

Όνοματεπώνυμο: Ιωάννης Γιαννούκος		Ομάδα: 3
Όνομα PC/ΛΣ: JohnJohn / Windows 11	Ημερομηνία: 23/11/2022	
Διεύθυνση IP: 147.102.236.223	Διεύθυνση MAC: 3C-6A-A7-9A-B3-CF	

## Εργαστηριακή Άσκηση 6

### Πρωτόκολλο ICMP

Απαντήστε στα ερωτήματα στον χώρο που σας δίνεται παρακάτω και στην πίσω σελίδα εάν δεν επαρκεί. Το φυλλάδιο αυτό θα παραδοθεί στον επιβλέποντα.

#### Άσκηση 1

1.1) Φίλτρο σύλληψης: «ether host 3C-6A-A7-9A-B3-CF»

1.2) Φίλτρο απεικόνισης: «arp or icmp»

1.3) Δεν καταγράφηκαν πακέτα ARP.

1.4) Στην επικεφαλίδα IPv4 του πρώτου πακέτου ICMP υπάρχει το πεδίο «Protocol», το οποίο έχει την τιμή 1, επειδή πρόκειται για πακέτο πρωτοκόλλου ICMP.

1.5) 8 bytes

1.6)

Type (1B)	Code (1B)	Checksum (2B)	
Identifier(BE) [1Byte]	Identifier(LE) [1Byte]	Sequence Number (BE) [1Byte]	Sequence Number (LE) [1Byte]

1.7) Τα μηνύματα ICMP Echo request έχουν τις εξής τιμές πεδίων:

Type → 8, Code → 0

1.8) Το πρώτο μήνυμα ICMP Echo request έχει τις εξής τιμές πεδίων:

Identifier(BE) → 1, Identifier(LE) → 256,

Sequence Number(BE) → 80, Sequence Number(LE) → 20480

1.9) Η εντολή ping στέλνει μηνύματα ICMP Echo request με 32 bytes δεδομένων, το περιεχόμενο των οποίων είναι «abcdefghijklmnopqrstuvwxyzabcdefghi».

1.10) Τα μηνύματα ICMP Echo reply έχουν μέγεθος επικεφαλίδας 8 bytes, η οποία επικεφαλίδα έχει ακριβώς την ίδια δομή με αυτή των μηνυμάτων ICMP echo request.

1.11) Τα μηνύματα ICMP Echo request έχουν τις εξής τιμές πεδίων:

Type → 0, Code → 0

1.12) Το είδος του μηνύματος το καθορίζει το πεδίο Type, αφού είναι το μόνο που διαφέρει μεταξύ των μηνυμάτων Echo request και Echo reply.

1.13) Το πρώτο μήνυμα ICMP Echo reply έχει τις εξής τιμές πεδίων:  
Identifier(BE) → 1 , Identifier(LE) → 256,  
Sequence Number(BE) → 80 , Sequence Number(LE) → 20480

1.14) Οι τιμές των πεδίων Identifier και Sequence Number για κάθε ζευγάρι μηνυμάτων Echo request – Echo reply είναι κοινές.

1.15) Τα δύο αυτά πεδία εξυπηρετούν τον σκοπό να μπορούμε να αναγνωρίσουμε τα ζευγάρια ICMP Echo request – ICMP Echo reply. Η τιμή των δύο αυτών πεδίων σε ένα μήνυμα ICMP Echo request είναι κοινές με τις τιμές των αντίστοιχων πεδίων ενός (το πολύ) μηνύματος ICMP Echo reply.

1.16) Το μήκος και το περιεχόμενο των μηνυμάτων ICMP Echo reply είναι ακριβώς οι ίδιες με αυτά των μηνυμάτων ICMP Echo request, δηλαδή 32 bytes και «abcdefghijklmnopqrstuvwabcdefghi».

1.17) Όχι.

1.18) Στο παράθυρο εντολών εμφανίζονται οι απαντήσεις, δηλαδή πληροφορίες για τα μηνύματα ICMP Echo reply, όπως το μήκος δεδομένων τους, η τιμή RTT και η τιμή TTL.

1.19) “ping -n 2 -4 147.102.236.169”

1.20) Στάλθηκαν 4 πακέτα ARP.

1.21) Κάθε περίπου 1 δευτερόλεπτο.

1.22) Κανένα, αφού δεν βρέθηκε η MAC του παραλήπτη.

1.23) Στο παράθυρο εντολών εμφανίστηκαν 2 μηνύματα «απάντησης» “Destination host unreachable”. Αυτό υποδηλώνει ότι ο παραλήπτης δεν βρέθηκε στο δίκτυο.

## Άσκηση 2

2.1)

```
PS C:\WINDOWS\system32> arp -a

Interface: 192.168.56.1 --- 0xc
Internet Address      Physical Address      Type
192.168.56.255        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

Interface: 147.102.236.223 --- 0xf
Internet Address      Physical Address      Type
147.102.236.2         46-a0-ea-51-03-2a    dynamic
147.102.236.167       d0-9c-7a-d9-34-36    dynamic
147.102.236.200       08-ec-f5-d0-d9-1d    dynamic
147.102.236.230       00-50-56-b5-aa-aa    dynamic
147.102.238.163       7c-67-a2-7b-c2-12    dynamic
147.102.239.110       28-3a-4d-8f-38-d5    dynamic
147.102.239.189       a0-c5-89-c7-da-3a    dynamic
147.102.239.255       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
239.255.102.18        01-00-5e-7f-66-12    static
239.255.255.250       01-00-5e-7f-ff-fa    static
255.255.255.255       ff-ff-ff-ff-ff-ff    static
PS C:\WINDOWS\system32>
```

2.2)

Source: 3c:6a:a7:9a:b3:cf

Destination: 08:ec:f5:d0:d9:1d

2.3)

Source Address: 147.102.236.223

Destination Address: 147.102.40.1

2.4) Η MAC του πεδίου Source αντιστοιχεί στον προσωπικό μου υπολογιστή, δηλαδή στην διεύθυνση 147.102.236.223 και η διεύθυνση του πεδίου Destination αντιστοιχεί στην Default Gateway.

2.5) Όχι.

2.6) Δεν παρατήρησα κάποια ανταλλαγή πακέτων ARP, επειδή, παρόλο που ο πίνακας DNS του υπολογιστή μου δεν περιείχε ζευγάρι διεύθυνσης-ονόματος στην προκειμένη περίπτωση, ίσως το ζευγάρι αυτό υπήρχε αποθηκευμένο στον router του πολυτεχνείου, κι έτσι δεν χρειάστηκε να σταλεί πακέτο ARP.

2.7) "icmp.type == 0"

2.8) Η τιμή των μηνυμάτων ICMP Echo reply είναι 63. Αυτό συμβαίνει επειδή η απόσταση μεταξύ του υπολογιστή μου και της διεύθυνσης IP 147.102.40.1 είναι πολύ κοντινή (αφού προορισμός και αφετηρία βρίσκονται σε κοινό δίκτυο, αν και σε διαφορετικό υποδίκτυο), κι έτσι χρειάζεται μόνο ένα βήμα για να φτάσει το μήνυμα στον προορισμό του. Σημειώνεται ότι το πακέτο αυτό ξεκίνησε την διαδρομή του με τιμή TTL = 64.

2.9) Εμφανίζονται μόνο τύποι μηνυμάτων ICMP Echo request.

2.10) Το μόνο που διαφέρει σε αυτήν την περίπτωση σε σύγκριση με την προηγούμενη είναι ότι η τιμή TTL είναι μεγαλύτερη. (??)

### ***Άσκηση 3***

3.1) Η εντολή **tracert** παράγει μηνύματα ICMP Echo request με 64 bytes δεδομένων, τα οποία περιέχουν μόνο μηδενικά, δηλαδή 64 κενά διαστήματα.

3.2) Η εντολή **ping** παράγει μηνύματα ICMP Echo request με 32 bytes με περιεχόμενο δεδομένων «abcdefghijklmnopqrstuvwxyzabcdefghi». Επομένως, η εντολή **tracert** παράγει μηνύματα με διπλάσιο μέγεθος δεδομένων και μικρότερο «φάσμα» πληροφορίας.

3.3) Το μήνυμα ICMP Time-to-live exceed, καθώς το πακέτο που στέλνεται «λήγει» μόλις φτάσει στον ενδιαμέσο δρομολογητή.

3.4) Type: 11  
Code: 0

3.5) Περιέχονται ακόμα τα πεδία Checksum (2 bytes), Unused (1 byte), Length (1 byte), Unused (2 bytes), Internet Protocol Version 4 (20 bytes), Internet Control Message Protocol (48 bytes).

3.6) Μήκος Επικεφαλίδας: 20 bytes  
Μήκος Δεδομένων: 76 bytes

3.7) Τα δεδομένα που μεταφέρει το μήνυμα ICMP Time exceeded είναι, ουσιαστικά, πληροφορίες σχετικά με το αρχικό μήνυμα ICMP που έφτασε στον δρομολογητή και προκάλεσε την δημιουργία του.

### ***Άσκηση 4 (IP: 147.102.203.161)***

4.1) Το μέγεθος των πακέτων χωρίς αυτό των δεδομένων είναι ίσο με 42 bytes, από τα οποία 14 είναι η επικεφαλίδα Ethernet, 20 η επικεφαλίδα IPv4 και 8 η επικεφαλίδα ICMP. Επομένως, εκτέλεσα την εντολή ping για τιμές 1458, 1450, 964 και 534 bytes.

4.2) Όχι, δεν έλαβα μήνυμα λάθους ICMP Destination Unreachable.

4.3) –

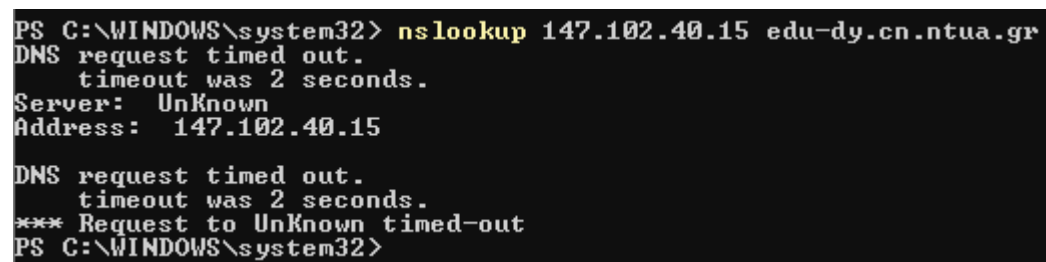
4.4) Type: 3 (Destination Unreachable)  
Code: 4 (Fragmentation needed)

4.5) Αυτό το δηλώνει το πεδίο “Code”. Η επικεφαλίδα MTU of next hop έχει τιμή 1492.

- 4.6) Στο πεδίο των δεδομένων έχουν αποθηκευτεί πληροφορίες που αφορούν το αρχικό πακέτο που θελήσαμε να στείλουμε χωρίς θρυμματισμό.
- 4.7) MTU: 1500 bytes
- 4.8) Το 147.102.40.15 δεν απαντά για MTU τιμές 1500, 1492 και 1006.
- 4.9) Απάντηση λαμβάνω για τιμή MTU 576 bytes.
- 4.10) Η MTU αυτή ανήκει στην δικτυακή διεπαφή του 147.102.40.15, διότι δεν στέλνεται μήνυμα λάθους ICMP Destination unreachable. Το μήνυμα αυτό αποστέλλεται μόνο από ενδιάμεσο κόμβο, όταν αυτός έχει μικρότερη MTU από το μέγεθος του πακέτου.
- 4.11) Δεν παράγεται ICMP Destination Unreachable, επειδή το μήνυμα ICMP request έφτασε στον τελικό προορισμό του. Σημειώνεται εδώ ότι η MTU ενός δρομολογητή/εξυπηρετητή καθορίζει το μέγεθος των εξερχόμενων μηνυμάτων, επομένως μπορούν να λάβουν μηνύματα μεγαλύτερα αυτής.
- 4.12) Όχι, το πρώτο θραύσμα που λαμβάνω έχει μέγεθος 586 bytes, δηλαδή 10 bytes περισσότερο από την MTU που βρήκα στο ερώτημα 4.9.

## ***Άσκηση 5***

- 5.1) “host 147.102.40.15”
- 5.2) “nslookup 147.102.40.15 edu-dy.cn.ntua.gr”
- 5.3)



```
PS C:\WINDOWS\system32> nslookup 147.102.40.15 edu-dy.cn.ntua.gr
DNS request timed out.
    timeout was 2 seconds.
Server:      Unknown
Address:     147.102.40.15

DNS request timed out.
    timeout was 2 seconds.
*** Request to Unknown timed-out
PS C:\WINDOWS\system32>
```

Ο εξυπηρετητής 147.102.40.15 δεν έχει καταχωρημένη τη διεύθυνση IPv4 του edu-dy.cn.ntua.gr, κι έτσι δεν στέλνει απάντηση.

5.4) Ναι, καταγράφηκαν 2 μηνύματα DNS, τα οποία στάλθηκαν από τον υπολογιστή μου στον εξυπηρετητή 147.102.40.15.

- 5.5)     Protocol:                UDP  
         Destination Port:       53

5.6) Ναι, καταγράφηκαν δύο τέτοια μηνύματα, ένα μετά από κάθε πακέτο DNS που έστειλα από τον υπολογιστή μου.

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

5.8) Το πεδίο Code.

5.9) Διότι ως δεδομένα στα πακέτα αυτά υπάρχουν όλες οι πληροφορίες των μηνυμάτων UDP από τα οποία προκλήθηκαν.

5.10) (Εχω Windows 11 και λαμβάνω ICMP Destination Unreachable.)

## ***Άσκηση 6***

6.1) “ping -6 2001:648:2000:329::101”  
“tracert -6 2001:648:2000:329::101”

6.2) Φίλτρο σύλληψης: “ip6”  
Φίλτρο απεικόνισης: “icmpv6”

6.3) Type: 0x86dd

6.4) Το μήκος της επικεφαλίδας των πακέτων IPv6 είναι 40 bytes.

6.5)

**Version:** ½ byte

**Traffic Class:** 1 byte

**Flow Label:** 2 ½ bytes

**Payload Length:** 2 bytes

**Next Header:** 1 byte

**Hop Limit:** 1 byte

**Source Address:** 16 bytes

**Destination Address:** 16 bytes

Version [½]	Traffic Class [1]	Flow Label [2½]	
Payload Length [2]		Next Header [1]	Hop Limit [1]
SOURCE ADDRESS [16]			
DESTINATION ADDRESS [16]			

6.6) Το πεδίο Hop Limit.

6.7) Το πεδίο Next Header, που στην περίπτωση μας έχει τιμή 58.

6.8) Δεν είναι ακριβώς η ίδια δομή. Στην περίπτωση των ICMPv6, αντί για δύο πεδία Identifier και Sequence, υπάρχει μόνο ένα.

6.9) Type: Echo (ping) request (128)  
Μήκος Δεδομένων: 64 bytes

6.10) Ναι, είναι ακριβώς η ίδια.

6.11) Type: Echo (ping) reply (129)  
Μήκος Δεδομένων: 64 bytes

6.12) Δεν διαφέρει σε τίποτα από το αντίστοιχο πακέτο που παράγεται από την εντολή ping.

6.13) Όχι, δεν έχουν ακριβώς την ίδια δομή.

6.14) Το πεδίο Type έχει τιμή 3 και το μήκος των δεδομένων είναι 112 bytes.

6.15) Το πεδίο των δεδομένων του μηνύματος ICMPv6 Time exceeded περιέχει όλες τις τιμές των πεδίων του μηνύματος που στάλθηκε από την κλήση της εντολής ping.

6.16) Ναι, παρατήρησα ότι καταγράφηκαν μηνύματα “Router Advertisement”, “Multicast Listener Report Message” και διάφορα άλλα από διάφορους δρομολογητές του δικτύου.

6.17)

- Για το μήνυμα “Router Advertisement” έχουμε:

Type: Router Advertisement (134) , Length: 48 bytes

- Για το μήνυμα “Multicast Listener Report Message” έχουμε:

Type: Multicast Listener Report Message (143) , Length: 28 bytes