Δίκτυα Υπολογιστών
Εργαστηριακή Άσκηση 6

Ονοματεπώνυμο: Κυριακόπουλος Γεώργιος – el18153
Ομάδα: 4
Όνομα PC/ΛΣ: George – Windows 10 Pro, 21H1
Ημερομηνία: 29/11/2021
Διεύθυνση IP: 192.168.1.7
Διεύθυνση MAC: 60-A4-B7-75-72-0F

Άσκηση 1:

1.1.
Το φίλτρο σύλληψης που χρησιμοποίησα είναι το: *ether host 60:a4:b7:75:72:0f.*

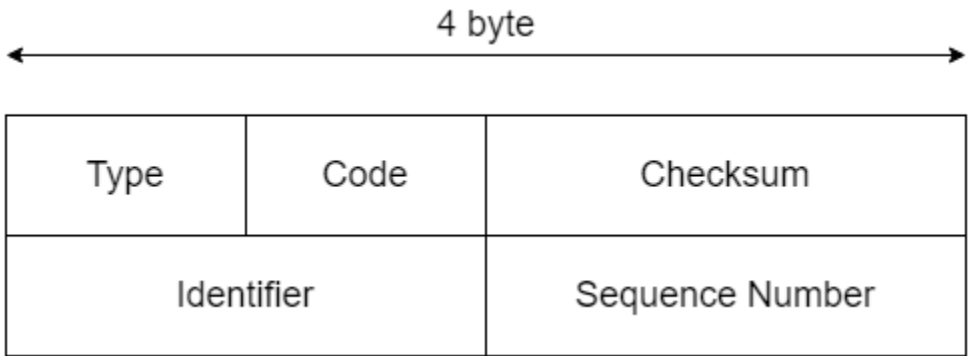
1.2.
Το φίλτρο απεικόνισης που χρησιμοποίησα είναι το: *arp or icmp.*

1.3.
Έχει καταγραφεί ένα ζευγάρι ARP μηνυμάτων, που ουσιαστικά αποσκοπεί στο να μάθει η default gateway την διεύθυνση MAC του υπολογιστή μου, η οποία αντιστοιχεί στην διεύθυνση IPv4 μου, 192.168.1.7.

1.4.
Είναι το πεδίο Protocol με τιμή 1 (0x01), που δηλώνει ICMP πρωτόκολλο.

1.5.
Η επικεφαλίδα των ICMP Echo request μηνυμάτων έχει μήκος 8 bytes.

1.6
Έχουμε τα παρακάτω πεδία (με το αντίστοιχο μήκος σε bytes): Type (1), Code (1), Checksum (2), Identifier (2), Sequence Number (2). Οι θέσεις τους φαίνονται και στο παρακάτω σχήμα:



1.7.
Το πεδίο Type έχει τιμή 8 (0x08), ενώ το πεδίο Code έχει τιμή 0 (0x00).

1.8.
Το πεδίο Identifier έχει τιμή 1 ή 256 σε BE ή LE αντίστοιχα (0x0001 ή 0x0100), ενώ το Sequence Number έχει, ομοίως, τιμή 1 ή 256 σε BE ή LE αντίστοιχα (0x0001 ή 0x0100).

1.9.
Το πεδίο δεδομένων των μηνυμάτων ICMP Echo request έχει μήκος 32 bytes και περιεχόμενο την λατινική αλφάβητο μέχρι και το w και ξανά από την αρχή. Φυσικά, ως τιμές έχει τους αντίστοιχους 16δικούς αριθμούς 0x61 έως και 0x77 και πάλι από το 0x61.

1.10.
Η επικεφαλίδα των ICMP Echo reply μηνυμάτων έχει, επίσης, μήκος 8 bytes και η δομή της είναι ίδια με του Echo request.

1.11.
Το πεδίο Type έχει τιμή 0 (0x00), ενώ το πεδίο Code έχει και αυτό τιμή 0 (0x00).

1.12.
Το πεδίο Type καθορίζει το είδος του μηνύματος ICMP (8 για Echo request και 0 για Echo reply).

1.13.
Το πεδίο Identifier έχει τιμή 1 ή 256 σε BE ή LE αντίστοιχα (0x0001 ή 0x0100), ενώ το Sequence Number έχει, ομοίως, τιμή 1 ή 256 σε BE ή LE αντίστοιχα (0x0001 ή 0x0100).

1.14.
Είναι ίδιες, όπως φαίνεται και από τις απαντήσεις στα παραπάνω ερωτήματα.

1.15.
Τα δύο αυτά πεδία χρησιμοποιούνται για να ταιριάξουν τα Echo request με τα Echo reply μηνύματα.

1.16.
Το πεδίο δεδομένων των μηνυμάτων ICMP Echo reply έχει μήκος 32 bytes και περιεχόμενο την λατινική αλφάβητο μέχρι και το w και ξανά από την αρχή. Φυσικά, ως τιμές έχει τους αντίστοιχους 16δικούς αριθμούς 0x61 έως και 0x77 και πάλι από το 0x61.

1.17.
Όχι, το περιεχόμενο είναι ίδιο με αυτό του Echo request.

1.18.
Ουσιαστικά για κάθε ένα ping που βλέπουμε στο παράθυρο εντολών αντιστοιχεί και ένα ζευγάρι Echo request – Echo reply μηνυμάτων.

1.19.
Χρησιμοποίησα την εξής σύνταξη: $ *ping 192.168.1.11 -n 2.*

1.20.
Στάλθηκαν 6 πακέτα ARP request για να βρουν την διεύθυνση MAC του μη ενεργού υπολογιστή.

1.21.
Τα πακέτα αυτά στέλνονται περίπου κάθε 1 second.

1.22.
Δεν στάλθηκε κανένα ICMP μήνυμα.

1.23.
Ουσιαστικά, επιχείρησα να κάνω ping σε μία IPv4 διεύθυνση, για την οποία πρέπει πρώτα να μάθω την MAC διεύθυνση της. Αυτό προσπαθεί να γίνει μέσω των ARP request μηνυμάτων, αλλά αφού αποτυγχάνει να λάβει απάντηση μετά από κάποια δευτερόλεπτα, τυπώνει το μήνυμα Destination host unreachable στο παράθυρο εντολών, ενώ στο Wireshark βλέπουμε ότι δεν υπάρχουν απαντήσεις στα ARP request πακέτα.

Άσκηση 2:

2.1.
Ο πίνακας ARP περιέχει τις παρακάτω καταχωρήσεις:

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

Interface: 192.168.1.7 --- 0x5
  Internet Address      Physical Address      Type
  192.168.1.1           98-3b-67-9a-54-70     dynamic
  192.168.1.5           50-56-bf-07-1b-4b     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

Interface: 172.22.48.1 --- 0x25
  Internet Address      Physical Address      Type
  172.22.62.205         00-15-5d-9a-33-83     dynamic
  172.22.63.255         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
  239.255.255.250       01-00-5e-7f-ff-fa     static
```

2.2.
Η διεύθυνση MAC του αποστολέα είναι η 60:a4:b7:75:72:0f, ενώ του παραλήπτη είναι η 98:3b:67:9a:54:70.

2.3.
Η διεύθυνση IPv4 του αποστολέα είναι η 192.168.1.7, ενώ του παραλήπτη είναι η 147.102.1.1.

2.4.
Η 60:a4:b7:75:72:0f αντιστοιχεί στην 192.168.1.7 (του υπολογιστή μου), ενώ η 98:3b:67:9a:54:70 αντιστοιχεί στην 192.168.1.1 (του router μου).

2.5.
Όχι, δεν παρατήρησα ARP πακέτα κατά την καταγραφή.

2.6.
Δεν υπήρξαν, αφού η διεύθυνση της default gateway, μέσω της οποίας εξυπηρετήθηκε το ping που έτρεξα για μία διεύθυνση διαφορετικού υποδικτύου, βρίσκεται ήδη στον ARP πίνακα του

υπολογιστή μου, επομένως δεν χρειάστηκε να στείλει ή να λάβει κάποιο ARP request ή reply πακέτο.

2.7.
Χρησιμοποίησα το παρακάτω φίλτρο απεικόνισης: *icmp.type == 0.*

2.8.
Για τα ICMP Echo reply πακέτα η τιμή του πεδίου TTL είναι 58. Αρχικά τα reply εκκινούν με TTL ίσο με 64, άρα αυτό σημαίνει πως έκανα συνολικά 6 hops μέχρι να φτάσουν στον υπολογιστή μου, δηλαδή ο στόχος βρίσκεται 6 κόμβους μακριά. Αυτό επιβεβαιώνεται εύκολα και με την εκτέλεση της εντολής $ *tracert 147.102.1.1*, όπου βλέπουμε πως όντως μεσολαβούν 6 κόμβοι μέχρι τον στόχο και για αυτό τα reply φτάνουν με TTL ίσο με 58.

2.9.
Εμφανίζονται μόνο ICMP Echo request μηνύματα.

2.10.
Αυτή τη φορά, επειδή εξυπηρετείται το ping μέσω της default gateway της οποία τη διεύθυνση έχω στον πίνακα ARP του υπολογιστή μου, δεν στέλνεται κάποιο ARP request, όπως στην προηγούμενη φορά. Για αυτό, στέλνονται επιτυχώς τα πακέτα ICMP Echo request, παρόλο που δε λαμβάνω κανέναν πακέτο ICMP Echo reply, αφού ο στόχος είναι ανενεργός και δεν στέλνει κάποια απάντηση. Στην προηγούμενη περίπτωση, τα ICMP Echo request δε στάλθηκαν ποτέ, αφού δεν ήταν γνωστή η διεύθυνση MAC του στόχου στο υποδίκτυο μου και δεν κατάφερε να γνωστοποιηθεί μέσω των ARP request πακέτων. Τέλος, σε αυτήν την περίπτωση στο παράθυρο εντολών βλέπουμε μηνύματα Request timed out, καθώς δεν λαμβάνεται οποιαδήποτε απάντηση στα σταλμένα Echo request, ενώ στην προηγούμενη περίπτωση λαμβάναμε μηνύματα Destination host unreachable από τον υπολογιστή μας, καθώς δεν έπαιρνε κάποια απάντηση στα ARP request του.

Άσκηση 3:

3.1.
Το μήκος και το περιεχόμενο του πεδίου δεδομένων των μνημάτων ICMP Echo request που παράγει η εντολή tracert είναι 64 bytes με περιεχόμενο μηδενικά (0x00).

3.2.
Στην περίπτωση της ping, έχει μήκος 32 bytes και περιεχόμενο τη λατινική αλφάβητο μέχρι και το w και ξανά από την αρχή.

3.3.
Το μήνυμα λάθος στις απαντήσεις των ενδιάμεσων κόμβων είναι το εξής: *Time-to-live exceeded (Time to live exceeded in transit).*

3.4.
Το πεδίο Type έχει τιμή 11 (0x0b, *Time-to-live exceeded*), ενώ το πεδίο Code έχει τιμή 0 (0x00, *Time to live exceeded in transit*).

3.5.
Έχει το πεδίο Checksum με μήκος 2 bytes και το πεδίο Unused με μήκος 4 bytes.

3.6.
Η επικεφαλίδα του μηνύματος λάθους έχει μήκος 8 bytes ενώ τα δεδομένα του έχουν μήκος 92 bytes.

3.7.
Το περιεχόμενο είναι η επικεφαλίδα IPv4 και το ICMP περιεχόμενο του προηγούμενου Echo request πακέτου στο οποίο οφείλεται αυτή η απάντηση με μήνυμα λάθους.

Άσκηση 4:

4.1.
Χρησιμοποίησα την εντολή: $ *ping 147.102.40.15 -f -l <length>*, με μήκη ίσα με 1472, 1464, 978, 548. Οι τιμές αυτές επιλέχθηκαν ώστε μαζί με τα 20 bytes του IPv4 header και τα 8 bytes του ICMP Header να είναι ίσες με τα συνηθισμένα MTU.

4.2.
Ναι, υπήρξε ένα μήνυμα λάθους ICMP *Destination Unreachable*.

4.3.
Αυτό το μήνυμα το παρήγαγε το router μου, αφού η διεύθυνση IPv4 αποστολέα είναι η 192.168.1.1.

4.4.
Το πεδίο Type έχει τιμή 3 (0x03, *Destination unreachable)*, ενώ το πεδίο Code έχει τιμή 4 (0x04, *Fragmentation needed*).

4.5.
Το πεδίο Code με τιμή 4 (0x04, *Fragmentation needed*) δηλώνει ότι πρόκειται για λάθος, λόγω απαίτησης μη θρυμματισμού του πακέτου IPv4. Η τιμή της επικεφαλίδας Next-Hop MTU είναι 1492.

4.6.
Περιέχει την επικεφαλίδα IPv4, την επικεφαλίδα ICMP και 520 από τα 1472 bytes δεδομένων του ICMP Echo request μηνύματος.

4.7.
Η MTU για την οποία δε λαμβάνουμε πρώτη φορά μήνυμα λάθους ICMP *Destination unreachable* είναι η 1492, δηλαδή μήκος δεδομένων ICMP 1464.

4.8.
Το 147.102.40.15 δεν απαντάει, επίσης, για την 1492 (1464) και για την 1006 (978).

4.9.
Λαμβάνω απάντηση πρώτη φορά από το 147.102.40.15 για MTU ίση με 576 (548 μήκος δεδομένων ICMP).

4.10.
Θα πρέπει να ελέγξω έναν ένα τους ενδιάμεσους κόμβους, για να δω εάν η MTU αυτή είναι κάποιου από αυτούς. Τρέχω αρχικά την εντολή: $ *ping 147.102.40.15 -n 1 -r 9* για να καταγράψω τη διαδρομή με τους ενδιάμεσους κόμβους. Έπειτα στέλνω σε κάθε έναν ξεχωριστά ένα ping request με μέγεθος ICMP δεδομένων 978 ώστε να ελέγξω τη μεγαλύτερη τάξη των συνηθισμένων MTU, δηλαδή την 1006, με την εντολή: $ *ping <IPv4> -n 1 -f -l 978.* Το ping λαμβάνει απάντηση σε όλους τους ενδιάμεσους κόμβους και κάνει time out στο στόχο μας, δηλαδή το 147.102.40.15, επομένως η MTU 576 ανήκει στη διεπαφή αυτή.

4.11.
Το 147.102.40.15 δεν είναι υποχρεωμένο να απαντάει με ICMP *Destination Unreachable* μηνύματα, όταν λαμβάνει πακέτα IPv4 μεγέθους μεγαλύτερου από την MTU της διεπαφής του. Μόνο οι δρομολογητές οφείλουν, σύμφωνα με τους κανονισμούς, να απαντούν με τέτοια μηνύματα λάθους σε παρόμοια περίπτωση.

4.12.
Δεν παρατηρώ θρυμματισμό των πακέτων, αλλά μόνο ένα ζευγάρι ICMP Echo request – reply.

Άσκηση 5:

5.1.
Χρησιμοποίησα το παρακάτω φίλτρο σύλληψης: *ip and host 147.102.40.15*.

5.2.
Χρησιμοποίησα την εντολή: $ *nslookup edu-dy.cn.ntua.gr 147.102.40.15*.

5.3.
Έλαβα την παρακάτω απάντηση:

```
C:\Users\george>nslookup edu-dy.cn.ntua.gr 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.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
*** Request to UnKnown timed-out
```

Ουσιαστικά, το αίτημα μας δεν εξυπηρετείται και δεν λαμβάνεται κάποια απάντηση, άρα τυπώνεται μήνυμα time out, αφού περνάνε τα 2 δευτερόλεπτα.

5.4.
Ναι, παρατηρώ 5 μηνύματα DNS.

5.5.
Το πρωτόκολλα μεταφοράς των μηνυμάτων DNS είναι το UDP και η θύρα προορισμού είναι η θύρα 53.

5.6.
Ναι, παρατηρώ 5 μηνύματα λάθους ICMP *Destination unreachable*.

5.7.
Το πεδίο Type έχει τιμή 3 (0x03, *Destination unreachable)*, ενώ το πεδίο Code έχει τιμή 3 (0x03, *Port unreachable*).

5.8.
Το πεδίο Code με τιμή 3 (0x03, *Port unreachable*) δηλώνει ότι ο λόγος αποτυχίας είναι κάποια απρόσιτη θύρα.

5.9.
Εφόσον έχουμε ως θύρα προορισμού του μηνύματος τη θύρα 53, η οποία είναι η προκαθορισμένη θύρα για εξυπηρετητές DNS, καταλαβαίνουμε ότι πρόκειται για τη θύρα προορισμού των μηνυμάτων DNS.

5.10.
Δεν έχω τη δυνατότητα εκτέλεσης της εντολής αυτής, αφού χρησιμοποιώ λειτουργικό Windows.

Άσκηση 6:

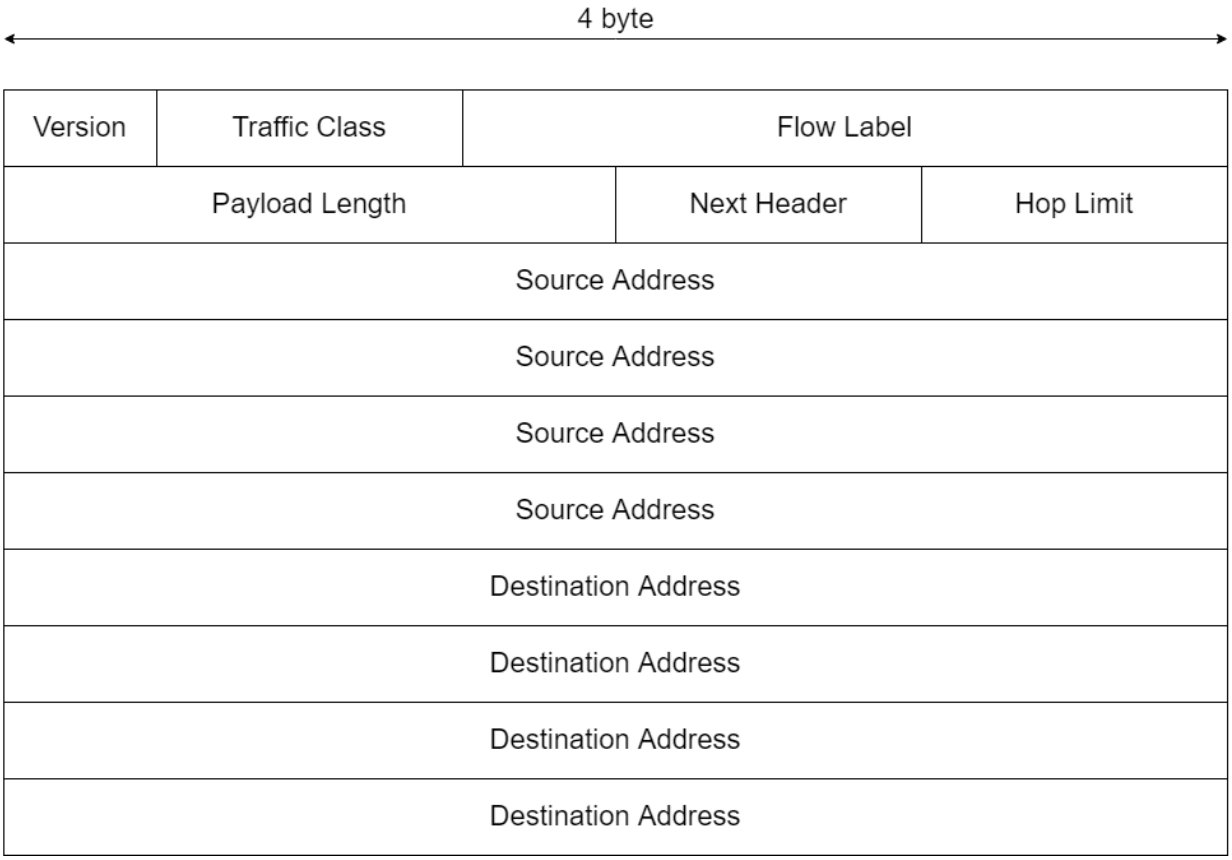
6.1.
Χρησιμοποίησα τις εξής εντολές: *$ ping -6 2001:648:2000:329::101* και *$ tracert -6 2001:648:2000:329::101.*

6.2.
Χρησιμοποίησα το φίλτρο σύλληψης *ip6* και το φίλτρο απεικόνισης *icmpv6.*

6.3.
Το πεδίο Type της επικεφαλίδας Ethernet έχει τιμή 0x86dd (IPv6).

6.4.
Η επικεφαλίδα των πακέτων IPv6 έχει μήκος 40 bytes.

6.5.
Έχουμε τα παρακάτω πεδία (με το αντίστοιχο μήκος σε bits): Version (4), Traffic Class (8), Flow Label (20), Payload Length (16), Next Header (8), Hop Limit (8), Source Address (128), Destination Address (128). Οι θέσεις τους φαίνονται και στο παρακάτω σχήμα:



6.6.
Η επικεφαλίδα Hop Limit (με default τιμή 128 – 0x80) είναι αντίστοιχη της επικεφαλίδας TTL των πακέτων IPv4.

6.7.
Η επικεφαλίδα Next Header με τιμή 58 (0x3a) υποδεικνύει το πρωτόκολλο ICMPv6 τα δεδομένα του οποίου μεταφέρει το πακέτο IPv6.

6.8.
Ναι, είναι ίδια με τη διαφορά ότι έχουμε σκέτο Sequence και όχι Sequence Number.

6.9.
Το πεδίο Type έχει τιμή 128 (0x80, *Echo (ping) request*), ενώ το ICMPv6 Echo request μεταφέρει 32 bytes δεδομένων.

6.10.
Ναι, είναι ίδια με τη δομή του ICMPv6 Echo request.

6.11.
Το πεδίο Type έχει τιμή 129 (0x81, *Echo (ping) reply*), ενώ το ICMPv6 Echo reply μεταφέρει και αυτό 32 bytes δεδομένων.

6.12.
Το ICMPv6 Echo request της tracert διαφέρει στα πεδία Checksum, Sequence και στο μέγεθος των δεδομένων που μεταφέρει (32 vs 64) σε σχέση με το ICMPv6 Echo request της ping.

6.13.
Είναι ίδια με εξαίρεση το τελευταίο πεδίο που έχει όνομα Reserved στο ICMPv6, ενώ στο ICMP έχει όνομα Unused.

6.14.
Το πεδίο Type έχει τιμή 3 (0x03, *Time Exceeded*) και το μήκος των δεδομένων που μεταφέρει είναι 112 bytes.

6.15.
Περιέχει την IPv6 επικεφαλίδα, την ICMP επικεφαλίδα και 64 bytes δεδομένων από το μήνυμα που το προκάλεσε.

6.16.
Παρατήρησα μερικά ακόμα ICMPv6 μηνύματα, όπως τα *Router Advertisement, Neighbor Advertisement* και *Neighbor Solicitation.*

6.17.
Το πεδίο Type έχει τιμή αντίστοιχα 134 (0x86), 136 (0x88), 135 (0x87), ενώ το μήκος αυτών των μηνυμάτων είναι αντίστοιχα 56, 32 και 32 bytes.