

# ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

## ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΙΣΤΩΝ

### ΔΙΚΤΥΑ ΥΠΟΛΟΓΙΣΤΩΝ – 7<sup>ο</sup> ΕΞΑΜΗΝΟ

Τζομάκα Αφροδίτη – ΑΜ: 03117107

Όνοματεπώνυμο: Τζομάκα Αφροδίτη	Ομάδα: 2
Όνομα PC/ΛΣ: DESKTOP-II5SP0K/windows 10	Ημερομηνία: 3-11-2020
Διεύθυνση IP: 192.168.1.3	Διεύθυνση MAC: A8:6B:AD:73:3E:A5

### 6<sup>η</sup> Ομάδα Ασκήσεων

#### ΑΣΚΗΣΗ 1

- 1.1. ether host A8:6B:AD:73:3E:A5
- 1.2. arp or icmp
- 1.3. Για επικοινωνία στο τοπικό δίκτυο απαιτείται γνώση των φυσικών διευθύνσεων. Η αντιστοίχιση IPv4 – MAC διευθύνσεων αποθηκεύεται στον πίνακα ARP. Στην καταγραφή μας παρατηρούμε ένα ζεύγος arp request – reply με πηγή την προκαθορισμένη πύλη και προορισμό τον υπολογιστή μας. Αυτό σημαίνει ότι η MAC του υπολογιστή μας δεν ήταν αποθηκευμένη στον arp της προκαθορισμένης πύλης και γι' αυτό υπήρξε αυτό το αίτημα(polling).
- 1.4. Ο τύπος του πακέτου προσδιορίζεται από την ετικέτα Protocol της επικεφαλίδας IPv4 και εν προκειμένω για πακέτο ICMP έχει τιμή 1.
- 1.5. 8bytes.
- 1.6. Type (1byte), Code (1byte), Checksum (2bytes), Identifier(BE-LE) (2bytes), Sequence Number(BE-LE) (2bytes).

Τα παραπάνω πεδία κατανέμονται στην επικεφαλίδα ICMP όπως φαίνεται στο παρακάτω σχήμα (πηγή Wikipedia) με πράσινο χρώμα.

+	Bits 0–3	4–7	8–15	16–18	19–31
0	Version	IHL	TOS/DSCP/ECN	Total Length	
32	Identification			Flags	Fragment Offset
64	Time to Live		Protocol	IP Header Checksum	
96	Source Address				
128	Destination Address				
160	Type		Code	Checksum	
192	ID			Sequence	

1.7.

Type: 8 (Echo (ping) request)  
Code: 0

1.8.

Identifier (BE): 1 (0x0001)  
Identifier (LE): 256 (0x0100)  
Sequence Number (BE): 5 (0x0005)  
Sequence Number (LE): 1280 (0x0500)

1.9. Το πεδίο δεδομένων έχει μήκος 32 bytes και παρατηρούμε ότι το περιεχόμενο του είναι η αγγλική αλφάβητος μέχρι το w επαναλαμβανόμενα έως να συμπληρωθεί το μήκος αυτό:

0020	01 01 08 00 4d 56 00 01 00 05 61 62 63 64 65 66	...MV.. ..abcdef
0030	67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76	ghijklmn opqrstuv
0040	77 61 62 63 64 65 66 67 68 69	wabcdefg hi

1.10. 8bytes, ίδιο με εκείνο του ICMP request, ενώ ίδια φαίνεται να είναι κ η δομή του.

1.11.

Type: 0 (Echo (ping) reply)  
Code: 0

1.12. Το πεδίο Type.

1.13.

Identifier (BE): 1 (0x0001)  
Identifier (LE): 256 (0x0100)  
Sequence Number (BE): 5 (0x0005)  
Sequence Number (LE): 1280 (0x0500)

1.14.

Identifier (BE): 1 (0x0001)  
Identifier (LE): 256 (0x0100)  
Sequence Number (BE): 5 (0x0005)  
Sequence Number (LE): 1280 (0x0500)

1.15. Τα πεδία Identifier και Sequence Number έχουν ως ρόλο την αντιστοίχιση πακέτων request – reply και πρέπει να επιστραφούν μέσω του reply στο requester αναλλοίωτα.

1.16. 32 Bytes που αντιστοιχούν στην αγγλική αλφάβητο.

1.17. Το περιεχόμενο αυτό είναι ίδιο με εκείνο του request πακέτου.

1.18. Οι ανταλλαγές μηνυμάτων ICMP φαίνονται να έχουμε πλήρη αντιστοιχία με τα αποτελέσματα της εντολής Ping στο παράθυρο εντολών:

```
C:\Users\Afroditi>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=7ms TTL=64
Reply from 192.168.1.1: bytes=32 time=12ms TTL=64
Reply from 192.168.1.1: bytes=32 time=6ms TTL=64
Reply from 192.168.1.1: bytes=32 time=9ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 6ms, Maximum = 12ms, Average = 8ms
```

Βλέπουμε την πληροφορία για τα 32 byte δεδομένων καθώς και τους χρόνους απόκρισης κάθε request που αναγράφονται επίσης στο πεδίο λεπτομερειών του wireshark για κάθε πακέτο reply.

- 1.19. 12 πακέτα.
- 1.20. Κάθε περίπου 1 sec.
- 1.21. Δεν στάθηκε κανένα πακέτο ICMP.
- 1.22. Ο υπολογιστής προσπαθεί να μάθει την φυσική διεύθυνση που κάνουμε Ping ωστόσο επειδή είναι αυτή αντιστοιχεί σε ανενεργό υπολογιστή δεν μπορούμε να επικοινωνήσουμε μαζί του κ έτσι να έχουμε ανταλλαγή πακέτων ICMP (destination host unreachable).

## ΑΣΚΗΣΗ 2

- 2.1. Ταυτίζονται με τις διευθύνσεις που είχε και πριν το ping.

```
C:\Users\Afroditi>arp -a

Interface: 192.168.1.3 --- 0x9
    Internet Address      Physical Address          Type
    192.168.1.1           74-b5-7e-1f-6b-7a        dynamic
    192.168.1.255         ff-ff-ff-ff-ff-ff        static
    224.0.0.22            01-00-5e-00-00-16        static
    224.0.0.251           01-00-5e-00-00-fb        static
    224.0.0.252           01-00-5e-00-00-fc        static
    239.255.255.250       01-00-5e-7f-ff-fa        static
    255.255.255.255       ff-ff-ff-ff-ff-ff        static
```

- 2.2. MAC αποστολέα: A8:6B:AD:73:3E:A5, MAC παραλήπτη: 74:B5:7E:1F:6B:7A
- 2.3. IPv4 αποστολέα: 192.168.1.3, IPv4 παραλήπτη: 192.168.1.1.
- 2.4. MAC αποστολέα: Ο υπολογιστής μας, MAC παραλήπτη: Προκαθορισμένη πύλη.
- 2.5. N
- 2.6. Όπως και πριν παρατηρούμε ένα ζεύγος arp request – reply με πηγή την προκαθορισμένη πύλη και προορισμό τον υπολογιστή μας. Αυτό σημαίνει ότι η MAC του υπολογιστή μας δεν ήταν αποθηκευμένη στον arp πίνακα της προκαθορισμένης πύλης και γι' αυτό υπήρξε αυτό το αίτημα.
- 2.7. icmp.type == 0.
- 2.8. Το πεδίο Time to live έχει την τιμή 59. Επομένως σωστά εμφανίζεται και στο παράθυρο εντολών, TTL=59.
- 2.9. Echo request.
- 2.10. Στην προηγούμενη περίπτωση το μήνυμα που παίρναμε ήταν: Reply from 192.168.1.1: Destination host unreachable, ενώ τώρα: Request timed out, διότι τώρα έχουμε αποστολή μηνυμάτων απλά δεν φτάνουν στον προορισμό επειδή αυτός είναι ανενεργός

### **ΑΣΚΗΣΗ 3**

- 3.1. 64bytes μηδενικών.
- 3.2. Παρατηρούμε ότι η εντολή tracert παράγει ICMP πακέτα με διπλάσιο μήκος δεδομένων και διαφορετικό περιεχόμενο.
- 3.3. Time-to-live exceeded (Time to live exceeded in transit).
- 3.4. Type: 11 (Time-to-live exceeded), Code: 0 (Time to live exceeded in transit).
- 3.5. Type(1byte), Code(1byte), Checksum(2bytes), Unused(4bytes).
- 3.6. Το μήκος του πεδίου δεδομένων είναι 92bytes(Original IPv4 header+Original ICMP header+Data).
- 3.7. Είναι αυτά του αρχικού δεδομενογράμματος που στάλθηκε και χρησιμοποιούνται από τον host για να αντιστοιχίσει το μήνυμα με την κατάλληλη διεργασία (identification field).

### **ΑΣΚΗΣΗ 4**

- 4.1. Λαμβάνοντας υπόψη την προσθήκη επικεφαλίδας 28byte χρησιμοποιούμε μήκος δεδομένων 1472, 1464, 978, 548, 524, 516, 480, 268.
- 4.2. Ναι.
- 4.3. Η προκαθορισμένη πύλη.
- 4.4. Type: 3 (Destination unreachable), Code: 4 (Fragmentation needed).
- 4.5. Το πεδίο Code. MTU of next hop: 1492.
- 4.6. Η αγγλική αλφάβητος μέχρι το w επαναλαμβανόμενα έως να συμπληρωθεί το μήκος αυτό(520bytes).
- 4.7. 1492.
- 4.8. 1500, 1492, 1006.
- 4.9. 576.
- 4.10. Ναι, διότι σε αυτό απαντάει ο προορισμός.
- 4.11. Σύμφωνα με το RFC 1191, το μήνυμα Destination Unreachable στέλνετε όταν ένα δεδομενόγραμμα ξεπερνά την MTU του next hop και έχει set το πεδίο Don't Fragment. Μόνο η πρώτη τιμή MTU από αυτές που δοκιμάσαμε ξεπερνά την τιμή του πεδίου MTU of Next-Hop που είναι ο δρομολογητής μας κ είναι 1492.
- 4.12. Το συνολικό μήκος είναι 572 και το μήκος των δεδομένων είναι 552 bytes αντί 576 και 556 αντίστοιχα που ήτα το αναμενόμενο. Αυτό συμβαίνει επειδή το Offset έχει 13 bit προκειμένου να γίνει το reassembly χρειαζόμαστε τα δεδομένα του θραύσματος να είναι πολλαπλάσιο του 8 ( $2^{16-13}=3$ ).

### **ΑΣΚΗΣΗ 5**

- 5.1. ip and host 147.102.40.15
- 5.2. nslookup server 147.102.40.15

- 5.3. Λαμβάνουμε την εξής απάντηση

```
C:\Users\Afroditi>nslookup server 147.102.40.15
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  147.102.40.15

DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
*** Request to UnKnown timed-out
```

Από τα μηνύματα αυτά καταλαβαίνουμε ότι δεν μπορούμε να φτάσουμε τον DNS και ο server δεν αναγνωρίζεται.

- 5.4. Ναι.

- 5.5. Protocol: UDP, Destination port: 53.

- 5.6. Ναι.

- 5.7.

```
Type: 3 (Destination unreachable)
Code: 3 (Port unreachable)
```

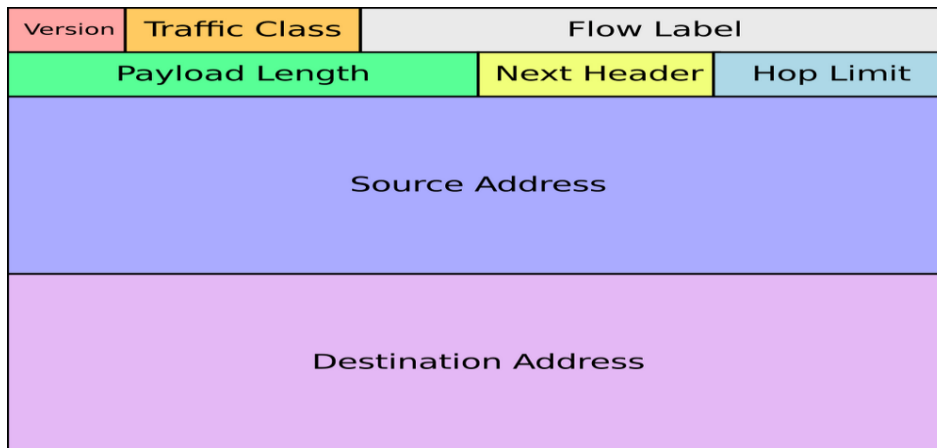
- 5.8. Το πεδίο Code.

- 5.9. Από το Type (destination unreachable και destination=dns port).

- 5.10. ICMP Port Unreachable.

## **ΑΣΚΗΣΗ 6**

- 6.1. ping -6 2001:648:2000:329::101 και tracert -6 2001:648:2000:329::101.
- 6.2. ip6 και icmpv6.
- 6.3. Type: IPv6 (0x86dd).
- 6.4. 40bytes.
- 6.5. Version(4bits), Traffic Class(8bits), Flow Label(20bits), Payload Length(2bytes), Next Header(1byte), Hop Limit(1byte), Source Address(16bytes), Destination Address(16bytes).



- 6.6. Hop Limit.
- 6.7. Next Header: ICMPv6 (58).
- 6.8. Ναι.
- 6.9. Type: Echo (ping) request (128) και μεταφέρει δεδομένα μήκους 32 bytes.
- 6.10. Ναι.
- 6.11. Type: Echo (ping) reply (129) και μεταφέρει δεδομένα μήκους 32 bytes.
- 6.12. Μεταφέρει μεγαλύτερο μήκος δεδομένων (64bytes) και δεν έχει σταθερό hop limit (λόγω της διαδικασίας του tracing).
- 6.13. Είναι σχεδόν ίδια. Στο v4 παρατηρούμε ότι το πεδίο type έχει τιμή 11 για time-to-live exceeded ενώ εδώ έχουμε type = 3 και time exceeded, δεν έχουμε unused αλλά reserved και επίσης μεγαλώνει το μήκος των επικεφαλίδων που ενθυλακώνει το ICMPv6 (λογικό αφού επιστρέφει αυτά που του στάλθηκαν κ πλέον είναι v6).
- 6.14. Type: Time exceeded (3) και μεταφέρει δεδομένα μήκους 112bytes (40(IPv6Header)+8(ICMPv6Header)+64(Data)).
- 6.15. 40 bytes IPv6Header + 8 bytes ICMPv6Header + 64 bytes μηδενικών = 112 bytes.