Δίκτυα Υπολογιστών
Εργαστηριακή Άσκηση 3

Ονοματεπώνυμο: Κυριακόπουλος Γεώργιος – el18153
Ομάδα: 4
Όνομα PC/ΛΣ: George – Windows 10 Pro, 21H1
Ημερομηνία: 1/11/2021
Διεύθυνση IP: 192.168.1.8
Διεύθυνση MAC: 60-A4-B7-75-72-0F

Άσκηση 1:

1.1.
Με χρήση της εντολής *$ arp -a* μπορούμε να δούμε τα περιεχόμενα του ARP πίνακα.

1.2.
Με χρήση της εντολή *$ netsh interface ip delete arpcache* μπορούμε να διαγράψουμε τα περιεχόμενα του ARP πίνακα, καθώς η εντολή *$ arp -d* δεν φαίνεται να δουλεύει στον υπολογιστή μου.

1.3.
Με χρήση της εντολή *$ ipconfig /all* βρίσκω τις διευθύνσεις IPv4 της προκαθορισμένης πύλης (Default Gateway) και των εξυπηρετητών DNS του υπολογιστή μου, που είναι αντίστοιχα 192.168.1.1 και 192.168.1.1, δηλαδή ίδιες (η διεύθυνση του router μου).

1.4.
Interface: 192.168.1.8 --- 0x16

Internet Address	Physical Address	Type
192.168.1.1	98-3b-67-9a-54-70	dynamic
192.168.1.5	bc-7f-a4-1f-96-31	dynamic
192.168.1.7	50-56-bf-07-1b-4b	dynamic
192.168.1.255	ff-ff-ff-ff-ff-ff	static
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

1.5.
Υπάρχει η διεύθυνση 192.168.1.1 που λειτουργεί και ως προκαθορισμένη πύλη και ως εξυπηρετητής DNS στον υπολογιστή μου, άρα υπάρχει η διεύθυνση και των δύο στον πίνακα ARP.

1.6.
Χρησιμοποίησα τη διεύθυνση 192.168.1.5 και έλαβα απάντηση.

1.7.
Παρατηρώ ότι στον πίνακα έχει προστεθεί και πάλι το ζευγάρι 192.168.1.5 με την αντίστοιχη Physical Address (MAC address).

1.8.
Έχει προστεθεί η διεύθυνση 192.168.1.1 που αποτελεί τόσο τη διεύθυνση της προκαθορισμένης πύλης όσο και του εξυπηρετητή DNS. Αφού καθαρίσαμε τόσο τη DNS cache όσο και τον πίνακα ARP, τότε αρχικά πρέπει μέσω του DNS να βρούμε την IPv4 διεύθυνση του edu-dy.cn.ntua.gr. Έπειτα, πρέπει να γίνει ο έλεγχος εάν αυτή η διεύθυνση IPv4 ανήκει στο υποδίκτυο που βρίσκεται και ο υπολογιστής μας, οπότε θα μαθαίναμε μέσω του ARP τη διεύθυνση MAC του, ή εάν ανήκει σε άλλο υποδίκτυο, οπότε θα μαθαίναμε τη διεύθυνση του δρομολογητή που θα μας οδηγήσει στο υποδίκτυο που ανήκει η διεύθυνση IPv4 του edu-dy.cn.ntua.gr. Για αυτό, χρειάστηκε να έρθουμε σε επικοινωνία με τον εξυπηρετητή DNS και με την προκαθορισμένη πύλη.

1.9.
Όχι, αφού το edu-dy.cn.ntua.gr δεν ανήκει στο ίδιο υποδίκτυο με τον υπολογιστή μας.

Άσκηση 2:

2.1.
Το Wireshark καταγράφει τα πεδία MAC destination, MAC source, Ethertype (Ethernet II).

2.2.
Δεν έχει καταγραφεί, διότι αυτά τα bits (preamble + start frame delimiter) έχουν αφαιρεθεί από το πλαίσιο μέσω της κάρτας δικτύου στο πρώτο επίπεδο (φυσικό επίπεδο), ενώ τα packet sniffer προγράμματα, όπως το Wireshark, λαμβάνουν τα δεδομένα τους από το 2ο επίπεδο, το επίπεδο ζεύξης δεδομένων.

2.3.
Το CRC μήκους 32-bit ή αλλιώς FCS, ομοίως με το προοίμιο, δεν καταγράφεται. Για να γίνει αυτό, πρέπει να το επιτρέπει το λειτουργικό σύστημα, να μπορεί να γίνει κάποια αντίστοιχη τροποποίηση σε αυτό, να γίνει τροποποίηση στη βιβλιοθήκη που χρησιμοποιείται για την καταγραφή των πλαισίων και στο να γίνει τροποποίηση και στο πρόγραμμα που χρησιμοποιείται.

2.4.
Η τιμή του πεδίου Type για πακέτα IPv4 είναι 0x0800.

2.5.
Η τιμή του πεδίου Type για πακέτα ARP είναι 0x0806.

2.6.
Η τιμή του πεδίου Type για πακέτα IPv6 είναι 0x86dd.

2.7.
Η διεύθυνση MAC πηγής (MAC source) είναι η 60:a4:b7:75:72:0f (του υπολογιστή μου).

2.8.
Η διεύθυνση MAC προορισμού (MAC destination) είναι η 98:3b:67:9a:54:70.

2.9.
Όχι, δεν είναι η διεύθυνση MAC του edu-dy.cn.ntua.gr.

2.10.
Η διεύθυνση αυτή αποτελεί τόσο τη διεύθυνση της προκαθορισμένης πύλης, όσο και του εξυπηρετητή DNS του υπολογιστή μου (το router μου και στις δύο περιπτώσεις). Αυτό συμβαίνει διότι το edu-dy.cn.ntua.gr δεν ανήκει στο υποδίκτυο που είναι άμεσα συνδεδεμένος ο υπολογιστής μου και επομένως χρειάζεται να έρθει σε επικοινωνία με το router ώστε να προωθηθεί το αίτημα αυτό μέσω του δρομολογητή, στο κατάλληλο υποδίκτυο που θα το εξυπηρετήσει.

2.11.
Το μήκος του πλαισίου είναι 493 bytes.

2.12.
Προηγούνται 54 bytes πριν από το χαρακτήρα ASCII “G” της λέξης GET.

2.13.
Η διεύθυνση MAC του αποστολέα (MAC source) είναι η 98:3b:67:9a:54:70.

2.14.
Όχι, δεν είναι η διεύθυνση MAC του edu-dy.cn.ntua.gr.

2.15.
Αυτή η διεύθυνση ανήκει στο router μου, καθώς από αυτό επιστρέφεται η απάντηση για το αίτημα GET που έστειλε ο υπολογιστής μου. Αυτό λειτουργεί ως προκαθορισμένη πύλη και ως εξυπηρετητής DNS.

2.16.
Η διεύθυνση MAC του παραλήπτη (MAC destination) είναι η 60:a4:b7:75:72:0f.

2.17.
Η διεύθυνση αυτή ανήκει στον υπολογιστή μου, που είναι ο παραλήπτης της απάντησης του GET αιτήματος.

2.18.
Το μήκος του πλαισίου είναι 536 bytes.

2.19.
Προηγούνται 67 bytes πριν από το χαρακτήρα ASCII “O” της λέξης OK.

Άσκηση 3:

3.1.
Οι διευθύνσεις MAC πηγής των πλαισίων Ethernet είναι όλες ατομικές (unicast) και παγκοσμίως μοναδικές.

3.2.
Οι διευθύνσεις MAC προορισμού των πλαισίων Ethernet είναι όλες ομαδικές (multicast) και τοπικές.

3.3.
Γενικά γνωρίζουμε πως η μετάδοση των byte γίνεται από αριστερά προς τα δεξιά και για κάθε byte πρώτα μεταδίδεται το λιγότερο σημαντικό bit (LSB)και τελευταίο το περισσότερο σημαντικό bit (MSB). Επομένως, για τη διεύθυνση MAC, όταν μεταδίδεται το πρώτο της byte (το πρώτο από αριστερά), πρώτα θα μεταδοθούν τα δύο IG και LG bits που είναι αυτά τα οποία μας δείχνουν αυτό που ζητήθηκε στο ερώτημα 3.2. Άρα το πρώτο bit της διεύθυνσης MAC θα βρίσκεται στην 8η θέση και το δεύτερο bit στην 7η.

3.4.
Η διεύθυνση MAC των πλαισίων εκπομπής είναι η ff:ff:ff:ff:ff:ff.

3.5.
Παραμένουν μόνο πλαίσια με τύπο IEEE 802.3 Ethernet και όχι Ethernet II.

3.6.
Το πεδίο Length μετά τις διευθύνσεις MAC στα πλαίσια IEEE 802.3 δηλώνει το μήκος των δεδομένων (payload) σε bytes.

3.7.
Τα δύο αυτά είδη πλαισίων ξεχωρίζουν από το περιεχόμενο του πεδίου μετά τις δύο διευθύνσεις MAC (destination και source). Αυτό το πεδίο (με όνομα EtherType για Ethernet II πλαίσια και Length για IEEE 802.3), εάν έχει τιμή από 1500 και κάτω, πρόκειται για IEEE 802.3 πλαίσιο και υποδηλώνει το μήκος του σε bytes, ενώ εάν έχει τιμή από 1536 και πάνω, πρόκειται για Ethernet II πλαίσιο και υποδηλώνει τον τύπο του πρωτοκόλλου που είναι ενθυλακωμένο στα δεδομένα.

3.8.
Η επικεφαλίδα LLC (Logical-Link Control) έχει μέγεθος 3 bytes και περιέχει τα πεδία DSAP, SSAP, Control field.

3.9.
Μεταφέρουν δεδομένα του Spanning Tree Protocol και έχουν μήκος 60 bytes.

3.10.
Το παραγέμισμα (padding) έχει μέγεθος 7 bytes και υπάρχει για να φτάσει το κομμάτι των δεδομένων το ελάχιστο μέγεθος των 46 bytes. Εδώ, το LLC έχει μέγεθος 3 byte και το Spanning

Tree Protocol έχει μέγεθος 36 bytes, άρα 39 bytes σύνολο το data field. Επομένως, χρειάζονται 7 bytes padding για να φτάσει το ελάχιστο των 46 bytes.

Άσκηση 4:

4.1.
Εμφανίζονται στη λίστα όλα τα πλαίσια που έχουν την MAC Address της κάρτας δικτύου μου είτε ως διεύθυνση MAC πηγής (MAC source), είτε ως διεύθυνση MAC προορισμού (MAC destination).

4.2.
Από τα προηγούμενα πλαίσια, τώρα εμφανίζονται μόνο αυτά που έχουν ως πρωτόκολλο το ARP.

4.3.
Ανταλλάχθηκαν 2 πακέτα ARP. Μία ερώτηση και μία απάντηση.

4.4.
Το πεδίο Type διαφοροποιεί τα ARP πακέτα από τα IPv4, καθώς έχει διαφορετική τιμή, υποδηλώνοντας τη χρήση του συγκεκριμένου πρωτόκολλου (ARP = 0x0806 και IPv4 = 0x0800).

4.5.
Τα ονόματα των πεδίων του πακέτου ARP είναι Hardware type, Protocol type, Hardware size, Protocol Size, Opcode, Sender MAC address, Sender IP address, Target MAC address, Target IP address. Τα αντίστοιχα μήκη των πεδίων αυτών σε bytes είναι: 2, 2, 1, 1, 2, 6, 4, 6, 4.

4.6.
Η τιμή του πεδίου Hardware type είναι 0x0001 και υποδεικνύει κάρτα δικτύου υλικού Ethernet.

4.7.
Η τιμή του πεδίου Protocol type είναι 0x0800 και υποδεικνύει το IPv4 πρωτόκολλο.

4.8.
Το πεδίο Protocol type του ARP και το πεδίο Ethertype του Ethernet II δέχονται παρόμοιες τιμές στα ορίσματα τους σχετικά με το ποιο πρωτόκολλο χρησιμοποιούν τα δεδομένα τους.

4.9.
Το Protocol size δηλώνει το μήκος των διευθύνσεων που χρησιμοποιεί το πρωτόκολλο του πεδίου Protocol type, που στην περίπτωση μας είναι το IPv4, το οποίο χρησιμοποιεί διευθύνσεις μήκους 4 bytes (IPv4).

4.10.
Το Hardware size δηλώνει το μήκος των διευθύνσεων που χρησιμοποιεί το υλικό της κάρτας δικτύου του πεδίου Hardware type, που στην περίπτωση μας είναι το Ethernet, το οποίο χρησιμοποιεί διευθύνσεις μήκους 6 bytes (MAC).

4.11.
Η διεύθυνση MAC αποστολέα του πλαισίου Ethernet ανήκει στο router μου.

4.12.
Η διεύθυνση MAC παραλήπτη του πλαισίου Ethernet είναι η 60:a4:b7:75:72:0f και ανήκει στον υπολογιστή μου.

4.13.
Το πακέτο ARP request έχει μέγεθος 28 bytes, ενώ το πλαίσιο Ethernet που το μεταφέρει έχει μέγεθος 60 bytes.

4.14.
Πριν το πεδίο opcode στο ARP request προηγούνται 20 bytes από το πλαίσιο Ethernet.

4.15.
Η τιμή του πεδίου opcode στο ARP request είναι 1 (0x0001).

4.16.
Στο πεδίο Sender MAC address περιέχεται η διεύθυνση MAC του αποστολέα.

4.17.
Στο πεδίο Sender IP address περιέχεται η διεύθυνση IPv4 του αποστολέα.

4.18.
Στο πεδίο Target IP address περιέχεται η διεύθυνση IPv4 της οποία τη διεύθυνση MAC αναζητάει το request.

4.19.
Υπάρχει τέτοιο πεδίο, με όνομα Target MAC address το οποίο έχει την default διεύθυνση MAC 00:00:00:00:00:00.

4.20.
Η διεύθυνση MAC αποστολέα του πλαισίου Ethernet ανήκει στον υπολογιστή μου, ενώ του παραλήπτη ανήκει στο router μου.

4.21.
Η τιμή του πεδίου opcode στο ARP reply είναι 2 (0x0002).

4.22.
Στο πεδίο Sender IP address περιέχεται η διεύθυνση IPv4 του αποστολέα.

4.23.
Στο πεδίο Sender MAC address περιέχεται η διεύθυνση MAC του αποστολέα.

4.24.
Στο πεδίο Target IP address περιέχεται η διεύθυνση IPv4 της οποία τη διεύθυνση MAC αναζητούσε το request.

4.25.
Στο πεδίο Target MAC address περιέχεται η διεύθυνση MAC την οποία αναζητούσε το request και αποτελεί η απάντηση (reply) στο ερώτημα αυτό.

4.26.
Το πακέτο ARP request έχει μέγεθος 28 bytes, ενώ το πλαίσιο Ethernet που το μεταφέρει έχει μέγεθος 42 bytes.

4.27.
Το μέγεθος του ARP reply είναι το ίδιο με το μέγεθος του ARP request, ενώ τα πλαίσια Ethernet έχουν διαφορετικό μέγεθος.

4.28.
Το πακέτο ARP request προέρχεται από το router και κατευθύνεται στον υπολογιστή μου. Επομένως, όταν καταγράφεται από το Wireshark, έχει ήδη περάσει από την προσθήκη του padding στο Ethernet hardware του αποστολέα και για αυτό το Wireshark το καταγράφει μαζί με το padding του. Σε αντίθεση, το πακέτο ARP reply προέρχεται από τον υπολογιστή μου και κατευθύνεται στο router. Επομένως, όταν καταγράφεται από το Wireshark, δεν έχει περάσει από το Ethernet hardware του αποστολέα (του υπολογιστή μου), δηλαδή δεν έχει προστεθεί το padding και για αυτό το Wireshark το καταγράφει χωρίς το padding του. Για αυτό, έχει μέγεθος μειωμένο κατά τα 18 bytes που αποτελούν το padding στο ARP request.

4.29.
Το πεδίο opcode μας υποδεικνύει εάν πρόκειται για πακέτο ARP request (με τιμή 1 - 0x0001) ή για πακέτο ARP reply (με τιμή 2 - 0x0002).

4.30.
Οι μόνες διαφορές που εντοπίζω είναι το γεγονός ότι έχουν διαφορετικό opcode, 1 (0x0001) το request και 2 (0x0002) το reply και πως στο request η Target MAC address είναι η 00:00:00:00:00:00.

4.31.
Τότε οι υπόλοιποι κόμβοι του τοπικού δικτύου θα έστελναν τα διάφορα πακέτα τους σε οποιοδήποτε άλλο κόμβο, αλλά στην πραγματικότητα θα τα λάμβανε ο κακόβουλος υπολογιστής, ο οποίος βρίσκεται στη μέση της γραμμής της επικοινωνίας τους και μπορεί στη συνέχεια να τα μεταχειριστεί όπως αυτός επιθυμεί. Αυτή η τακτική είναι γνωστή ως MITM attack ή Man-in-the-middle attack.