

**δικτυα υπολογιστων**

**Εργαστηριακη ασκηση 3:Επικοινωνία στο τοπικό δίκτυο**



**(πλαίσιο Ethernet και πρωτόκολλο ARP)**



25 οκτωβριου, 2022

ΘΟΔΩΡΗΣ ΑΡΑΠΗΣ – EL18028

|  |  |  |
| --- | --- | --- |
| **Ονοματεπώνυμο:** Θοδωρής Αράπης | | **Ομάδα:** 2 |
| **Όνομα PC/ΛΣ:** DESKTOP-JGHL94V/ WINDOWS 10 | | **Ημερομηνία:** 25/10/2022 |
| **Διεύθυνση IP:** 192.168.1.5 | **Διεύθυνση MAC:** 70-85-C2-88-FD-B1 | |

**Άσκηση 1: Ο Πίνακας ARP**

***1.1***

Οι εντολές «arp -a» και «arp -g» κάνουν ακριβώς την ίδια δουλειά και μας εμφανίζουν τα περιεχόμενα του πίνακα arp.

***1.2***

Με την εντολή «arp -d \*» μπορούμε να διαγράψουμε όλους τους host που είναι αποθηκευμένοι στον πίνακα ARP.

***1.3***

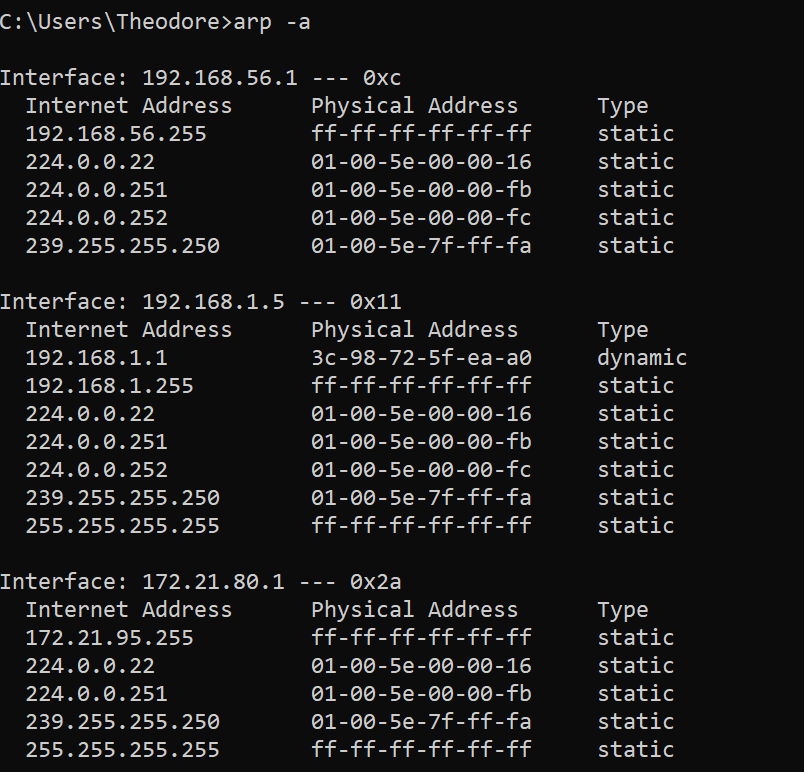
Με την εντολή «ipconfig /all» βρίσκουμε της πληροφορίες που χρειαζόμαστε.

Οι ζητούμενες IP διευθύνσεις είναι οι ακόλουθες:

**Default Gateway:** 192.168.1.1

**DNS Servers:** 192.168.1.1 (Η ίδια συσκευή εκτελεί και τους δύο ρόλους)

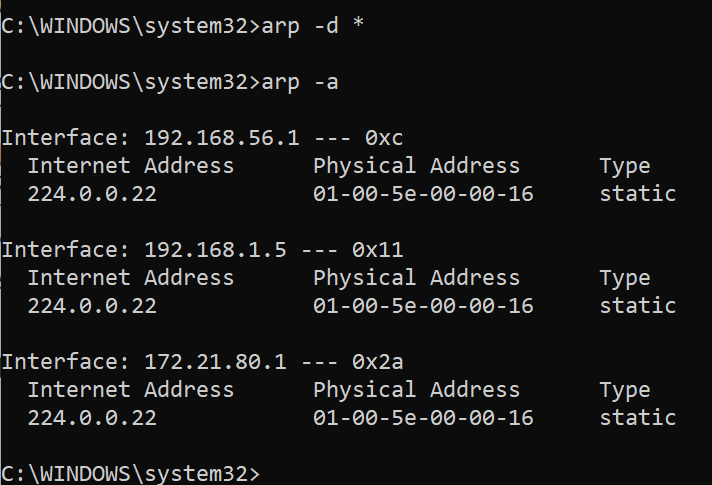
***1.4***

Ο πίνακας περιεχομένων ARP είναι ο ακόλουθος.

***1.5***

Οι διευθύνεις IP του DNS server με το Default Gateway είναι ίδιες και παρατηρούμε ότι η IP αυτή εμφανίζεται στον πίνακα ARP με τους Host που έχει επικοινωνήσει πρόσφατα ο υπολογιστής μας.

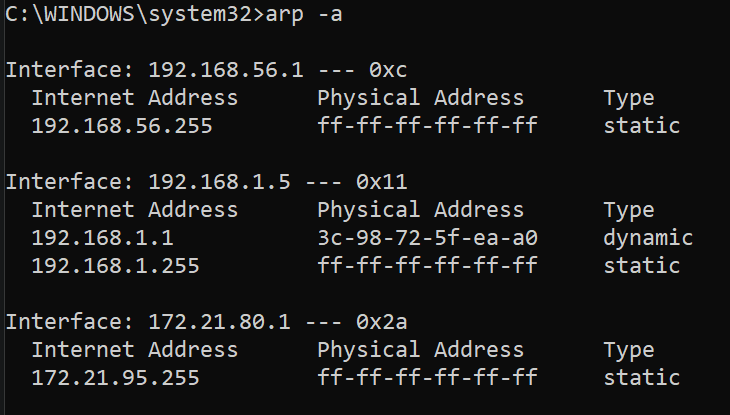
***1.6***

Ανοίγουμε ένα command prompt των windows ως administrators και τρέχουμε την εντολή «arp -d \*».

Κάνουμε ping προς όλες τις διευθύνσεις αλλά καμία δεν ανταποκρίνεται, καθώς δεν υπάρχει επικοινωνία σε τοπικό δίκτυο. Μόνο η διεύθυνση της συσκευής που εξυπηρετεί ως DNS και default Gateway ανταποκρίνεται.

***1.7***

Παρατηρούμε ότι ο πίνακας arp είναι ίδιος με πριν την διαγραφή των περιεχομένων του.

***1.8***

Έχει καταχωρηθεί η διεύθυνση του Default Gateway. Αυτό συμβαίνει διότι ο server της σχολής που είναι υπεύθυνος να μας απαντήσει με τα δεδομένα της σελίδας βρίσκεται σε διαφορετικό υποδίκτυο από το δικό μας. Συνεπώς, με την σύνδεσή μας στην σελίδα, στέλνουμε μήνυμα πρώτα στον router μας (default gateway) και αυτός με την σειρά του δρομολογεί το αίτημά μας στο υπόλοιπο δίκτυο.

***1.9***

Όχι, δεν υπάρχει καταχώρηση της διεύθυνσης IPv4 της σελίδας της σχολής, καθώς o server βρίσκεται σε διαφορετικό υποδίκτυο. Επομένως εμείς απλά επικοινωνούμε με τον router μας (default gateway) όποτε γνωρίζουμε μόνο την δική του IP διεύθυνση.

**Άσκηση 2: Το πλαίσιο Ethernet**

***2.1***

Το Wireshark καταγράφει τα πεδία Source MAC address, Destination MAC address και Type του πλαισίου Ethernet.

***2.2***

Όχι, δεν καταγράφεται το προοίμιο γιατί δεν θεωρείται μέρος του frame.

***2.3***

Το Wireshark κάνει capture πακέτα που πιάνει η packet capture library του λειτουργικού μας συστήματος, συγκεκριμένα η Npcap για Windows. Η βιβλιοθήκη αυτή καταγράφει πακέτα τα οποία το raw packet capture mechanism του λειτουργικού συστήματος μας επιτρέπει. Συνεπώς, δεν βλέπουμε το πεδίο CRC (Cyclic Redundancy Check), τον αλγόριθμος που παράγεται από το FCS (Frame Check Sequence) αφού πολλά λειτουργικά συστήματα δεν υποστηρίζουν την καταγραφή ενός frame στο Ethernet. Με ειδικά configurations στις βιβλιοθήκες ίσως είναι δυνατή η επίτευξη της καταγραφής αυτής.

***2.4***

Για πακέτα IPv4 η τιμή του πεδίου Type στην επικεφαλίδα Ethernet είναι: 0x0800

***2.5***

Για πακέτα IPv4 η τιμή του πεδίου Type στην επικεφαλίδα Ethernet είναι: 0x0806

***2.6***

Για πακέτα IPv4 η τιμή του πεδίου Type στην επικεφαλίδα Ethernet είναι: 0x86dd

***2.7***

Η διεύθυνση MAC πηγής του πλαισίου είναι: 70:85:c2:88:fd:b1

***2.8***

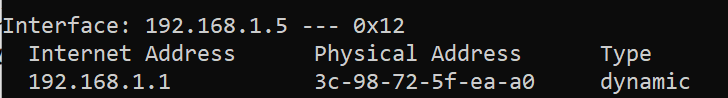
Η διεύθυνση MAC προορισμού του πλαισίου είναι: 3c:98:72:5f:ea:a0

***2.9***

Όχι, δεν ανήκει στο edu-dy.cn.ntua.gr.

***2.10***

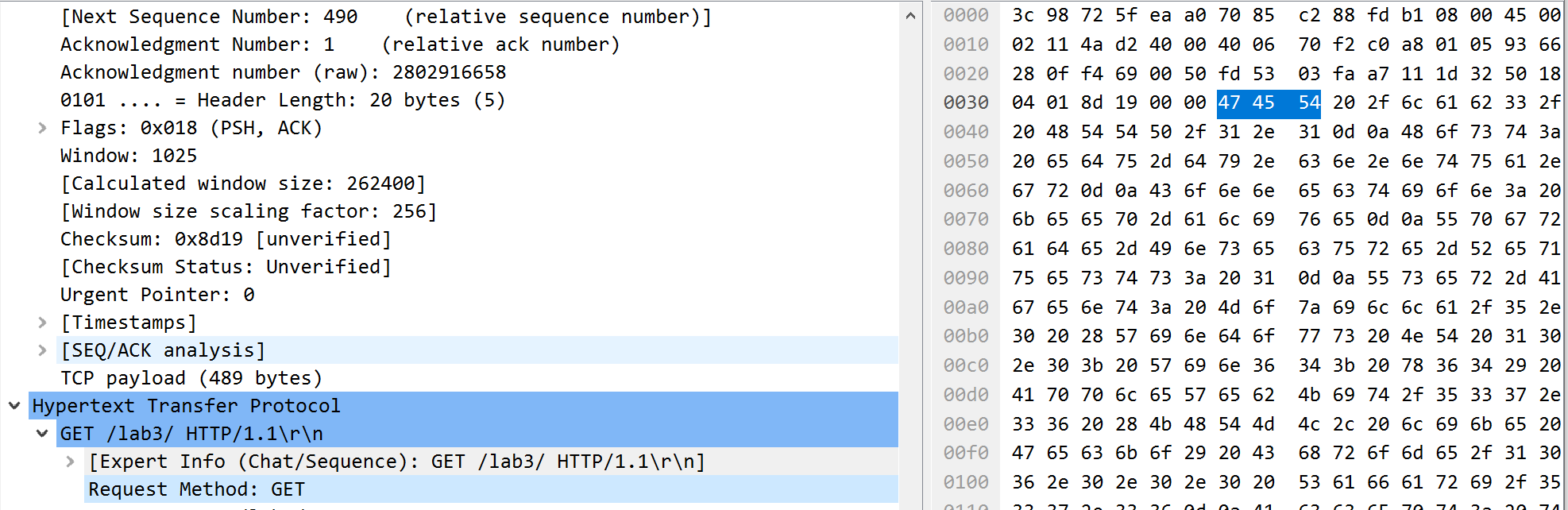
Ανήκει στην συσκευή που δρα ως Default Gateway, δηλαδή τον router μας, αφού ο υπολογιστής μας χρειάζεται να επικοινωνήσει μόνο με αυτόν και ύστερα αυτός είναι υπεύθυνος να μεταδώσει την πληροφορία στο υπόλοιπο δίκτυο μέχρι τον επιθυμητό προορισμό.

ARP entry:

***2.11***

Το πλαίσιο έχει σύνολο 543 bytes.

***2.12***

Παρατηρούμε ότι προηγούνται 54 byte (η λέξη GET είναι οι δεκαεξαδικοί 47 45 54).

***2.13***

Η διεύθυνση MAC του αποστολέα είναι: 3c:98:72:5f:ea:a0

***2.14***

Όχι, δεν ανήκει στο edu-dy.cn.ntua.gr.

***2.15***

Η διεύθυνση αυτή, όπως αναφέραμε και σε προηγούμενα ερωτήματα, ανήκει στον router μας.

***2.16***

Η διεύθυνση MAC του παραλήπτη είναι: 70:85:c2:88:fd:b1

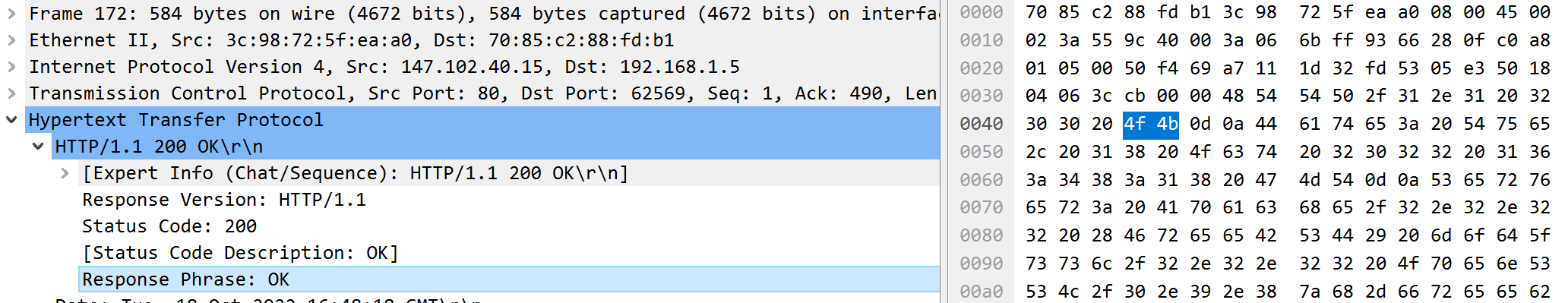
***2.17***

Η διεύθυνση αυτή ανήκει στην κάρτα δικτύου του υπολογιστή μας.

***2.18***

Το πλαίσιο έχει μήκος 584 bytes.

***2.19***

Προηγούνται 67 bytes (Η λέξη ΟΚ είναι η οι δεκαεξαδικοί 4f 4b).

**Άσκηση 3: Περισσότερα για τα πλαίσια Ethernet**

***3.1***

Οι διευθύνσεις MAC πηγής που καταγράφουμε είναι οι ακόλουθες:

**Α)** 3c:98:72:5f:ea:a0 (router)

**Β)** 70:85:c2:88:fd:b1 (υπολογιστής μας)

**Γ)** 70:5f:a3:b1:cf:56 (κινητή συσκευή)

Εξετάζουμε το byte 0 σε κάθε MAC διεύθυνση. Σε δυαδική μορφή έχουμε για κάθε περίπτωση:

**Α)** 001111**00**

**Β)** 011100**00**

**Γ)** 011100**00**

Σε όλες τις περιπτώσεις το LSB του byte 0 είναι 0, άρα έχουμε ατομικές διευθύνσεις.

Σε όλες τις περιπτώσεις το δεύτερο LSB του byte 0 είναι 0, άρα έχουμε παγκόσμιες διευθύνσεις.

***3.2***

Οι διευθύνσεις MAC προορισμού που καταγράφουμε είναι οι ακόλουθες:

**Α)** 01:80:c2:00:00:00

**Β)** 01:00:5e:40:98:8f

**Γ)** 33:33:ef:c0:98:8f

**Δ)** 33:33:00:00:00:01

**Ε)** 01:00:5e:00:00:fb

Εξετάζουμε το byte 0 σε κάθε MAC διεύθυνση. Σε δυαδική μορφή έχουμε για κάθε περίπτωση:

**Α)** 000000**01**

**Β)** 000000**01**

**Γ)** 001100**11**

**Δ)** 001100**11**

**Ε)** 000000**01**

Σε όλες τις περιπτώσεις το LSB του byte 0 είναι 1, άρα έχουμε ομαδικές διευθύνσεις (multicast).

Οι διευθύνσεις Α, Β, Ε έχουν στο δεύτερο LSB του byte 0 την τιμή 0, άρα έχουμε παγκόσμιες διευθύνσεις, ενώ οι υπόλοιπες έχουν τιμή 1, άρα τοπικές διευθύνσεις.

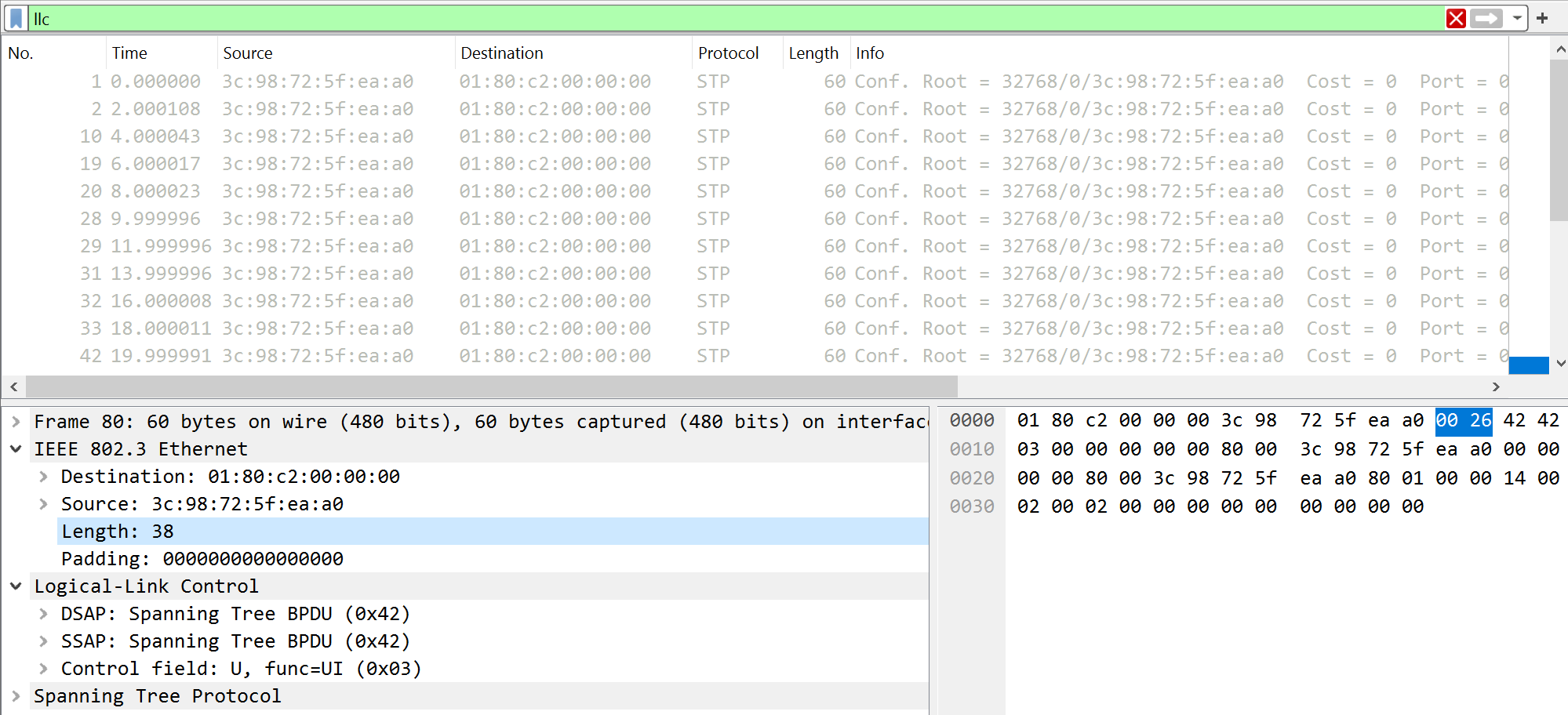
***3.3***

Γνωρίζουμε ότι η διεύθυνση MAC μεταδίδεται κατά byte από αριστερά προς τα δεξιά, ενώ κάθε byte μεταδίδεται από αριστερά προς τα δεξιά. Επομένως πρώτα εμφανίζεται το LSB του πρώτου byte (8ο bit του byte 0) της MAC διεύθυνσης και ύστερα το δεύτερο (7ο bit του byte 0) (δηλαδή τα δύο bytes που εξετάσαμε στα προηγούμενα ερωτήματα.)

***3.4***

Η διεύθυνση MAC για τα broadcast πλαίσια περιέχει μόνο άσσους (δηλαδή «ff:ff:ff:ff:ff:ff»).

***3.5***

Εμφανίζει μόνο τα πακέτα που διέπονται από το πρωτόκολλο IEEE 802.3 Ethernet.

***3.6***

Στα πλαίσια IEEE 802.3, μετά τις διευθύνσεις MAC υπάρχει το πεδίο length που δηλώνει το μήκος σε byte των δεδομένων που περιέχονται στο πεδίο δεδομένων.

***3.7***

Αρχικά, τα πλαίσια IEEE 802.3 περιέχουν το πεδίο Length αντί για το type που περιέχουν τα πλαίσια Ethernet II. Ακόμη, τα πλαίσια IEEE 802.3 περιέχουν τη επικεφαλίδα Logical Link Control (LLC) η οποία προσδιορίζει το πρωτόκολλο ανωτέρου στρώματος, ενώ τα πλαίσια Ethernet II όχι.

***3.8***

Η επικεφαλίδα Logical Link Control (LLC) έχει μέγεθος 3 byte και περιλαμβάνει τα πεδία:

***DSAP:*** Destination Service Access Point, δρα ως δείκτης σε ένα memory buffer στον αποδέκτη και λέει στον NIC του δέκτη σε ποιο buffer να αποθηκεύσει την πληροφορία που δέχεται

***SSAP:*** Source Service Access Point, παρόμοια λειτουργία με το DSAP αλλά για τον αποστολέα

***Control field***

***3.9***

Μεταφέρουν δεδομένα του πρωτοκόλλου STP (Spanning Tree Protocol) και έχουν μέγεθος 38 bytes.

***3.10***

Το padding έχει μέγεθος 8 byte στην περίπτωσή μας και χρησιμεύει ώστε τα πλαίσια να φτάσουν το ελάχιστον μήκος που απαιτείται να έχουν (64 bytes). Οπότε έχουμε αναλυτικά:

6 bytes διεύθυνση προορισμού, 6 bytes διεύθυνση πηγής, 2 bytes Length, 38 bytes payload (ελάχιστο απαιτούμενο 46 οπότε γι’ αυτό έχουμε padding 8 bytes), padding 8 bytes και 4 bytes FCS, τα οποία δεν εμφανίζονται, άρα συνολικά 64 bytes.

**Άσκηση 4: Περισσότερα για πακέτα ARP**

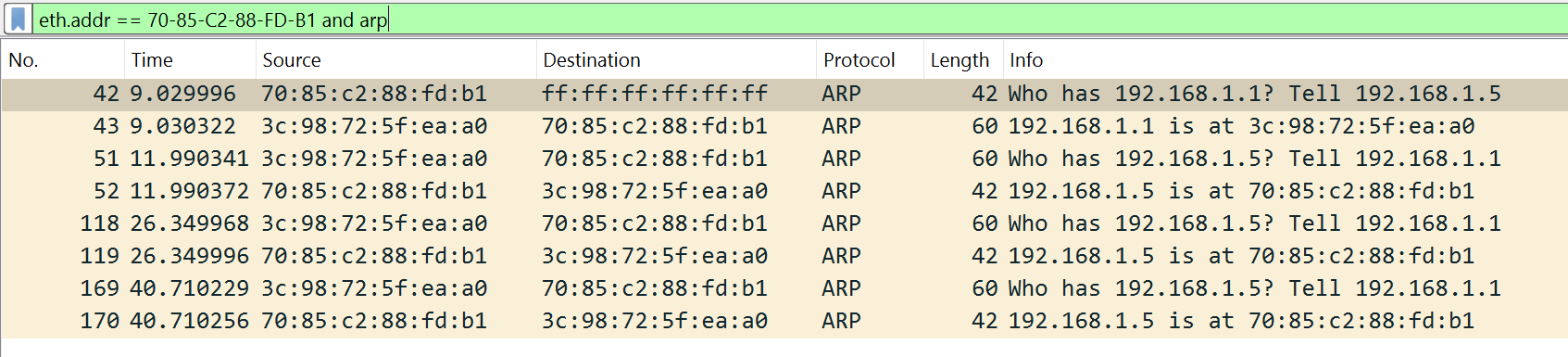
***4.1***

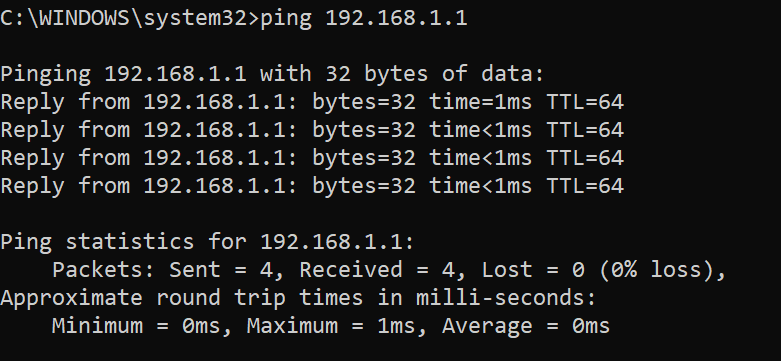
Το φίλτρο αυτό μας εμφανίζει όλα τα πλαίσια που στέλνονται ή λαμβάνονται από τ=την διεύθυνση MAC που συμπληρώσαμε (συγκεκριμένα του υπολογιστή μας).

***4.2***

Το φίλτρο κάνει ότι και πριν απλά σαν επιπλέον περιορισμό στα πλαίσια που εμφανίζει έχουμε τώρα ότι αυτά πρέπει να ενθυλακώνουν ΚΑΙ το ARP πρωτόκολλο.

***4.3***

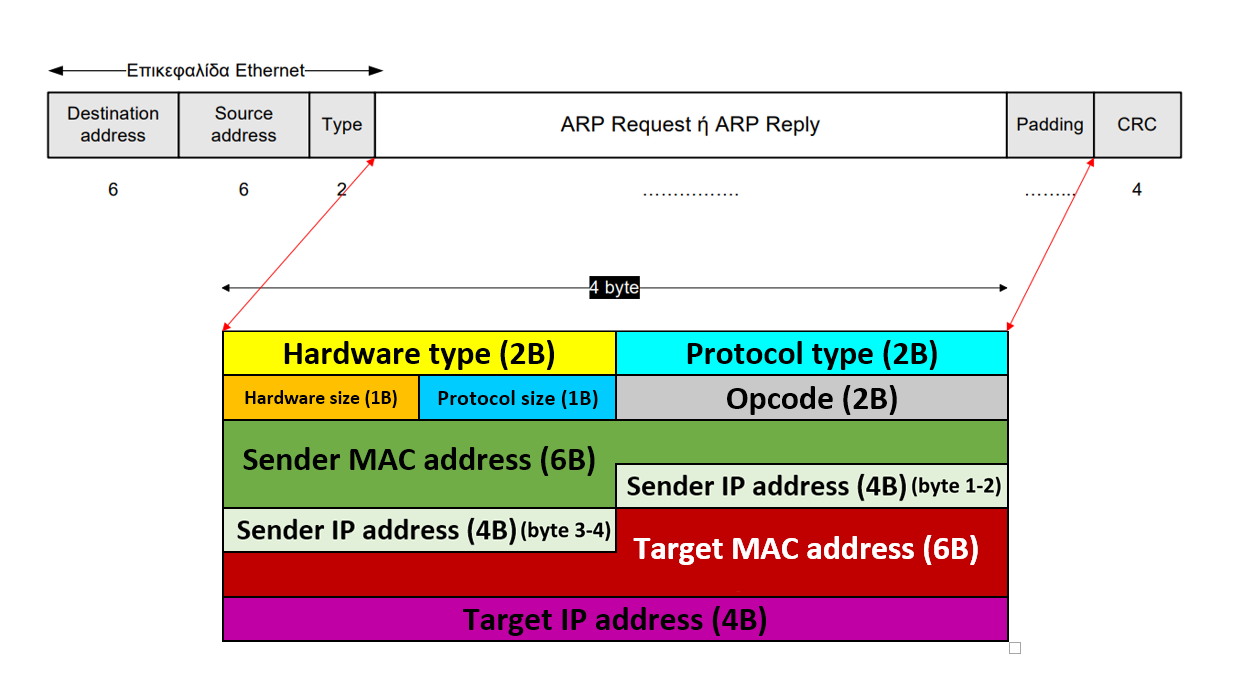
Ανταλλάχθηκαν 8 πακέτα ARP.



Παρατηρήσαμε ότι χρειάστηκε να περιμένουμε λίγα δευτερόλεπτα αφότου τελείωσε η εκτέλεση της εντολής «ping …» προκειμένου να καταγράψει όλα τα πακέτα το Wireshark.

***4.4***

Η διαφοροποίηση βρίσκεται στο πεδίο Type του πλαισίου Ethernet, όπου τα πακέτα ARP έχουν τιμή 0x0806, ενώ τα πακέτα IPv4 έχουν τιμή 0x0800.

***4.5***

***4.6***

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

***4.7***

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

***4.8***

Το πεδίο Protocol Type αναφέρεται στο πρωτόκολλο του Network Layer (π.χ. IPv4), ενώ το EtherType αναφέρεται στο πρωτόκολλο που είναι ενθυλακωμένο στο payload του πλαισίου και χρησιμοποιείται στο άκρο λήψης από το Data Link Layer για να προσδιορίσει τον τρόπου επεξεργασίας του payload αυτού (π.χ. ARP).

***4.9***

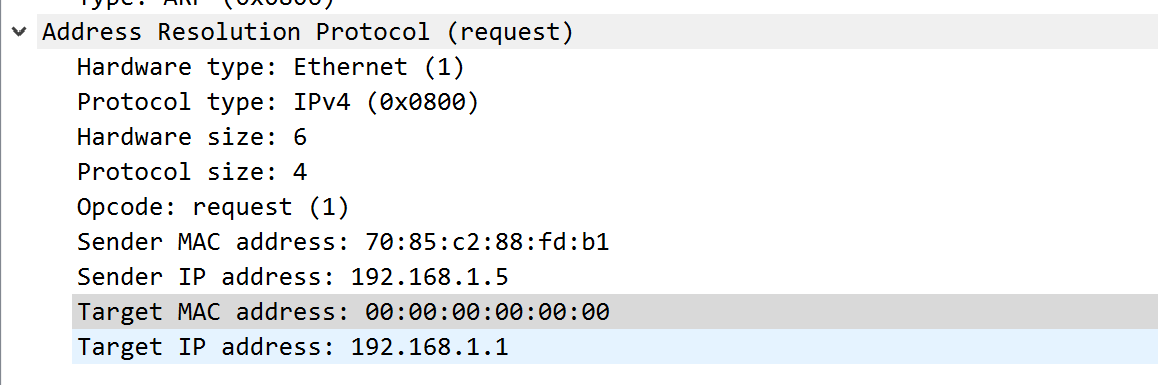
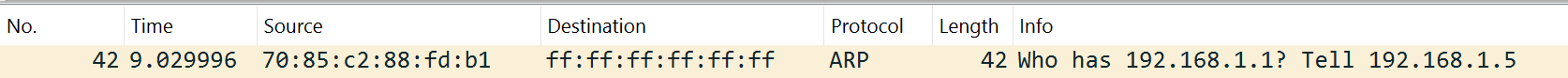
Το πεδίο Protocol size έχει τιμή 4 γιατί συμβολίζει το μήκος της διεύθυνσης πρωτοκόλλου, η οποία στην περίπτωσή μας είναι IPv4 άρα αναπαρίσταται με 4 bytes.

***4.10***

Όσον αφορά το Hardware Size, διαβάζουμε ότι πρόκειται για το μήκος των διευθύνσεων Hardware σε bytes. Επομένως, αναφέρεται σε διευθύνσεις MAC, οι οποίες αποτελούνται από 6 bytes.

***4.11***

Η διεύθυνση MAC αποστολέα του πλαισίου Ethernet που μεταφέρει το εν λόγω ARP Request ανήκει στον υπολογιστή μας.

***4.12***

Η διεύθυνση MAC του παραλήπτη του πλαισίου αυτού είναι: ff:ff:ff:ff:ff:ff. (broadcast). Από τα πεδία του ARP βλέπουμε ως Target MAC address το 00:00:00:00:00:00, το οποίο υποδηλώνει πως δε γνωρίζουμε τη MAC του παραλήπτη, του οποίου ωστόσο γνωρίζουμε την IP. Επομένως, ο υπολογιστής μας κάνει broadcast το request προκειμένου να λάβει ως απάντηση τη MAC διεύθυνση του Gateway gate (router).

***4.13***

Το πλαίσιο Ethernet έχει συνολικό μήκος 42 bytes, ενώ το πακέτο ARP αποτελεί τα 28 εξ αυτών.

***4.14***

Του πεδίου Opcode προηγούνται 20 bytes.

***4.15***

Η τιμή του πεδίου Opcode είναι 0x0001 (request).

***4.16***

Η διεύθυνση MAC του αποστολέα είναι στο πεδίο Sender MAC address εντός του πακέτου ARP request.

***4.17***

Αντίστοιχα, η διεύθυνση IP του αποστολέα, είναι στο πεδίο Sender IP address.

***4.18***

Η διεύθυνση IPv4 του υπολογιστή, του οποίο αναζητείται η MAC είναι στο πεδίο Target IP address.

***4.19***

Το πεδίο Target MAC address αναφέρεται στη ζητούμενη διεύθυνση MAC. Στην δική μας περίπτωση, έχει τιμή 00:00:00:00:00:00. Η διεύθυνση αυτή υποδηλώνει άγνωστη διεύθυνση, πράγμα αναμενόμενο, καθώς το ARP request στέλνεται προκειμένου να ληφθεί ως απάντηση η MAC της συσκευής της οποία γνωρίζουμε την IP.***4.20***

Η διεύθυνση MAC του αποστολέα ανήκει στο router μας, ενώ του παραλήπτη στον υπολογιστή μας.

***4.21***

Η τιμή του πεδίου Opcode στο ARP reply έχει τιμή 0x0002.

***4.22***

Η διεύθυνση IPv4 του αποστολέα βρίσκεται στο πεδίο Sender IP address του πακέτου ARP reply.

***4.23***

Η διεύθυνση MAC του αποστολέα βρίσκεται στο πεδίο Sender MAC address.

***4.24***

Η διεύθυνση IPv4 του παραλήπτη βρίσκεται στο πεδίο Target IP address.

***4.25***

Η διεύθυνση MAC του υπολογιστή που έχει τη διεύθυνση IPv4 για την οποία έγινε η ερώτηση βρίσκεται στο πεδίο Sender MAC address, αφού δίνει την απάντηση στην ερώτηση που κάναμε broadcast προηγουμένως, οπότε τώρα είναι ο αποστολέας του ARP reply.

***4.26***

Το πλαίσιο Ethernet έχει συνολικό μήκος 60 bytes, ενώ το πακέτο ARP αποτελεί τα 28 εξ αυτών. Εμφανίζονται επιπλέον 18 byte trailer (padding και CRC).

***4.27***

Το μέγεθος του ARP είναι ακριβώς το ίδιο και στις δύο περιπτώσεις, διαφέρει όμως το συνολικό μήκος του frame, με το reply να είναι μεγαλύτερο κατά 18 bytes.

***4.28***

Το πεδίο Opcode προσδιορίζει εάν πρόκειται για request(0x0001) ή reply(0x0002).

***4.29***

Η διαφορά αυτή οφείλεται στο γεγονός ότι τα προς αποστολή πλαίσια συλλαμβάνονται προτού μεταδοθούν, επομένως δεν έχει προστεθεί το Padding σε αυτά, σε αντίθεση με τα πακέτα που λαμβάνουμε.

***4.30***

Μία διαφορά μεταξύ αιτήματος και απάντησης ARP είναι πως η ερώτηση γίνεται με σκοπό να γίνει γνωστή η MAC address μιας εκ των προτέρων γνωστής IP. Έτσι, το Target MAC address είναι το 00:00:00:00:00:00, δηλαδή άγνωστο, ενώ στην απάντηση, είναι πλέον γνωστή η διεύθυνση αυτή και έχει τον ρόλο του Sender MAC address. Επιπρόσθετα, επειδή ακριβώς δε γνωρίζουμε ποια συσκευή έχει τη δεδομένη IP, το request γίνεται broadcast (ff:ff:ff:ff:ff:ff) προκειμένου να το λάβουν όλες οι συσκευές και να απαντήσει εκείνη της οποίας το IP address ταυτίζεται με το Sender IP address του αιτήματος. Αντίθετα, στην απάντηση είναι γνωστές οι διευθύνσεις MAC αποστολέα και παραλήπτη και συνεπώς έχουμε unicast μεταξύ αυτών.

***4.31***

Εάν ένας κακόβουλος χρήστης απαντούσε σε όλα τα αιτήματα ARP παραχωρώντας την δική του MAC, τότε ότι πακέτα έστελναν οι χρήστες στο τοπικό δίκτυο προς τις διευθύνσεις IP με τις οποίες έκαναν τα request προηγουμένως θα στέλνονται προς τον κακόβουλο χρήστη. Συνεπώς, θα αποκτούσε πρόσβαση στα δεδομένα αυτά.