Ονοματεπώνυμο: ΔΗΜΗΤΡΙΟΣ ΓΕΩΡΓΟΥΣΗΣ	**ΑΜ: 03119005**	**Ομάδα: 4**
Όνομα PC/ΛΣ: dimitris-Laptop / WINDOWS 11 HOME		**Ημερομηνία: 10/11/2022**
Διεύθυνση IP: 147.102.238.97	**Διεύθυνση MAC: 10-6F-D9-64-91-87**	

1 Εντολή ping στο τοπικό υποδίκτυο

1.1: Φίλτρο σύλληψης: ether host 10:6f:d9:64:91:87

1.2: Φίλτρο απεικόνισης: arp or icmp

1.3: Δεν καταγράφηκαν πακέτα ARP. Αν υπήρχαν, ο ρόλος τους θα ήταν να γίνει η αντιστοίχιση IP και MAC διευθύνσεων. Με έκανε ping πρώτα ο άλλος υπολογιστής οπότε το ARP resolution είχε ήδη συμβεί.

Βρίσκω το πρώτο Echo request του πρωτοκόλλου ICMP.

1.4:

Όνομα Πεδίου	Τιμή
Protocol	1 (ICMP)

1.5: Μήκος επικεφαλίδας ICMP Echo request: 8 bytes

1.6:

Ονόματα	Μήκος	(Για το ICMP Echo request)
Type	1 byte	
Code	1 byte	
Checksum	2 bytes	
Identifier (BE/LE)	2 bytes	
Sequence Number (BE/LE)	2 bytes	

1.7:

Όνομα	Τιμή	(Για το ICMP Echo request)
Type	0x08	
Code	0x00	

1.8:

Όνομα	Τιμή
Identifier (BE)	1
Sequence Number (BE)	4

1.9:

Όνομα	Μήκος	Περιεχόμενο
Data	32 bytes	Τα γράμματα του αγγλικού αλφαβήτου κυκλικά

Βρίσκω το πρώτο Echo reply.

1.10: Μήκος επικεφαλίδας ICMP Echo reply: 8 bytes

Ναι, έχει την ίδια δομή με το Echo request.

1.11:

Όνομα	Τιμή	(Για το ICMP Echo reply)
Type	0x00	
Code	0x00	

1.12:

Το πεδίο Type καθορίζει το είδος του μηνύματος ICMP.	Τιμή	Σημασία
	8	Request
	0	Reply

1.13:

Όνομα	Τιμή
Identifier (BE)	1
Sequence Number (BE)	4

Έχω εντοπίσει τα 2 πακέτα

1.14:

	Request	Reply
Identifier (BE)	1	1
Sequence Number (BE)	4	4

1.15: Τα πεδία αυτά ταυτοποιούν την επικοινωνία δύο υπολογιστών για ανταλλαγή Request – Reply μηνυμάτων.

Ρόλος πεδίου ταυτότητας: Το πεδίο Identifier παραμένει ίδιο για όλα τα μηνύματα του ίδιου ping δείχνοντας ότι ανήκουν όλα στην ίδια απόπειρα επικοινωνίας μας με άλλο σύστημα.

Ρόλος πεδίου αύξοντα αριθμού: Το πεδίο Sequence Number έχει διαφορετικές τιμές (αυξάνει κατά 1) για κάθε ζεύγος Echo Request – Reply ώστε να μπορούμε να ξεχωρίσουμε τα ζεύγη μεταξύ τους και να καταλαβαίνουμε ποια απάντηση αντιστοιχεί σε ποιο αίτημα.

1.16:

Όνομα	Μήκος	Περιεχόμενο
Data	32 bytes	Το ίδιο με το ερώτημα 1.9

1.17: Τα 2 περιεχόμενα δεν διαφέρουν.

1.18:

```
C:\Users\dimig>ping 147.102.236.200

Pinging 147.102.236.200 with 32 bytes of data:
Reply from 147.102.236.200: bytes=32 time=6ms TTL=255
Reply from 147.102.236.200: bytes=32 time=4ms TTL=255
Reply from 147.102.236.200: bytes=32 time=2ms TTL=255
Reply from 147.102.236.200: bytes=32 time=10ms TTL=255
```

Παραπάνω είναι η έξοδος από το ping. Από το πεδίο time και συγκρίνοντας με τους χρόνους στο Wireshark μπορούμε να δούμε ότι τα replies στα αποτελέσματα της εντολής ping στο παράθυρο εντολών ταιριάζουν με τα replies που λάβαμε με σειρά αυξανόμενου Sequence Number.

147.102.238.254

1.19: ping -n 2 -4 147.102.238.254

1.20: Στάλθηκαν 6 ARP requests

1.21: Στέλνονται ανά περίπου 1 second

1.22: Στάλθηκαν 0 μηνύματα ICMP.

1.23: Αποτελέσματα εντολής ping στο παράθυρο εντολών:

C:\Users\dimig>ping -n 2 -4 147.102.238.254

Pinging 147.102.238.254 with 32 bytes of data:
Reply from 147.102.238.97: Destination host unreachable.
Reply from 147.102.238.97: Destination host unreachable.

Ping statistics for 147.102.238.254:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),

Ο προορισμός των ping είναι απρόσιτος με βάση τα pings μας. Αυτό το βλέπουμε από το ότι κανείς δεν απάντησε στα ARP requests μας με βάση τα captured πακέτα από το Wireshark.

2 Εντολή ping σε άλλο υποδίκτυο

Το ερώτημα αυτό πραγματοποιήθηκε αργότερα από τα άλλα. Έχω IP: 147.102.236.35

2.1:

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

Interface: 147.102.236.35 --- 0xa
  Internet Address      Physical Address      Type
  147.102.236.93        60-67-20-88-fc-46     dynamic
  147.102.236.200       08-ec-f5-d0-d9-1d     dynamic
  147.102.236.230       00-50-56-b5-aa-aa     dynamic
  147.102.239.255       ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     static
  224.0.0.5             01-00-5e-00-00-05     static
  224.0.0.13            01-00-5e-00-00-0d     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.113           01-00-5e-00-00-71     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  224.0.1.60            01-00-5e-00-01-3c     static
  224.77.77.77          01-00-5e-4d-4d-4d     static
  230.86.6.15           01-00-5e-56-06-0f     static
  238.238.238.238       01-00-5e-6e-ee-ee     static
  239.192.152.143       01-00-5e-40-98-8f     static
  239.255.102.18        01-00-5e-7f-66-12     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  239.255.255.253       01-00-5e-7f-ff-fd     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 172.23.64.1 --- 0x16
  Internet Address      Physical Address      Type
  172.23.76.33          00-15-5d-02-06-02     static
  172.23.79.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     static
  224.0.0.5             01-00-5e-00-00-05     static
  224.0.0.13            01-00-5e-00-00-0d     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.113           01-00-5e-00-00-71     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  224.0.1.60            01-00-5e-00-01-3c     static
  224.2.2.2             01-00-5e-02-02-02     static
  224.77.77.77          01-00-5e-4d-4d-4d     static
  230.86.6.15           01-00-5e-56-06-0f     static
  238.238.238.238       01-00-5e-6e-ee-ee     static
  239.2.0.251           01-00-5e-02-00-fb     static
  239.2.0.252           01-00-5e-02-00-fc     static
  239.192.152.143       01-00-5e-40-98-8f     static
  239.255.102.18        01-00-5e-7f-66-12     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  239.255.255.253       01-00-5e-7f-ff-fd     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

Το 147.102.1.1 δεν υπάρχει στον πίνακα ARP.

Διαλέγω το πρώτο ICMP Echo request που έστειλα.

		Αποστολέας	Παραλήπτης
2.2:	MAC Address	10:6f:d9:64:91:87	08:ec:f5:d0:d9:1d
2.3:	IPv4 Address	147.102.236.35	147.102.1.1

2.4:

MAC Address	IPv4
10:6f:d9:64:91:87	147.102.236.35
08:ec:f5:d0:d9:1d	147.102.236.200

Η πρώτη MAC Addrerss αντιστοιχεί στην IP της κάρτας μας. Για την 2η MAC Address βρίσκουμε την αντίστοιχη IPv4 από τον πίνακα ARP που έχουμε παραπάνω.

2.5: Όχι

2.6: Δεν υπήρξαν, γιατί το παραπάνω μήνυμα στάλθηκε μέσω του κόμβου 147.102.236.200 η αντιστοιχία του οποίου με MAC Address υπήρχε ήδη στο ARP Table του συστήματός μας.

2.7: Σύνταξη φίλτρου: icmp.type == 0 (Type = 0 στα ICMP Echo reply πακέτα)

2.8: TTL = 63 για όλα τα replies. Η τιμή της παραμέτρου TTL προκύπτει από το πεδίο Time to Live των πακέτων

2.9: Εμφανίζονται μόνο ICMP Echo request

2.10:	Εντός τοπικού δικτύου	Εκτός τοπικού δικτύου
1	Η κίνηση είναι πακέτα ARP request	Η κίνηση είναι πακέτα ICMP Echo request
2	Γνωστοποίησα στον εαυτό μου ότι ο host που αναζητώ είναι unreachable	Τα Echo (ping) requests έκαναν απλά time – out

Η διαφορά αιτιολογείται από το γεγονός ότι όταν προσπαθούμε να συνδεθούμε με διεύθυνση εκτός του τοπικού δικτύου μας, τότε μας απαντά ένας ενδιάμεσος κόμβος (ή αν δεν υπάρχει ο τελικός μας προορισμός τότε δεν θα μας απαντήσει κανείς) ενώ όταν προσπαθούμε να επικοινωνήσουμε με διεύθυνση εντός του τοπικού μας δικτύου τότε στέλνουμε ARP request για να γίνει το MAC Address resolution και αφού δεν παίρνουμε απάντηση μπορούμε να συμπεράνουμε ότι ο host που θέλουμε είναι ανενεργός.

3 Εντολή tracert/traceroute

3.1:

Μήκος	Περιεχόμενο	(Πεδίο Data των ICMP Echo request της tracert)
64 bytes	Όλα μηδενικά	

3.2: Είναι διαφορετικά

3.3: Time-to-live exceeded (Time to live exceeded in transit)

3.4:

Πεδίο	Τιμή
Type	11 (Time-to-live exceeded)
Code	0 (Time to live exceeded in transit)

3.5:

Πεδίο	Μέγεθος
Checksum	2 bytes
Unused	1 byte
Length	1 byte
Unused	2 bytes

(Καταγράφουμε τα πεδία της επικεφαλίδας εκτός από τα Type, Code και πριν του τμήματος που περιέχει όσο το δυνατόν περισσότερο από το ICMP Echo request που στείλαμε αρχικά)

3.6:

	Μήκος
Επικεφαλίδα	8 bytes
Δεδομένα	68 bytes (= Length * 32 / 8 = 17 * 32 / 8 = 68)

3.7: Περιέχει όσο το δυνατόν μεγαλύτερο κομμάτι του αρχικού πακέτου ICMP το οποίο στείλαμε εμείς.

4 Ανακάλυψη MTU διαδρομής (Path MTU Discovery)

4.1: Το MTU θα περιέχει το IPv4 και το ICMP header άρα θα έχουμε buffer_size + 20 + 8 = MTU άρα δίνουμε ως buffer_size = MTU – 28.

Τρέχουμε το εξής script:

```
$Array = 1500,1492,1006,576,552,544,512,508,296
foreach($number in $Array)
{
$mTu = $number - 28
ping -f -4 -n 1 -l $mTu edu-dy.cn.ntua.gr
}
```

Από το παραπάνω script φαίνεται ότι οι τιμές που δίνουμε στην παράμετρο του ping για τον buffer είναι 1472, 1464, 978, 548, 524, 516, 484, 480, 268.

4.2: Όχι
4.3: Δεν παράχθηκε

4.4: Πεδίο Τιμή (ICMP Destination Unreachable)
Type 3 (Destination unreachable)
Code 4 (Fragmentation needed)

4.5: Το πεδίο Code δηλώνει ότι πρέπει να συμβεί θρυμματισμός. Η επικεφαλίδα Next-Hop MTU έχει τιμή 1492 (decimal)

4.6: Το πεδίο των δεδομένων περιέχει όσο το δυνατόν μεγαλύτερο μέρος του πακέτου ICMP Echo request που στείλαμε αρχικά

Τώρα γυρίζουμε στην δική μας καταγραφή (για τα 4.4 έως 4.6 χρησιμοποιήθηκε το mtu.pcap)

4.7: Για MTU = 1500 δεν λαμβάνω μήνυμα λάθους

4.8: Για MTU = 1500, 1492, 1006 δεν παίρνω απάντηση

4.9: Για MTU = 576 παίρνω απάντηση, αλλά και για κάθε μικρότερη τιμή

4.10: Με βάση την παράγραφο 4 του RFC 1191 έχουμε ότι αν κάποιος ενδιάμεσος κόμβος αναγνώριζε ότι το πακέτο δεν μπορεί να προωθηθεί λόγω του μεγέθους του τότε θα μας απαντούσε με ICMP Destination Unreachable μήνυμα. Αυτό όμως δεν συμβαίνει άρα είναι η MTU του edu-dy.cn.ntua.gr [147.102.40.15]

4.11: Το 147.102.40.15 είναι ο τελικός προορισμός, αν λαμβάναμε ICMP Destination Unreachable τότε δεν θα το έστελνε αυτός αλλά κάποιος προηγούμενος κόμβος που θα έβλεπε ότι το MTU στην σύνδεση με αυτόν τον επόμενό του (ή τον τελικό προορισμό) είναι μικρότερο από το μήκος του πακέτου που θέλουμε να στείλουμε

4.12: Το πεδίο fragment offset ενός θραύσματος δείχνει πόσες 8άδες από bytes δεδομένων προηγούνται αυτού. Επομένως πρέπει τα bytes δεδομένων που θα σταλθούν να είναι πολλαπλάσιο του 8, αφού το fragment offset πρέπει να είναι ακέραιος. Θα διαλεχτεί, λοιπόν, το μέγιστο πολλαπλάσιο του 8 που είναι μικρότερο ή ίσο των δεδομένων που μπορούν να μεταφερθούν με MTU = 576. Αρχικά αφαιρούμε την επικεφαλίδα του IPv4 που είναι 20 bytes και έχουμε ότι τα δεδομένα που θα σταλθούν είναι $\left\lfloor \frac{556}{8} \right\rfloor \cdot 8 = 552$ bytes. Βλέπουμε ότι το πρώτο πακέτο που στάλθηκε περιείχε όντως 552 bytes δεδομένων.

5 Απρόσιτη θύρα (Port Unreachable)

Το ερώτημα αυτό το πραγματοποίησα από το σπίτι. Όπου έχω:
IPv4 Address: 192.168.2.6 MAC Address: 7C-8A-E1-C3-47-5C

5.1: Φίλτρο σύλληψης: ip host 147.102.40.15

5.2: Σύνταξη εντολής: nslookup edu-dy.cn.ntua.gr 147.102.40.15

5.3: Στο παράθυρο εντολών λαμβάνουμε απάντηση “DNS request timed out” η οποία σημαίνει

ότι δεν πήραμε απάντηση που να μας βοηθά στην ταυτοποίηση του host, όπως επιθυμούσαμε.

5.4: Ναι
5.5: Το πρωτόκολλο μεταφοράς είναι το UDP και η θύρα προορισμού τους είναι η 53.

5.6: Ναι

5.7:

Πεδίο	Τιμή
Type	3 (Destination unreachable)
Code	3 (Port unreachable)

5.8: Το πεδίο Code

5.9: Η θύρα 53 είναι η πασίγνωστη θύρα την οποία χρησιμοποιεί το DNS Protocol

5.10: Ο προορισμός απαντά με ICMP Destination unreachable (Port unreachable) μήνυμα

6 IPv6 και ICMPv6

Το δίκτυο στο σπίτι μου δεν υποστηρίζει το πρωτόκολλο IPv6, οπότε χρησιμοποιώ την καταγραφή που μας δίνετε.

6.1:

Σύνταξη ping:	ping -6 2001:0648:2000:0329:0000:0000:0000:0101
Σύνταξη tracert:	tracert -6 2001:0648:2000:0329:0000:0000:0000:0101

6.2:

Φίλτρο σύλληψης:	ip6
Φίλτρο απεικόνισης:	icmpv6

6.3: Type (Επικεφαλίδα Ethernet όταν μεταφέρονται πακέτα IPv6) = 0x86dd

6.4: Μήκος IPv6 Header = 40 bytes

6.5:

Πεδίο	Μήκος
Version	4 bits
Traffic Class	1 byte
Flow Label	20 bits
Payload Length	2 bytes
Next Header	1 byte
Hop Limit	1 byte
Source Address	16 bytes
Destination Address	16 bytes

6.6: Η Hop Limit

6.7: Η Next Header και για ICMPv6 η τιμή της είναι 58 (0x3a)

6.8: Η δομή είναι ίδια με το ICMP Echo request

6.9: Type = 128 (0x80) και Data έχουν μήκος 32 bytes
6.10: Ναι

6.11: Type = 129 (0x81) και Data έχουν μήκος 32 bytes

6.12: Διαφέρει στα Checksum και Sequence πεδία, ενώ μεταφέρει 64 bytes Data αντί για 32 bytes που ήταν στο ping

6.13: Η δομή δεν είναι ίδια. Στο ICMPv6 το πεδίο Length προηγείται των reserved byte ενώ στο ICMP ήταν ανάμεσα σε 1 και 2 Unused bytes

6.14: Type = 3 (0x03) (Time Exceeded) και μεταφέρει 112 bytes δεδομένων

6.15: Το πεδίο των δεδομένων του περιέχει το αρχικό ICMPv6 Echo request που έστειλε ο υπολογιστής μας

6.16: Παρατηρούμε μηνύματα Neighbor Solicitation και Neighbor Advertisement

6.17:

Είδος Μηνύματος	Type
Neighbor Solicitation	135
Neighbor Advertisement	136

Το μήκος των μηνυμάτων αυτών είναι 32 bytes