Ονοματεπώνυμο: Ανδρέας Στάμος (03120***)	**Ομάδα:** 1
Όνομα PC/ΛΣ: linux / Ubuntu 22.04.2 LTS	**Ημερομηνία:** 17/10/2023
Διεύθυνση IP: 192.168.1.10	**Διεύθυνση MAC:** DE–3F–DC–B2–E0–D0

Εργαστηριακή Άσκηση 3
Επικοινωνία στο τοπικό δίκτυο
(πλαίσιο Ethernet και πρωτόκολλο ARP)

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 `ip neigh`

1.2 `ip neigh flush all`

1.3 Default Gateway: 192.168.1.1 (`ip route`)
DNS Server: 192.168.1.1 (`resolvectl`). Προκύπτει 192.168.1.1, διότι ο ISP έχει ρυθμίσει την συσκευή του δρομολογητή/router να λειτουργεί και ως DNS Server, δηλαδή να προωθεί τα αιτήματα σε κάποιον DNS Server του ISP.
Για τις ανάγκες τις ασκήσης ρυθμίζω τον DNS Server χειροκίνητα στον Google Public DNS με διευθύνσεις 8.8.8.8 και 4.4.4.4
Πλέον το `resolvectl` επιστρέφει αυτές τις διευθύνσεις.

1.4 Υπάρχει μόνο η IPv4 και η IPv6 διεύθυνση του δρομολογητή με την ίδια MAC διεύθυνση του δρομολογητή.

1.5 Υπάρχει του default gateway. Αν θεωρήσουμε την συσκευή δρομολογητή που παρέχει ο ISP ως DNS server, τότε τυγχάνει να είναι στο ίδιο δίκτυο με τον υπολογιστή μου, οπότε ναι υπάρχει στον ARP πίνακα. Γενικά, όμως, όπως συμβαίνει με το Google Public DNS εξυπηρετητή, η επικοινωνία με αυτόν γίνεται στο στρώμα δικτύου, αφού δεν βρίσκεται στο ίδιο υποδίκτυο.

1.6 Επειδή δεν υπήρχε κάποια άλλη πριν, έκανα αρχικά ping στο κινητό μου τηλέφωνο για να δημιουργηθεί εγγραφή (από τις ρυθμίσεις του κινητού βρήκα την IPv4 διεύθυνσή του ως 192.168.1.2).

1.7 Αφού απενεργοποιήσουμε οτιδήποτε αυτόματα ζητά συνέχεια το Λειτουργικό Σύστημα και οι διάφορες εφαρμογές από το διαδίκτυο, αδειάζουμε τον ARP πίνακα. Κάνουμε ping στην ip διεύθυνση του κινητού τηλεφώνου, και παρατηρούμε ότι μετά στον ARP πίνακα υπάρχει μόνο η διεύθυνση του κινητού τηλέφωνου. Με άλλα λόγια, ο υπολογιστής επικοινώνησε με το κινητό τηλέφωνο χωρίς να εμπλακεί ο δρομολογητής.

1.8 Στον πίνακα ARP έχει καταχωρθεί μόνο η διεύθυνση του default gateway 192.168.1.1 Ούτε ο DNS Server ούτε ο HTTP Server της ιστοσελίδας του μαθήματος βρίσκεται στο ίδιο υποδίκτυο με τον υπολογιστή μου. Συνεπώς η επικοινωνία μαζί τους (πρώτα με τον 1ο στην συνέχεια με τον 2ο) γίνεται μέσω του στρώματος δικτύου και άρα μέσω του default gateway.

1.9 Όπως είπαμε στο 1.8 ο HTTP Server της ιστοσελίδας του μαθήματος δεν βρίσκεται στο ίδιο υποδίκτυο με τον υπολογιστή μου, οπότε δεν θα γινόταν η IPv4 να υπάρχει στον ARP πίνακα. Η επικοινωνία μαζί του γίνεται στο στρώμα δικτύου μέσω του default gateway.

Άσκηση 2

2.1 MAC destination, MAC source και Ethertype

2.2 Το προοίμιο δεν έχει καταγραφεί καθώς αφενός υπάρχει εκεί για να συγχρονιστεί η κάρτα δικτύου με το σήμα χρονισμού του σήματος που φτάνει στην κάρτα, οπότε μπορεί να μην έχει γίνει ο συγχρονισμός από το 1ο bit, δηλαδή το προοίμιο να μην ληφθεί πλήρως σωστά. Επιπλέον, το προοίμιο δεν μεταφέρει πληροφορία, οπότε θα αποτελούσε σπατάλη υπολογιστικών πόρων να μεταφερθεί στην μνήμη, να φορτωθεί στην ΚΜΕ, κλπ.

2.3 Το Linux δεν παρέχει το FCS μέρος του frame στην βιβλιοθήκη libpcap και συνεπώς το Wireshark δεν μπορεί να ανιχνεύσει πληροφορίες για το FCS.

2.4 0x0800

2.5 0x0806

2.6 Δεν καταγράφηκαν, όμως σύμφωνα με την Wikipedia είναι 0x86DD

2.7 Η διεύθυνση MAC της κάρτας δικτύου του υπολογιστή μου de:3f:dc:b2:e0:d0

2.8 Η διεύθυνση MAC της κάρτας δικτύου του default gateway 39:c3:85:0c:37:d3

2.9 Όχι, η επικοινωνία με τον HTTP Server της ιστοσελίδας του μαθήματος γίνεται στο στρώμα δικτύου, δηλαδή, ως προς το επίπεδο μετάδοσης, δηλαδή το ethernet, το ip πακέτο προωθείται με ethernet στον δρομολογητή, που το προωθεί σε κάποιον άλλο δρομολογητή, κλπ, μέχρι που κάποιος δρομολογητής το προωθεί στον HTTP Server.

2.10 Ανήκει στο default gateway δηλαδή την συσκευή-δρομολογητή που δίνει ο ISP.

2.11 364 bytes

2.12 66 bytes

2.13 Η διεύθυνση MAC της κάρτας δικτύου του default gateway 39:c3:85:0c:37:d3

2.14 Όχι, η επικοινωνία με τον HTTP Server της ιστοσελίδας του μαθήματος γίνεται στο στρώμα δικτύου, δηλαδή, ως προς το επίπεδο μετάδοσης, δηλαδή το ethernet, το ip πακέτο προωθείται με ethernet στον δρομολογητή, που είναι "πλησιέστερα" στον HTTP Server, που το προωθεί σε κάποιον άλλο δρομολογητή, κλπ, μέχρι που ο δρομολογητής μου το προωθεί στο υπολογιστή μου.

2.15 Ανήκει στο default gateway δηλαδή την συσκευή-δρομολογητή που δίνει ο ISP. Είναι ίδια με του ερωτήματος 2.10.

2.16 Η διεύθυνση MAC της κάρτας δικτύου του υπολογιστή μου de:3f:dc:b2:e0:d0

2.17 Στην κάρτα δικτύου του υπολογιστή μου

2.18 5905 bytes

2.19 74 bytes

Άσκηση 3

3.1 Ατομικές (LSB 1ου byte = 0) και μοναδικές (2ο LSB 1ου byte = 0)

3.2 Ομαδικές (LSB 1ου byte = 1) και υπάρχουν και τοπικές και μοναδικές (2ο LSB 1ου byte = 1 ή 0)

3.3 Το Ethernet μεταδίδει ένα byte από το LSB bit προς το MSB bit. Αυτό όμως δεν μπορεί να φανεί στο wireshark εφόσον η κάρτα δικτύου θα φροντίσει να φτιάξει το byte ξανά με την σωστή σειρά. Πάραυτα το 1ο bit της MAC μεταδίδεται 8ο και το 2ο bit μεταδίδεται 7ο.

3.4 FF:FF:FF:FF:FF:FF

3.5 Το φίλτρο σημαίνει να παραμείνουν πλαίσια Logical Link Control. Στην συγκεκριμένη περίπτωση παραμένουν πλαίσια του πρωτοκόλλου STP, που αφορά στην επικοινωνία γεφυρών μεταξύ τους.

3.6 Στο IEEE 802.3 το πεδίο μετά τις διευθύνσεις MAC είναι το μέγεθος του πλαισίου σε πλήθος bytes.

3.7 Αν τα 2 bytes μετά τις διευθύνσεις MAC είναι αριθμός με τιμή <=1500, πρόκειται για το IEEE 802.3, ενώ αν είναι με τιμή >1500 πρόκειται για το Ethernet II.

3.8 Συνολικά 3 bytes και έχει τα πέδια DSAP, SSAP και Control που το καθένα είναι 1 byte.

3.9 Δεδομένα του πρωτοκόλλου STP (Spanning Tree Protocol) που αφορά στην επικοινωνία γεφυρών. Τα δεδομένα αυτά έχουν μέγεθος 36 bytes.

3.10 Το padding έχει μέγεθος 7 bytes, που είναι ίσο με: 64 bytes (ελάχιστο μέγεθος Ethernet πλαισίου) - 36 bytes (μέγεθος δεδομένων) - 21 bytes (επικεφαλίδα Ethernet)

Άσκηση 4

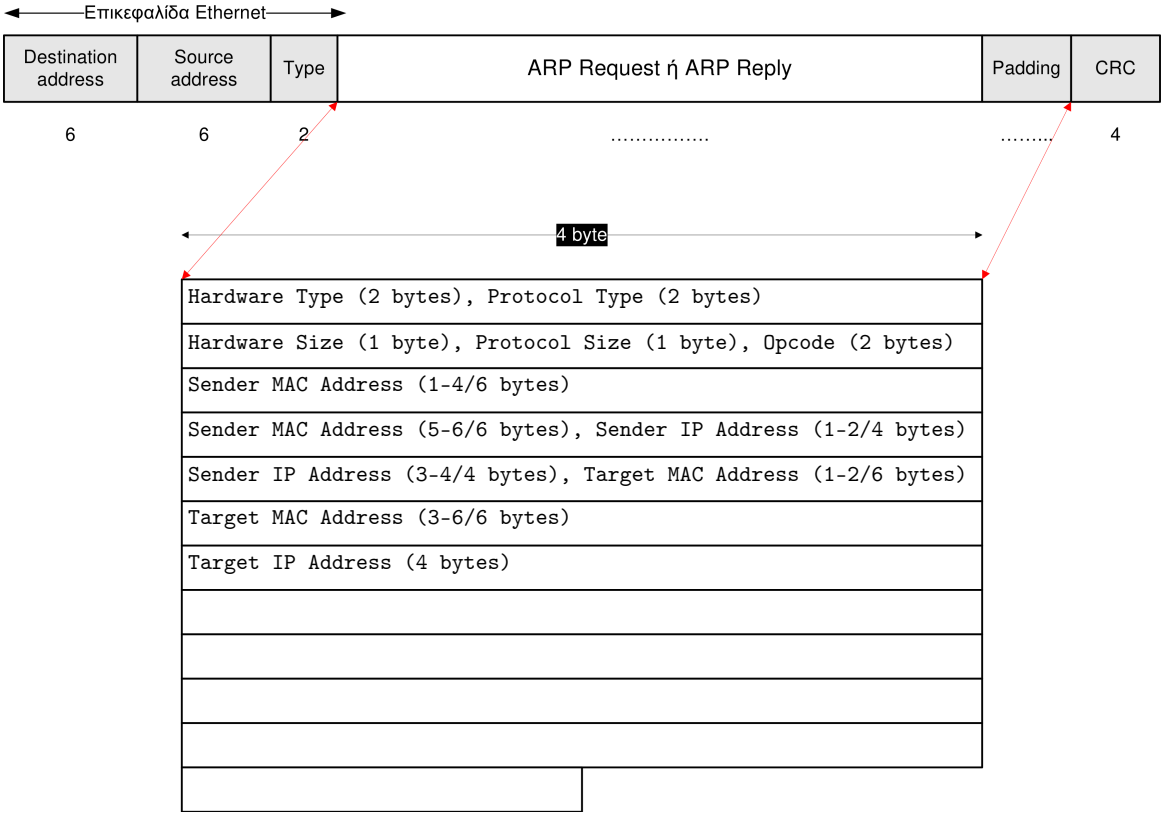
4.1 Εμφανίζει μόνο τα πλαίσια Ethernet που στάλθηκαν από ή απευθυνόνται συγκεκριμένα προς την κάρτα δικτύου του υπολογιστή μας.

4.2 Εμφανίζει μόνο τα πακέτα ARP που στάλθηκαν από ή απευθυνόνται προς την κάρτα δικτύου του υπολογιστή μας. Δηλαδή με άλλα λόγια φαίνονται οι ερωτήσεις ARP που έγιναν από τον υπολογιστή μας και οι απαντήσεις ARP στις ερωτήσεις αυτές.

4.3 2

4.4 Το Type που έχει για τα ARP τιμή 0x0806 (με δεδομένο πως πρόκειται για Ethernet II και όχι για IEEE 802.3)

4.5



4.6 0x0001 που υποδεικνύει Ethernet

4.7 0x0800 που υποδιεκνύει IP

4.8 Η τιμή 0x0800 αντιστοιχεί και στο ARP Protocol type και στο Ethernet II Ethertype το IPv4.

4.9 Οι protocol διεύθυνσεις στο ARP (δηλ οι IPv4) είναι γενικά μεταβλητού μεγέθους και το μέγεθος τους ισούται με το Protocol Size. Πράγματι εδώ οι protocol διευθύνσεις (δηλ. οι IPv4) έχουν μέγεθος 4 bytes.

4.10 Οι hardware διεύθυνσεις στο ARP (δηλ οι MAC) είναι γενικά μεταβλητού μεγέθους και το μέγεθος τους ισούται με το Hardware Size. Πράγματι εδώ οι hardware διευθύνσεις (δηλ. οι MAC) έχουν μέγεθος 6 bytes.

4.11 Στον υπολογιστή μου

4.12 Η broadcast διεύθυνση FF:FF:FF:FF:FF:FF, η οποία σημαίνει πως το πλαίσιο θα πρέπει να παραληφθεί από όλες τις κάρτες δικτύου στις οποίες θα φθάσει

4.13 Το ARP Request έχει μέγεθος 28 bytes και συνολικά όλο το Ethernet II πλαίσιο έχει μέγεθος 42 bytes.

4.14 20 bytes

4.15 0x0001

4.16 Sender MAC address (δηλ. στο Source Hardware Address)

4.17 Sender IP address (δηλ. στο Source Protocol Address)

4.18 Target IP address (δηλ. στο Destination Protocol Address)

4.19 Ναι υπάρχει στο Target MAC Address (δηλ. στο Destination Hardware Address) και έχει τιμή 00:00:00:00:00:00

4.20 Η διεύθυνση MAC του αποστολέα ανήκει στην συσκευή-δρομολογητή που παραχωρεί ο ISP (αφού έκανα ping στο default gateway πριν).

4.21 0x0002

4.22 Sender IP address (δηλ. στο Source Protocol Address) – αναφερόμαστε στον αποστολέα του παρόντος πακέτου ARP Reply

4.23 Sender MAC address (δηλ. στο Source Hardware Address) – αναφερόμαστε στον αποστολέα του παρόντος πακέτου ARP Reply

4.24 Target IP address (δηλ. στο Destination Protocol Address) – αναφερόμαστε στον παραλήπτη του παρόντος πακέτου ARP Reply

4.25 Sender MAC address (δηλ. στο Source Hardware Address)

4.26 Το ARP Reply έχει μέγεθος 28 bytes και συνολικά όλο το Ethernet II πλαίσιο έχει μέγεθος 42 bytes. (Βλ. και 4.29 για το μέγεθος του Ethernet πλαισίου)

4.27 Ναι

4.28 Το Opcode που για τα ARP Request έχει τιμή 0x0001 και για τα ARP Reply έχει τιμή 0x0002.

4.29 Τα πλαίσια Ethernet που αποστέλλονται συλλαμβάνονται πριν επεξεργαστούν από την κάρτα δίκτυου, που είναι εκείνη που εφαρμόζει το zero padding για να φθάσει στο ελάχιστο μέγεθος πλαίσιου Ethernet 60 bytes. Οπότε θα αναμέναμε ότι στα ARP Request θα βλέπαμε ως μέγεθος πλαισίου Ethernet μόνο τα 42 bytes, ενω στα ARP Reply (όπου το zero-padding έχει εφαρμοστεί από την κάρτα δικτύου του αποστολέα) θα βλέπαμε μέγεθος πλαισίου Ethernet 60 bytes (δηλ. μαζί με το zero padding). Ωστόσο, στην πραγματικότητα, στον υπολογιστή μου, δεν χρησιμοποιώ Ethernet, αλλά Wi-Fi (δηλ. IEEE 802.11) το οποίο δεν έχει ελάχιστο μέγεθος πλαισίου, οπότε και η κάρτα δικτύου δεν εφαρμόζει zero-padding.

4.30 Στο ARP Request η Target MAC Address (δηλ. Destination Hardware Address) έχει τιμή 00:00:00:00:00:00, ενώ στο ARP Reply όλες όλες οι protocol addresses αντιστιχούν στις αντίστοιχές τους hardware addresses.

4.31 Προκειμένου να απαντήσουμε διαβάσαμε το σχετικό για το ARP standard RFC 826. Όταν ένας υπολογιστής λάβει ένα ARP πακέτο, καταχωρεί το ζεύγος (Sender IP address, Sender MAC address) στον ARP πίνακα, αντικαθιστώντας προηγούμενη καταχώρηση και έπειτα αν η Target Protocol Address είναι δική του και το opcode είναι Request στέλνει ένα κατάλληλο ARP Reply. Δεν ελέγχεται αν πριν από το ARP Reply είχε στείλει ένα αντίστοιχο ARP Request. Συνεπώς αν ένας κακόβουλος υπολογιστής στο τοπικό δίκτυο απαντήσει στα ARP requests δίνοντας την δική του MAC διεύθυνση, φροντίζοντας τα ARP replies που στέλνει να σταλούν μετά τα ARP replies των "αυθεντικών" κατόχων των protocol addresses, τότε ο υπολογιστής που είχε στείλει το ARP Request θα καταγράψει πως μια IP διεύθυνση αντιστοιχεί στην MAC διεύθυνση του κακόβουλου υπολογιστή. Έτσι, στην συνέχεια, ο υπολογιστής θα στέλνει όλα τα IP πακέτα στον κακόβουλο υπολογιστή και όχι στο "αυθεντικό" κατόχο της IP διεύθυνσης στην οποία απευθύνονται τα πακέτα. Πρόκειται για την γνωστή επίθεση *ARP Spoofing*. Ο κακόβουλος υπολογιστής, τότε, μπορεί να προωθήσει τα πακέτα προς τον "αυθεντικό" παραλήπτη με στόχο να μην γίνει αντιληπτός αλλά να συλλάβει την κίνηση ενός υπολογιστή με έναν άλλο, μπορεί να αλλάξει το περιεχόμενο των πακέτων με στόχο μια *Man In The Middle* επίθεση ή μπορεί να πετάει ένα πόσοστό των πακέτων (ή και όλα) προωθώντας τα υπόλοιπα με σκοπό μια επίθεση DOS (η προώθηση ποσοστού των πακέτων θα είχε στόχο να μην γίνει αντιληπτό ότι έχει γίνει ARP Spoofing).