Port: 02 03

Destination Port: 00 50

Sequence number: 6A 86 7B 57

Acknowledgement number: B6 B6 B0 20

Header length: 0101 (2)

Flags: 0000 0001 0000 (2)

Window size value: 24 00

Checksum: 17 C4

Urgent pointer: 00 00

Payload: 02

Ethernet:

Padding: 02 54 41 4D 49 4C

Frame check sequence: D7 87 6C A4

Υποερώτημα 1:

Destination: 81 6E 02 11 = 129.110.2.17

Source: 81 6E 1E 1A = 129.110.30.26

Υποερώτημα 2:

20 Bytes

Υποερώτημα 3:

Αφού, στο τμήμα Internet Protocol, η σημαία More Fragments, καθώς και η σημαία Fragment Offset, ισούνται με 0, δηλαδή ούτε έπονται ούτε προηγούνται άλλα frames, τα οποία ανήκουν σε μεγαλύτερο πακέτο. Άρα το δεδομένο frame δεν αποτελεί τμήμα ενός μεγαλύτερου πακέτου.

Υποερώτημα 4:

Source Port: 02 03 (16) = 515 (10)

Destination Port: 00 50 (16) = 80 (10)

Υποερώτημα 5:

IP Header: 45 00 00 29 DB FB 40 00 FE 06 7D CB 81 6E 1E 1A 81 6E 02 11

45 00 (hex) = 0 1 0 0 0 1 0 1 0 0 0 0 0 0 0 0 (bin)

00 29 (hex) = 0 0 0 0 0 0 0 0 0 0 1 0 1 0 0 1 (bin)

Sum 1 = 0 1 0 0 0 1 0 1 0 0 1 0 1 0 0 1 (bin)

Sum 1 = 0 1 0 0 0 1 0 1 0 0 1 0 1 0 0 1 (bin)

DB FB (hex) = 1 1 0 1 1 0 1 1 1 1 1 1 1 0 1 1 (bin)

Sum 2 = 1 0 0 1 0 0 0 0 1 0 0 1 0 0 1 0 0 (bin) = 0 0 1 0 0 0 0 1 0 0 1 0 0 1 0 1 (bin)

Sum 2 = 0 0 1 0 0 0 0 1 0 0 1 0 0 1 0 1 (bin)

40 00 (hex) = 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 (bin)

Sum 3 = 0 1 1 0 0 0 0 1 0 0 1 0 0 1 0 1 (bin)

Sum 3 = 0 1 1 0 0 0 0 1 0 0 1 0 0 1 0 1 (bin)

FE 06 (hex) = 1 1 1 1 1 1 1 0 0 0 0 0 0 1 1 0 (bin)

Sum 4 = 1 0 1 0 1 1 1 1 1 0 0 1 0 1 0 1 1 (bin) = 0 1 0 1 1 1 1 1 0 0 1 0 1 1 0 0 (bin)

Sum 4 = 0 1 0 1 1 1 1 1 0 0 1 0 1 1 0 0 (bin)

7D CB (hex) = 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 (bin) // Checksum

Sum 5 = 0 1 0 1 1 1 1 1 0 0 1 0 1 1 0 0 (bin)

Sum 5 = 0 1 0 1 1 1 1 1 0 0 1 0 1 1 0 0 (bin)

81 6E (hex) = 1 0 0 0 0 0 0 1 0 1 1 0 1 1 1 0 (bin)

Sum 6 = 1 1 1 0 0 0 0 0 1 0 0 1 1 0 1 0 (bin)

Sum 6 = 1 1 1 0 0 0 0 0 1 0 0 1 1 0 1 0 (bin)

1E 1A (hex) = 0 0 0 1 1 1 1 0 0 0 0 1 1 0 1 0 (bin)

Sum 7 = 1 1 1 1 1 1 1 0 1 0 1 1 0 1 0 0

Sum 7 = 1 1 1 1 1 1 1 0 1 0 1 1 0 1 0 0 (bin)

81 6E (hex) = 1 0 0 0 0 0 0 1 0 1 1 0 1 1 1 0 (bin)

Sum 8 = 1 1 0 0 0 0 0 0 0 0 0 1 0 0 0 1 0 (bin) = 1 0 0 0 0 0 0 0 0 0 1 0 0 0 1 1 (bin)

Sum 8 = 1 0 0 0 0 0 0 0 0 0 1 0 0 0 1 1 (bin)

02 11 (hex) = 0 0 0 0 0 0 1 0 0 0 0 1 0 0 0 1 (bin)

Sum 9 = 1 0 0 0 0 0 1 0 0 0 1 1 0 1 0 0 (bin)

IP Checksum = 0 1 1 1 1 1 0 1 1 1 0 0 1 0 1 1 (bin) = 7DCB (hex)

Το IP Checksum είναι σωστό.

TCP Header: 02 03 00 50 6A 86 7B 57 B6 B6 B0 20 50 10 24 00 17 c4 00 00

02 03 (hex) = 0 0 0 0 0 0 1 0 0 0 0 0 0 0 1 1 (bin)

00 50 (hex) = 0 0 0 0 0 0 0 0 0 1 0 1 0 0 0 0 (bin)

Sum 1 = 0 0 0 0 0 0 1 0 0 1 0 1 0 0 1 1 (bin)

Sum 1 = 0 0 0 0 0 0 1 0 0 1 0 1 0 0 1 1 (bin)

6A 86 (hex) = 0 1 1 0 1 0 1 0 1 0 0 0 0 1 1 0 (bin)

Sum 2 = 0 1 1 0 1 1 0 0 1 1 0 1 1 0 0 1 (bin)

Sum 2 = 0 1 1 0 1 1 0 0 1 1 0 1 1 0 0 1 (bin)

7B 57 (hex) = 0 1 1 1 1 0 1 1 0 1 0 1 0 1 1 1 (bin)

Sum 3 = 1 1 1 0 1 0 0 0 0 0 1 1 0 0 0 0 (bin)

Sum 3 = 1 1 1 0 1 0 0 0 0 0 1 1 0 0 0 0 (bin)

B6 B6 (hex) = 1 0 1 1 0 1 1 0 1 0 1 1 0 1 1 0 (bin)

Sum 4 = 1 1 0 0 1 1 1 1 0 1 1 1 0 0 1 1 0 (bin) = 1 0 0 1 1 1 1 0 1 1 1 0 0 1 1 1 (bin)

Sum 4 = 1 0 0 1 1 1 1 0 1 1 1 0 0 1 1 1 (bin)

B0 20 (hex) = 1 0 1 1 0 0 0 0 0 0 1 0 0 0 0 0 (bin)

Sum 5 = 1 0 1 0 0 1 1 1 1 0 0 0 0 0 1 1 1 (bin) = 0 1 0 0 1 1 1 1 0 0 0 0 1 0 0 0 (bin)

Sum 5 = 0 1 0 0 1 1 1 1 0 0 0 0 1 0 0 0 (bin)

50 10 (hex) = 0 1 0 1 0 0 0 0 0 0 0 1 0 0 0 0 (bin)

Sum 6 = 1 0 0 1 1 1 1 1 0 0 0 1 1 0 0 0 (bin)

Sum 6 = 1 0 0 1 1 1 1 1 0 0 0 1 1 0 0 0 (bin)

24 00 (hex) = 0 0 1 0 0 1 0 0 0 0 0 0 0 0 0 0 (bin)

Sum 7 = 1 1 0 0 0 0 1 1 0 0 0 1 1 0 0 0 (bin)

Sum 7 = 1 1 0 0 0 0 1 1 0 0 0 1 1 0 0 0 (bin)

17 C4 v 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 (bin) // Checksum

Sum 8 = 1 1 0 0 0 0 1 1 0 0 0 1 1 0 0 0 (bin)

Sum 7 = 1 1 0 0 0 0 1 1 0 0 0 1 1 0 0 0 (bin)

00 00(hex) = 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 (bin)

Sum 9 = 1 1 0 0 0 0 1 1 0 0 0 1 1 0 0 0 (bin)

TCP Checksum = 0 0 1 1 1 1 0 0 1 1 1 0 0 1 1 1 (bin) = 3CE7 (hex)

To TCP Checksum είναι λάθος.

Απαντήσεις για το Πείραμα IP με την χρήση Wireshark

1. Η παράμετρος -d αποτρέπει την αντιστοίχιση διεύθυνσης IP με hostname.
2. Ethernet host 1c:6f:65:09:69:c0
3. Χρησιμοποιήθηκε το φίλτρο icmp.
4. Η διεύθυνση IP του υπολογιστή είναι 192.168.2.254. Αυτή η διεύθυνση εμφανίζεται στο πέμπτο πεδίο της κεφαλίδας.
5. Η τιμή του πρωτοκόλλου είναι: Protocol: ICMP.
6. Τα bytes της κεφαλίδας είναι 20 bytes.
7. Τα bytes που μεταφέρονται στο πεδίο δεδομένων του πακέτου IP είναι 36 bytes.

8. Το μήκος του πεδίου δεδομένων υπολογίζεται ως το υπόλοιπο της αφαίρεσης τους μήκους του IP πακέτου = 56 bytes – το μήκος του πεδίου κεφαλίδας = 20 bytes, άρα το μήκος του πεδίου δεδομένων είναι ίσο με 36 bytes.
9. Τα πεδία κεφαλίδας IP που αλλάζουν μεταξύ των πακέτων είναι το Identification και το Time to live.
10. Τα πεδία κεφαλίδας IP που παραμένουν αμετάβλητα μεταξύ των πακέτων είναι τα Version, Header Length, Differentiated Services Field, Total Length, Flags, Protocol, Header checksum, Source και Destination.
11. Τα πεδία κεφαλίδας IP που παραμένουν αμετάβλητα μεταξύ των πακέτων είναι τα Version, Header Length, Differentiated Services Field, Total Length, Flags, Protocol, Header checksum, Source και Destination. Τα πεδία αυτά πρέπει να παραμείνουν αμετάβλητα ώστε να μπορεί να γίνει η σωστή διασύνδεση των πακέτων μεταξύ τους.
12. Τα πεδία κεφαλίδας IP που αλλάζουν μεταξύ των πακέτων είναι το Identification και το Time to live. Τα πεδία αυτά αλλάζουν με βάση τα υπόλοιπα πακέτα, καθώς και τις ρυθμίσεις του αποστολέα.
13. Η διεύθυνση του κοντινότερου δρομολογητή προς τον υπολογιστή μου είναι 192.168.2.1.
14. Η τιμή του πεδίου TTL του πρώτου πακέτου ισούται με την IP του δρομολογητή, δηλαδή 192.168.2.1
15. Μερικά πακέτα μπορούν να χαθούν, να λήξουν κ.λ.π. Οπότε, όχι δεν παραμένει σταθερή η τιμή TTL του πεδίου της κεφαλίδας IP για όλα τα πακέτα της σειράς.

Απαντήσεις για το Cisco Packet Tracer - Υλοποίηση Hub

Ερωτήσεις:

Υποερώτημα Ι:

Η εντολή Ping 192.168.1.1, απευθύνεται στο τοπικό Interface του PC0. Η εντολή δημιούργησε μία σύνδεση με το Interface του PC0, έστειλε πακέτα στο Interface του PC0 και το Interface τα έλαβε σωστά και απάντησε με το κατάλληλο μήνυμα.

Υποερώτημα II:

Με την κλήση της εντολής Ping 192.168.1.2, λαμβάνουμε απάντηση από το PC1. Το PC0 χρησιμοποίησε την σύνδεση με το hub, προκειμένου να στείλει πακέτα στο PC1. Με την σειρά του το PC1, έλαβε τα απεσταλμένα πακέτα σωστά και απάντησε με κατάλληλο μήνυμα.

Υποερώτημα III:

Με την κλήση της εντολής Ping 192.168.1.2, λαμβάνουμε απάντηση από το PC1. Το PC0 χρησιμοποίησε την σύνδεση με το hub, προκειμένου να στείλει πακέτα στο PC1. Με την σειρά του το PC1, έλαβε τα απεσταλμένα πακέτα σωστά και απάντησε με κατάλληλο μήνυμα.

Απαντήσεις για το Cisco Packet Tracer - Configure SSH

Εντολές Μέρος Α

1. telnet 10.10.10.2
2. enable
3. copy running-config startup-config
4. show running-config
5. conf t
6. service password-encryption
7. ^z // CNTL/Z to exit the config terminal
8. show running-config

Εντολές Μέρος Β

1. conf t
2. ip domain-name netacad.pka
3. crypto key generate rsa
4. user
5. username up1054419 secret up1054419
6. line vty 0 15
7. login local
8. transport input ssh
9. ^z // CNTL/Z to exit the config terminal

10. conf t
11. username administrator secret cisco
12. line vty 0 15
13. transport input ssh
14. no password cisco

Εντολές Μέρος Γ

1. ^z // CNTL/Z to exit the config terminal
2. exit
3. telnet 10.10.10.2
4. ssh
5. ssh -l administrator 10.10.10.2
6. enable
7. copy running-config startup-config