Ονοματεπώνυμο: ΔΗΜΗΤΡΙΟΣ ΓΕΩΡΓΟΥΣΗΣ	**ΑΜ: 03119005**	**Ομάδα: 4**
Όνομα PC/ΛΣ: dimitris-Laptop / WINDOWS 11 HOME		**Ημερομηνία: 21/10/2022**
Διεύθυνση IP: 192.168.2.6	**Διεύθυνση MAC: 7C-8A-E1-C3-47-5C**	

Άσκηση 1:

1.1: Εντολή που βλέπουμε τα περιεχόμενα του πίνακα ARP: arp – a

1.2: Εντολή διαγραφής περιεχομένων πίνακα ARP: arp – d με administrative rights

1.3: IPV4 Default Gateway: 192.168.2.1
IPV4 DNS: 192.168.2.1

Χρησιμοποιήσαμε την εντολή ipconfig/all και πήγαμε στη κάρτα δικτύου μας για να πάρουμε τις πληροφορίες αυτές.

1.4: Περιεχόμενο πίνακα ARP υπολογιστή μου: (αποτέλεσμα εκτέλεσης εντολής arp -a)

Index			
1	Interface: 192.168.2.6 --- 0x8		
2	Internet Address	Physical Address	Type
3	192.168.2.1	60-ce-86-04-52-c8	dynamic
4	192.168.2.3	8c-19-b5-69-40-f2	dynamic
5	224.0.0.2	01-00-5e-00-00-02	static
6	224.0.0.22	01-00-5e-00-00-16	static
7	224.0.0.251	01-00-5e-00-00-fb	static
8	224.0.0.252	01-00-5e-00-00-fc	static
9	239.255.255.250	01-00-5e-7f-ff-fa	static
10			
11	Interface: 192.168.56.1 --- 0x9		
12	Internet Address	Physical Address	Type
13	224.0.0.22	01-00-5e-00-00-16	static
14	224.0.0.251	01-00-5e-00-00-fb	static
15	239.255.255.250	01-00-5e-7f-ff-fa	static

1.5: Υπάρχουν στον πίνακα οι διευθύνσεις του default gateway και του DNS:

Στον παραπάνω πίνακα ψάχνουμε την IP 192.168.2.1. Την εντοπίζουμε στην γραμμή 3. Ο πίνακας ARP περιέχει την διεύθυνση του default gateway και του DNS. (Στον υπολογιστή μου ταυτίζονται)

1.6: Η μόνη διεύθυνση που επέστρεψε κάποια απάντηση ήταν η 192.168.2.3.

Pinging 192.168.2.3 with 32 bytes of data:
Reply from 192.168.2.6: Destination host unreachable.
Reply from 192.168.2.6: Destination host unreachable.
Reply from 192.168.2.6: Destination host unreachable.
Reply from 192.168.2.6: Destination host unreachable.

Ping statistics for 192.168.2.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Ο host ήταν unreachable όμως…

1.7: Καταγραφή πίνακα ARP:

Interface: 192.168.2.6 --- 0x8

Internet Address	Physical Address	Type
192.168.2.1	60-ce-86-04-52-c8	dynamic
224.0.0.2	01-00-5e-00-00-02	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: 192.168.56.1 --- 0x9

Internet Address	Physical Address	Type
224.0.0.2	01-00-5e-00-00-02	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

Δοκίμασα να κάνω ping και τις υπόλοιπες IPs του πίνακα ARP από το ερώτημα 1.4.
Η διεύθυνση 192.168.2.3 δεν υπάρχει.

1.8: Καταγραφή πίνακα ARP μετά την πρόσβαση στη σελίδα http://edu-dy.cn.ntua.gr/lab3/ :

Interface: 192.168.2.6 --- 0x8

Internet Address	Physical Address	Type
192.168.2.1	60-ce-86-04-52-c8	dynamic
224.0.0.2	01-00-5e-00-00-02	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: 192.168.56.1 --- 0x9

Internet Address	Physical Address	Type
224.0.0.2	01-00-5e-00-00-02	static
224.0.0.22	01-00-5e-00-00-16	static
239.255.255.250	01-00-5e-7f-ff-fa	static

Βλέπουμε την διεύθυνση του default gateway.

1.9: Έχει καταχωρηθεί η IPV4 του edu-dy.cn.ntua.gr στην πίνακα ARP:

Αρχικά πρέπει να προσδιορίσουμε την IPV4 του edu-dy.cn.ntua.gr. Το κάνουμε εκτελώντας την εντολή ‘‘tracert edu-dy.cn.ntua.gr’’ και από τα αποτελέσματα βλέπουμε ότι η IP που θέλουμε είναι 147.102.40.15

Η IP αυτή δεν υπάρχει στον πίνακα ARP. Αυτό είναι αναμενόμενο, αφού η επίλυση διευθύνσεων MAC αφορά μόνο τοπικά υποδίκτυα, και το edu-dy.cn.ntua.gr δεν ανήκει στο τοπικό δίκτυο του υπολογιστή μας.

Άσκηση 2:

2.1: Πεδία επικεφαλίδας Ethernet: Destination, Source, Type.

2.2: Το προοίμιο δεν καταγράφεται. Είναι πληροφορία που χρησιμοποιείται από την κάρτα δικτύου για να καταλάβει πότε ένα πλαίσιο πρόκειται να ξεκινήσει.

2.3: Το CRC δεν καταγράφεται. Το CRC περιέχει πληροφορία που βοηθάει την κάρτα δικτύου να επιβεβαιώσει την ακεραιότητα του πλαισίου.

2.4: Type (IPV4) = 0x0800

2.5: Type (ARP) = 0x0806

2.6: Type (IPV6) = 0x86dd (στο οικιακό περιβάλλον δεν έχω την δυνατότητα χρήσης IPV6, είχα κάνει όμως ένα Capture από έναν υπολογιστή της σχολής.

2.7: MAC Source: 7c:8a:e1:c3:47:5c (κάρτα δικτύου μου)

2.8: MAC Destination: 60:ce:86:04:52:c8

2.9: Η παραπάνω MAC Address δεν είναι η MAC του edu-dy.cn.ntua.gr.
Το διαπιστώνουμε κοιτώντας τον πίνακα arp (arp -a εντολή) και βλέποντας ότι η MAC Address αυτή υπάρχει σε καταχώρηση του πίνακα.

2.10: Ανήκει στην συσκευή με IPV4 = 192.168.2.1, όπως βλέπουμε και από τους πίνακες που έχουμε δείξει σε προηγούμενα ερωτήματα. Είναι το MAC Address του default gateway.

2.11: Μήκος πλαισίου σε bytes = 491 bytes

2.12: Προηγούνται 16*3 + 6 = 54 bytes

2.13: MAC Αποστολέα: 60:ce:86:04:52:c8

2.14: Η παραπάνω MAC Address δεν είναι αυτή του edu-dy.cn.ntua.gr.

2.15: Είναι η MAC Address του default gateway.

2.16: MAC παραλήπτη: 7c:8a:e1:c3:47:5c

2.17: Ανήκει στον υπολογιστή μου.

2.18: Μήκος πλαισίου σε byte: 584 bytes

2.19: Bytes που προηγούνται του ‘‘O’’: 4*16 + 3 = 67 bytes.

Ένας τρόπος να το υπολογίσουμε είναι: πάμε στο σημείο που είναι το ‘‘O’’ στο Wireshark και μετράμε πόσα bytes προηγούνται. Άλλος τρόπος είναι:
Ethernet Header + IP Header + TCP Header + bytes(“HTTP/1.1 200 ’’) = 14 + 20 + 20 + 13 = 67 bytes

Άσκηση 3:

3.1: MAC πηγής πλαισίων: 60:ce:86:04:52:c8. Globally unique address και Individual Address, δηλαδή, μοναδική και ατομική διεύθυνση.

3.2: MAC προορισμού πλαισίων: ff:ff:ff:ff:ff:ff. Locally administered address και Group Address, δηλαδή, τοπική και ομαδική διεύθυνση.

Τις παραπάνω πληροφορίες μας δίνει το Wireshark από τα πεδία Source και Destination ενός πακέτου.

3.3: Τα byte μεταδίδονται από LSB προς MSB. Οπότε αν η ερώτηση εννοεί γενικά σε ποια θέση βρίσκεται το πρώτο bit μιας MAC Address στο πρώτο της byte τότε είναι το MSB. Αν η ερώτηση εννοεί σε ποια θέση βρίσκεται το πρώτο bit μιας MAC Address στο πρώτο της byte, το οποίο λαμβάνει κάποιος, τότε η απάντηση είναι: στο LSB.

3.4: ff:ff:ff:ff:ff:ff

3.5: Παραμένουν πλαίσια IEEE 802.3 Ethernet.

3.6: Πεδίο μετά τις MAC διευθύνσεις: Length: πλήθος ενθυλακωμένων byte (για να μπορούμε να καταλάβουμε πόσα bytes στο τέλος του πακέτου αποτελούν το padding).

3.7: Αν το πεδίο Type/Length έχει τιμή >= 1536 τότε είναι Type και το πλαίσιο είναι Ethernet II
Αν το πεδίο αυτό έχει τιμή <= 1500 τότε είναι Length και το πλαίσιο είναι IEEE 802.3 Ethernet.

3.8: Επικεφαλίδα LLC:
Πεδία: DSAP (1 byte)
SSAP (1 byte)
Control field (1 byte)
Μέγεθος: 3 bytes

3.9: Μεταφέρουν δεδομένα πρωτοκόλλου STP. Τα δεδομένα αυτού του πρωτοκόλλου έχουν μέγεθος 36 bytes.

3.10: Το padding έχει μέγεθος 7 byte. Το ελάχιστο μέγεθος του πακέτου είναι 60 bytes (χωρίς τα CRC bytes). Εδώ 14 bytes είναι η επικεφαλίδα και από το πεδίο length 39 bytes είναι τα ενθυλακωμένα δεδομένα άρα 60 – 14 – 39 = 7 bytes απαιτούνται ακόμα για να αποκτήσει το πακέτο το ελάχιστο μέγεθός του. Τα 7 αυτά bytes είναι το padding και είναι όλα μηδενικά.

Άσκηση 4:

4.1: Έχει αποτέλεσμα να εμφανίζονται μόνο πακέτα που έχουν πηγή ή προορισμό τον υπολογιστή μου.

4.2: Εμφανίζονται μόνο τα πακέτα πρωτοκόλλου ARP που έστειλα ή έλαβα.

4.3: 2 πακέτα ARP μόνο.

4.4: Το πεδίο Type έχει διαφορετική τιμή.

4.5:

<table>
<tr><td colspan="2">Hardware type (2 bytes)</td><td>Protocol type (2 bytes)</td></tr>
<tr><td>Hardware size (1 byte)</td><td>Protocol size (1 byte)</td><td>Opcode request (2 bytes)</td></tr>
<tr><td colspan="3">Sender MAC address (first 4 bytes)</td></tr>
<tr><td colspan="2">Sender MAC address (other 2 bytes)</td><td>Sender IP address (first 2 bytes)</td></tr>
<tr><td colspan="2">Sender IP address (first 2 bytes)</td><td>Target MAC address (first 2 bytes)</td></tr>
<tr><td colspan="3">Target MAC address (other 4 bytes)</td></tr>
<tr><td colspan="3">Target IP address (4 bytes)</td></tr>
</table>

4.6: Hardware type = 0x0001. Υποδεικνύει κάρτα Ethernet.

4.7: Protocol type = 0x0800. Υποδεικνύει πρωτόκολλο IPV4.

4.8: Μπορούν να πάρουν τιμές από το ίδιο σύνολο τιμών.

4.9: Το πεδίο Protocol size δείχνει το μέγεθος της διεύθυνσης του πρωτοκόλλου του πεδίου Protocol type σε byte. Το πρωτόκολλο είναι IPV4 και οι διευθύνσεις IPV4 είναι 4 bytes.

4.10: Το πεδίο Hardware size δείχνει το μέγεθος της διεύθυνσης του πρωτοκόλλου του πεδίου Hardware Type σε byte. Το πρωτόκολλο είναι Ethernet και οι MAC διευθύνσεις είναι 6 bytes.

Διαλέγουμε πακέτο με το μήνυμα “Who has 192.168.2.1? Tell 102.168.2.6”

4.11: Sender MAC Address του ARP request: 7c:8a:e1:c3:47:5c, διεύθυνση MAC της κάρτας δικτύου του υπολογιστή μου.

4.12: Παραλήπτης του πλαισίου αυτού:

```
> Frame 47: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF
> Ethernet II, Src: CompalIn_c3:47:5c (7c:8a:e1:c3:47:5c), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
v Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: CompalIn_c3:47:5c (7c:8a:e1:c3:47:5c)
    Sender IP address: 192.168.2.6
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 192.168.2.1
```

Παρατηρούμε αυτό το αποτέλεσμα. Το πακέτο ethernet έχει στο πεδίο destination την τιμή ff:ff:ff:ff:ff:ff, την οποία αναμέναμε. Ωστόσο, το ARP πακέτο έχει στο Target MAC address όλα μηδενικά. Μάλλον, για αυτό ευθύνεται ότι το πακέτο δεν είναι κανονικό ARP, στο οποίο οι 2 τιμές θα ταυτίζονταν αλλά είναι Gratuitous ARP το οποίο ορίζει την τιμή αυτή για το πεδίο Target MAC Address.

4.13: Συνολικό μήκος πακέτου ARP: 28 bytes
Συνολικό μήκος πλαισίου Ethernet που το μεταφέρει: 42 bytes

4.14: Bytes στο πλαίσιο Ethernet που προηγούνται του πεδίου Opcode:
Ethernet Header + 2 + 2 + 1 + 1 = 14 + 6 = 20 bytes

4.15: Opcode(ARP request) = 0x0001

4.16: Πεδίο MAC(Sender) στο πακέτο ARP request: Sender MAC address

4.17: Sender IP address

4.18: Target IP address

4.19: Target MAC address. Έχει την τιμή 00:00:00:00:00:00.

Εντοπίζουμε το ARP reply σε αυτό το request.

4.20: Source MAC = 60:ce:86:04:52:c8 (ανήκει στο default gateway)
Destination MAC = 7c:8a:e1:c3:47:5c (ανήκει στην κάρτα δικτύου του υπολογιστή μου)

4.21: Opcode(ARP reply) = 0x0002

4.22: Sender IP address

4.23: Sender MAC address

4.24: Target IP address

4.25: Target MAC address

4.26: Μέγεθος ARP reply = 28 bytes
Μέγεθος Ethernet frame = 60 bytes

4.27: Το μέγεθος των ARP πακέτων είναι ίδια, ωστόσο, τα πλαίσια Ethernet έχουν διαφορετικά μεγέθη.

4.28: Το πεδίο Opcode υποδεικνύει αν πρόκειται για request ή reply.

4.29: Στο Wireshark εμφανίζει τα extra bytes του reply ως ‘‘Trailer’’ πεδίο στο Ethernet II. Το Ethernet έχει ελάχιστο μέγεθος 60 bytes. Το Wireshark στα εισερχόμενα πλαίσια, αφού γνωρίζει ότι είναι ARP, δεν μας δείχνει το trailer δεδομένων στο τέλος του πλαισίου. Ωστόσο, συλλαμβάνει τα απερχόμενα πλαίσια προτού μεταδοθούν. Έτσι συλλαμβάνει και τα «συμπληρωματικά» bytes που μπαίνουν στο τέλος.

4.30: Arp request: ατομική διεύθυνση για την πηγή και ομαδική διεύθυνση για τον προορισμό
Arp reply: ατομική διεύθυνση για πηγή και προορισμό

4.31: Οι υπολογιστές του τοπικού δικτύου συσχετίζουν κάθε άλλη IP address του δικτύου αυτού με την MAC address του κακόβουλου υπολογιστή. Συνεπώς, όταν θέλουν να στείλουν κάτι στο τοπικό δίκτυο το στέλνουν στην πραγματικότητα σε αυτόν. Έτσι, ο κακόβουλος αυτός υπολογιστής λαμβάνει όλα τους τα πλαίσια (ARP spoofing).