

**δικτυα υπολογιστων**

**Εργαστηριακη ασκηση 9: SMTP, DHCP**



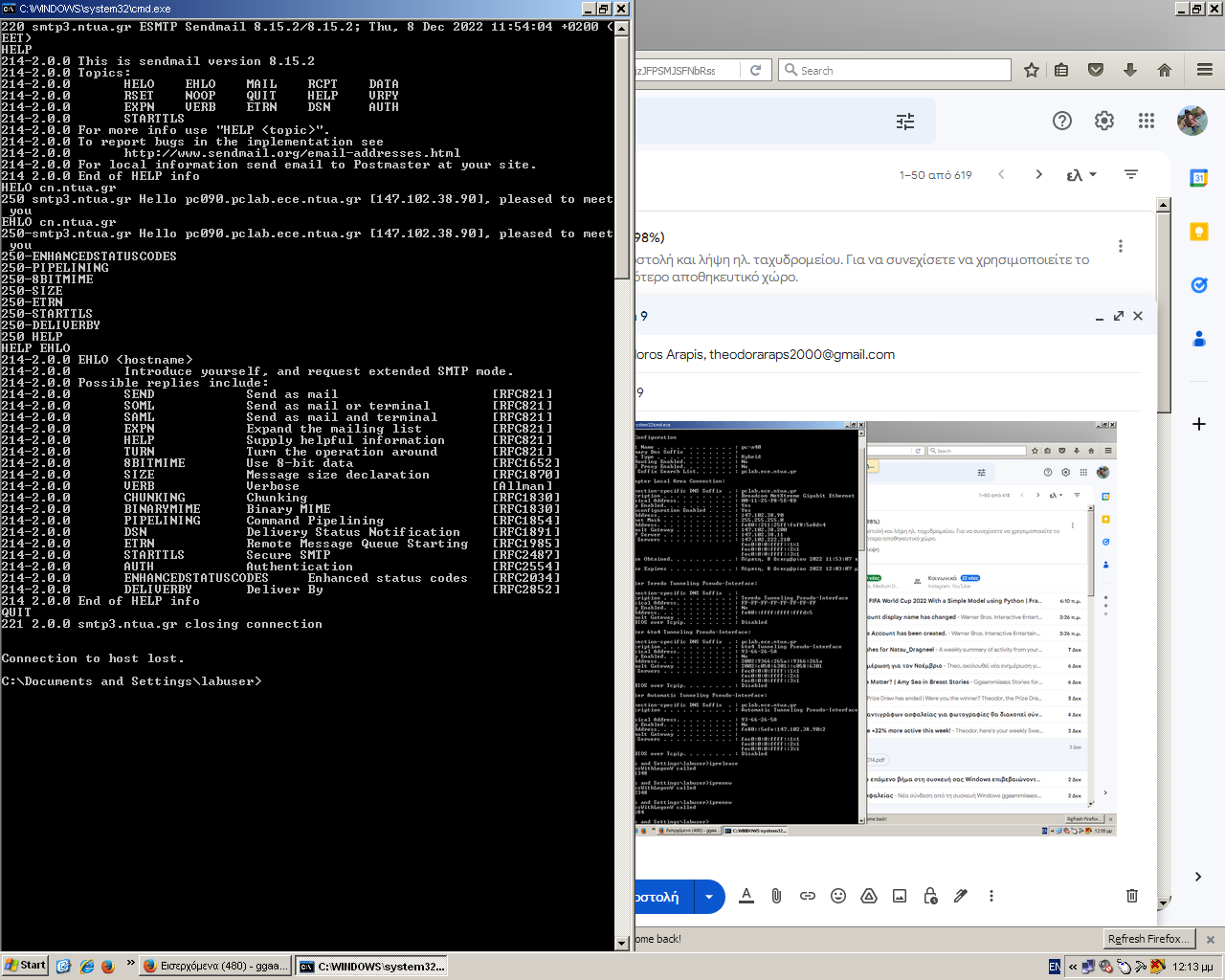


13 Δεκεμβρίου, 2022

ΘΟΔΩΡΗΣ ΑΡΑΠΗΣ – EL18028

|  |  |  |
| --- | --- | --- |
| **Ονοματεπώνυμο:** Θοδωρής Αράπης | | **Ομάδα:** 2 |
| **Όνομα PC/ΛΣ:**  pc-a40/ WINDOWS 95 (Άσκηση 1)  DESKTOP-JGHL94V/ WINDOWS 10 (Άσκηση 2) | | **Ημερομηνία:** 13/12/2022 |
| **Διεύθυνση IP:**  147.102.38.90 (Άσκηση 1)  192.168.0.193 (Άσκηση 2) | **Διεύθυνση MAC:**  00:11:25:F8:5E:8D (Άσκηση 2)  70-85-C2-88-FD-B1 (Άσκηση 2) | |

**Άσκηση 1: Το πρωτόκολλο SMTP**

Αρχικά τρέχουμε τις δοσμένες εντολές:

***1.1***

Ο τρόπος κλήσης της εντολής telnet που τρέξαμε («telnet smtp.ntua.gr 25»), δηλώνει πως εκκινούμε μια σύνδεση στον κεντρικό υπολογιστή με όνομα smtp.ntua.gr στη θύρα 25.

***1.2***

Όπως φαίνεται από το παραπάνω screenshot, κωδικός απόκρισης που αποστέλλει ο εξυπηρετητής SMTP μετά την εγκατάσταση της σύνδεσης είναι ο 220, ο οποίος είναι της μορφής 220 <domain> Service Ready, μας ενημερώνει επομένως πως η υπηρεσία είναι έτοιμη για χρήση.

***1.3***

Το DNS όνομα του εξυπηρετητή είναι: smtp3.ntua.gr.

***1.4***

Το αναγνωστικό κείμενο είναι το «ESMTP Sendmail 8.15.2/8.15.2; Thu, 8 Dec 2022 11:54:04 +0200 (EET)».

***1.5***

Όπως βλέπουμε από το screenshot, ο κωδικός απόκρισης στο HELP είναι ο 214.

***1.6***

Παρατηρούμε ότι ο σέρβερ αυτός υποστηρίζει 16 εντολές, 3 εκ των οποίων είναι οι HELO, EHLO, MAIL.

***1.7***

Η τελευταία γραμμή της απόκρισης διακρίνεται λόγω του γεγονότος ότι δε περιλαμβάνει hyphen, είναι δηλαδή της μορφής Code (214) και στη συνέχεια space αντί για hypen, ακολουθούμενο από το μήνυμα «End of HELP info».

***1.8***

Όπως φαίνεται στο αρχικό screenshot, ο κωδικός απόκρισης στην εντολή HELO είναι ο 250.

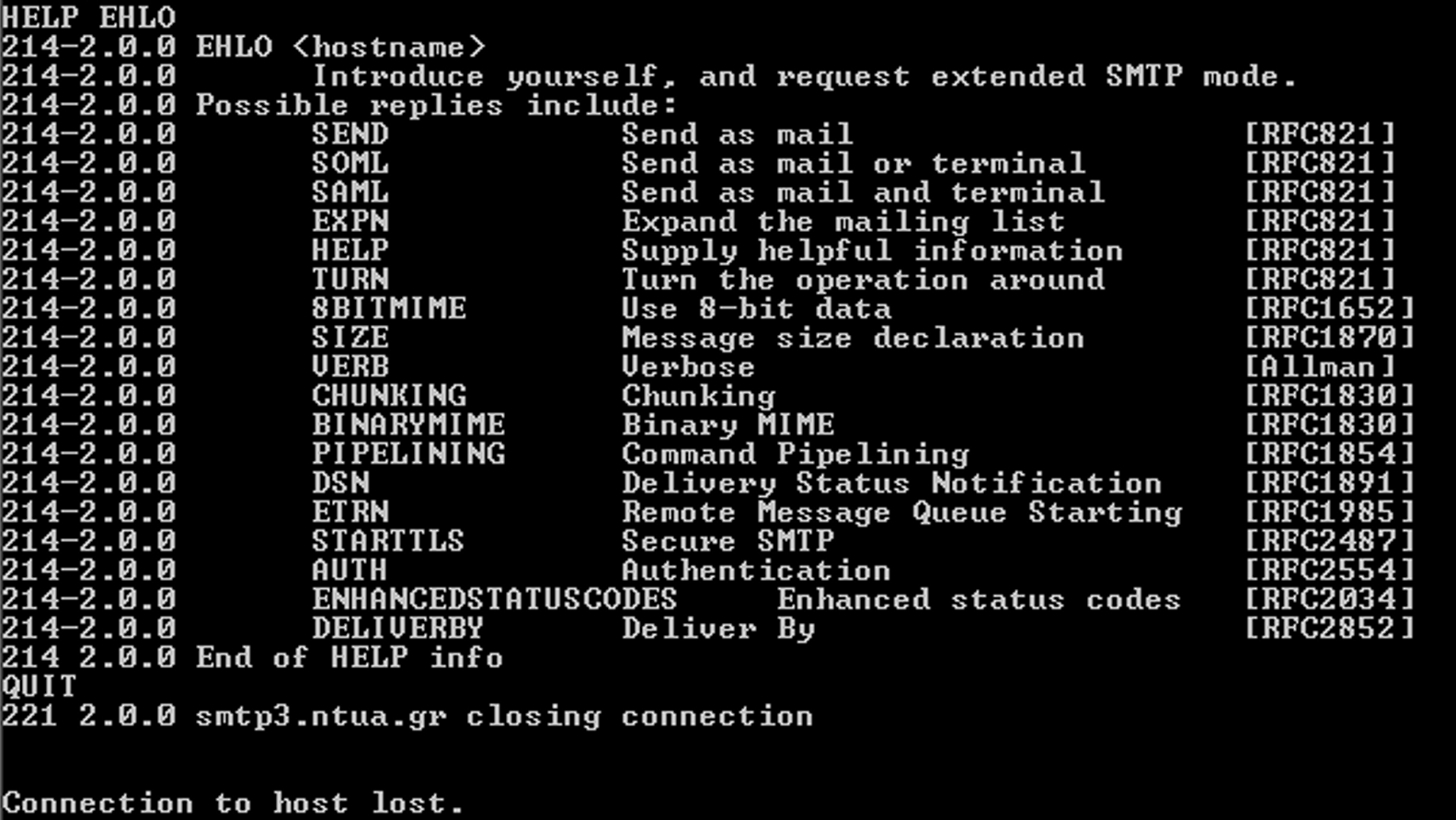
***1.9***

Παρατηρούμε στην απόκριση της εντολής HELO ότι δεν εμφανίζεται το όνομα του υπολογιστή που δηλώνει η εντολή HELO (cn.ntua.gr), αλλά εμφανίζεται η IPv6 του υπολογιστή αυτού.

***1.10***

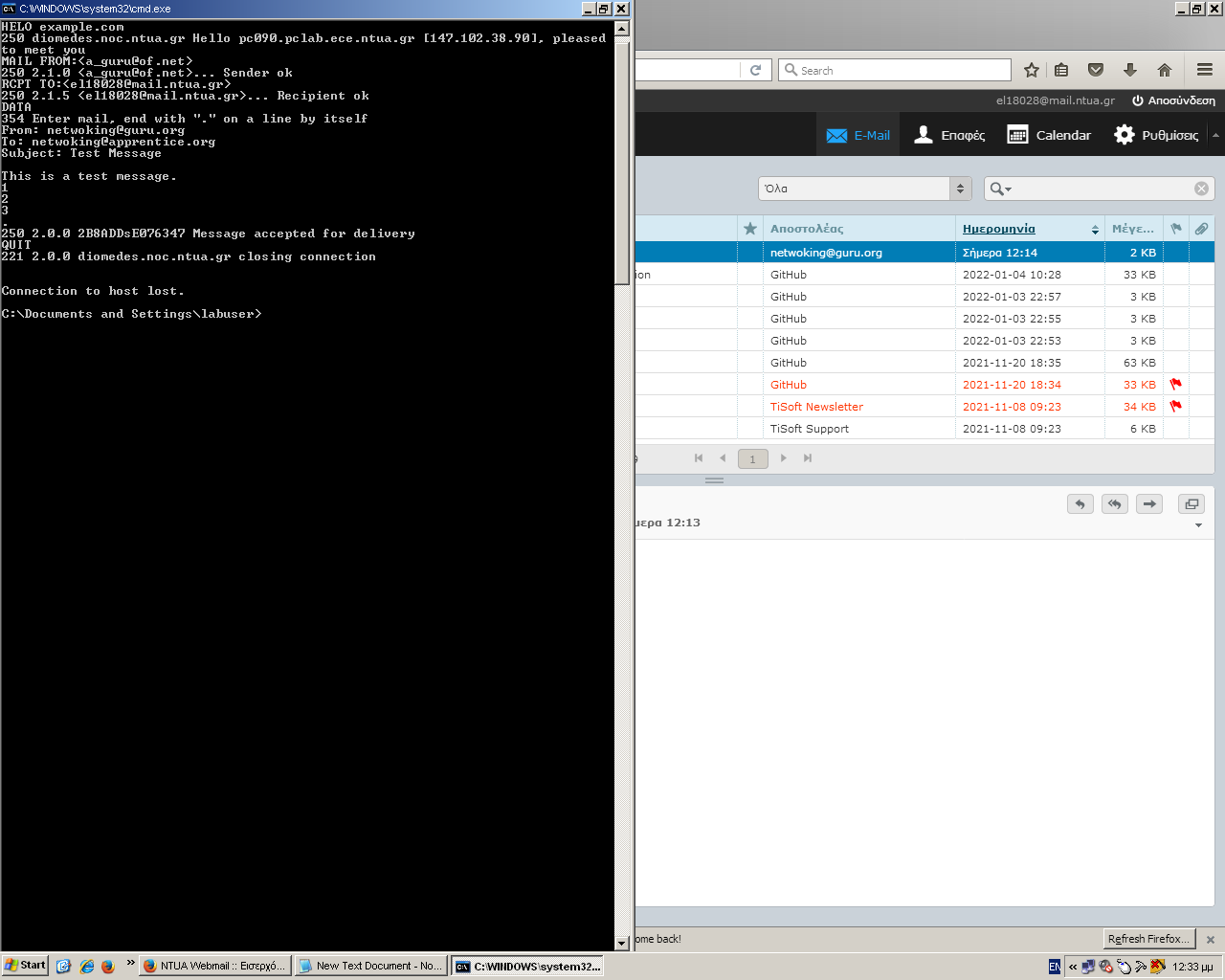
Η απόκριση του εξυπηρετητή στην εντολή EHLO περιλαμβάνει μία γραμμή.

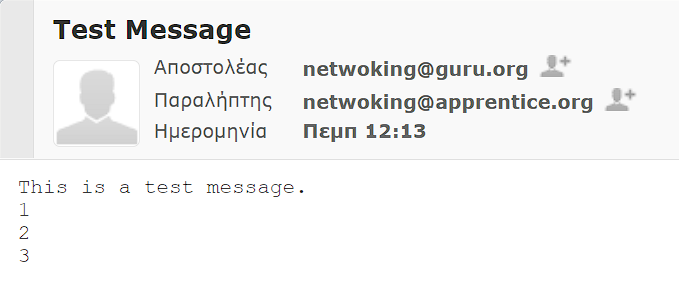
***1.11***

Τα έξτρα αποτελέσματα που εμφανίζονται, σε σχέση με αυτά της εντολής HELO, είναι keywords για κάθε επέκταση υπηρεσίας που υλοποιεί ο εξυπηρετητής. Τις υπηρεσίες αυτές τις βλέπουμε παρακάτω με το HELP EHLO:

***1.12***

Στο πρώτο μήνυμα που λάβαμε από τον εξυπηρετητή (ερώτημα 1.2) γίνεται εμφανές ότι ο σέρβερ smtp.ntua.gr υποστηρίζει το ESMTP.

******Εκτελούμε τώρα τις ζητούμενες εντολές:

Ανοίγουμε το ηλεκτρονικό ταχυδρομείο της ιστοσελίδας https://webmail.ntua.gr/ και επιβεβαιώνουμε την λήψη του μηνύματος.

***1.13***

Από την πρώτη απόκριση που λαμβάνουμε από τον σέρβερ relay.ntua.gr (την οποία καταλάθος δεν την περιέχουμε στο παραπάνω screenshot), η ημερομηνία και ώρα είναι: 8 Δεκεμβρίου 2022 12:13:13.

***1.14***

Η απόκριση του εξυπηρετητή και ο αντίστοιχος κωδικός απόκρισης στην εντολή DATA είναι: «354 Enter mail, end with “.” on a line by itself».

***1.15***

Η τελεία που πληκτρολογούμε πριν την εντολή QUIT δηλώνει το τέλος της εισαγωγής δεδομένων.

***1.16***

Λαμβάνουμε την εξής απόκριση του εξυπηρετητή με κωδικό 250:

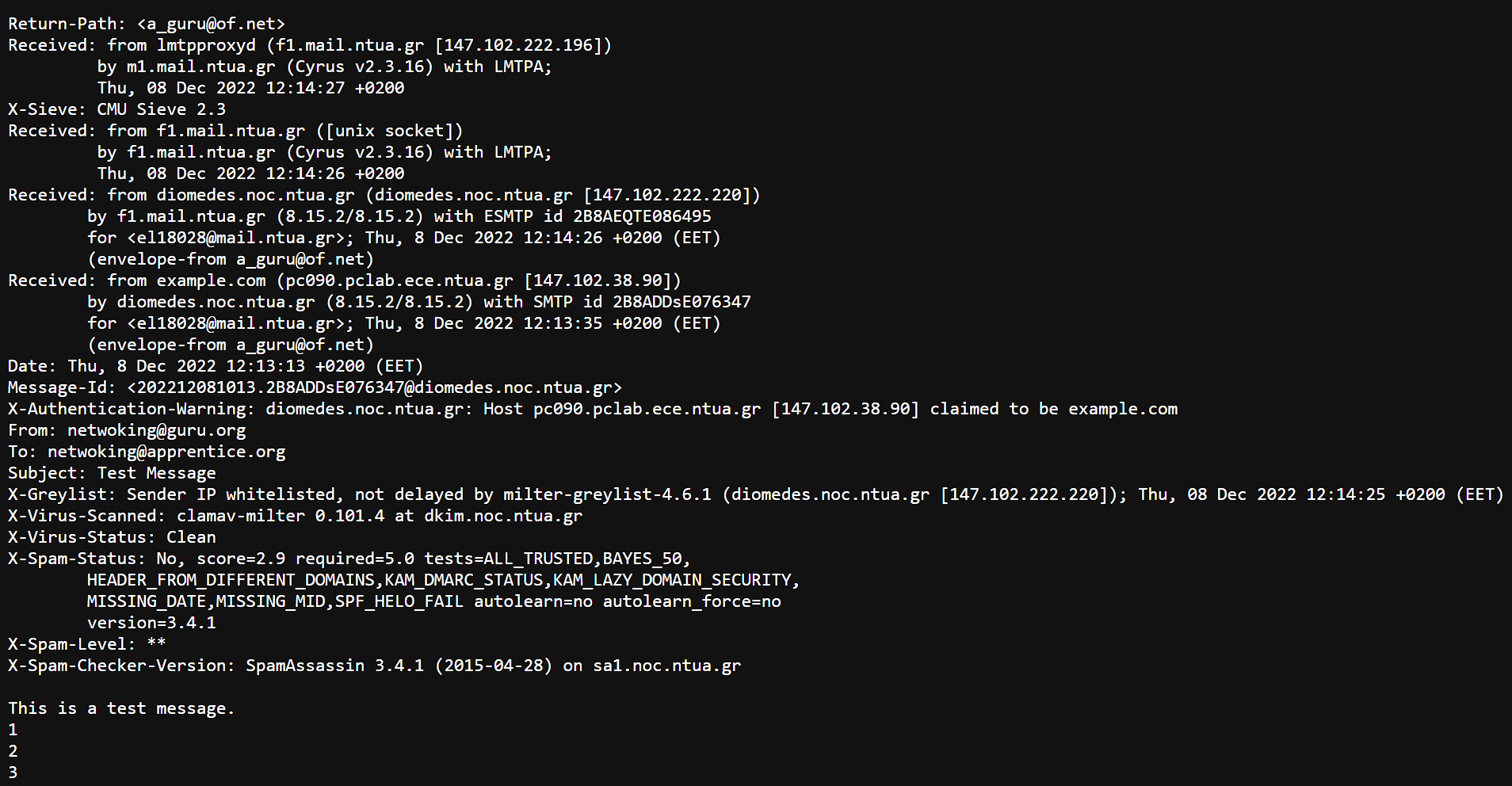
«250 2.0.0 2B8ADDsE076347 Message accepted for delivery».

***1.17***

Ως αποστολέας του μηνύματος εμφανίζεται ο netwoking@guru.org, δηλαδή αυτός του κειμένου της επικεφαλίδας From: του μηνύματος.

***1.18***

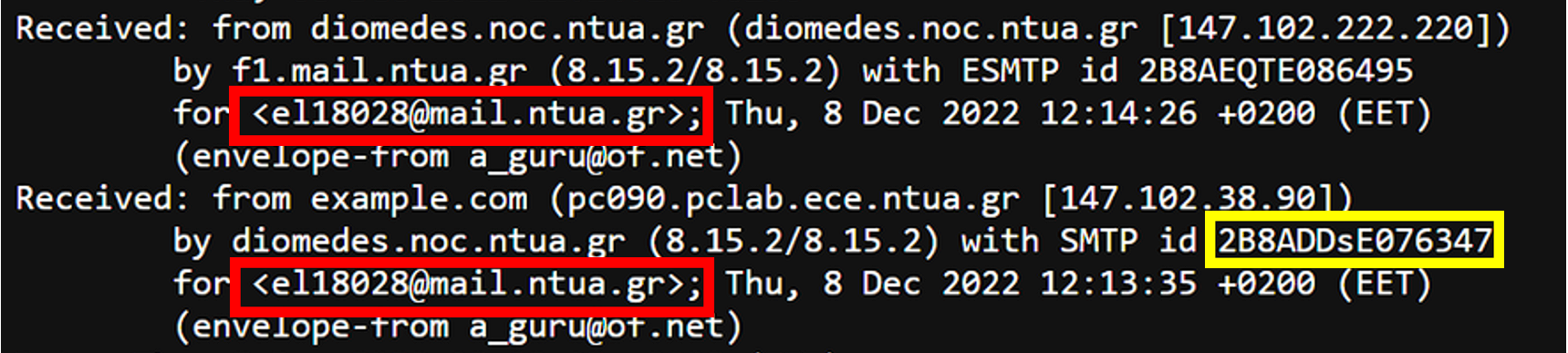
Εμφανίζεται ως παραλήπτης του μηνύματος ο netwoking@apprentice.org, δηλαδή αυτός του κειμένου της επικεφαλίδας To: του μηνύματος.

Εμφανίζουμε τώρα τον πηγαίο κώδικα του μηνύματος που στείλαμε:

***1.19***

Η διεύθυνση αποστολέα του φακέλου a\_guru@of.net εμφανίζεται στην επικεφαλίδα «Return-Path: »

***1.20***

 Η διεύθυνση παραλήπτη του φακέλου el18028@mail.ntua.gr εμφανίζεται σε 2 επικεφαλίδες «Received: » (με κόκκινο χρώμα)

***1.21***

Το αναγνωριστικό που είδαμε στο 1.16 εμφανίζεται στην επικεφαλίδα «Message-Id» καθώς και στην πρώτη επικεφαλίδα «Received: » (με κίτρινο χρώμα)

***1.22***

Το example.com εμφανίζεται στις επικεφαλίδες Χ-Authentication-Warning και στην πρώτη από τις Received επικεφαλίδες.

***1.23***

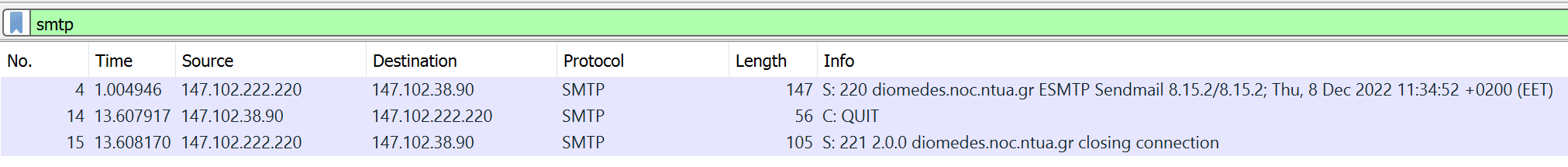
Η ακολουθία επικεφαλίδων Received είναι η εξής: diomedes.noc.ntua.gr → f1.mail.ntua.gr → f1.mail.ntua.gr → m1.mail.ntua.gr.

***1.24***

Προκειμένου να βρούμε τα πρωτόκολλα που χρησιμοποιήθηκαν, θα πρέπει να ψάξουμε τη λέξη κλειδή «with» στις Received επικεφαλίδες του πηγαίου κώδικα. Βλέπουμε επομένως τα εξής: SMTP, ESMTP, LMTPA.

***1.25***

Η ημερομηνία και ώρα που αναφέρει το κείμενο της επικεφαλίδας «Date: » είναι αυτές που δήλωσε αρχικά ο εξυπηρετητής όταν συνδεθήκαμε σε αυτόν.

Εκτελούμε την καταγραφή που ζητείται και έχουμε:

***1.26***

Το φίλτρο σύλληψης είναι: «host relay.ntua.gr».

***1.27***

Το φίλτρο απεικόνισης είναι: «smtp».

***1.28***

Το πρωτόκολλο εφαρμογής SMTP χρησιμοποιεί το πρωτόκολλο μεταφοράς TCP.

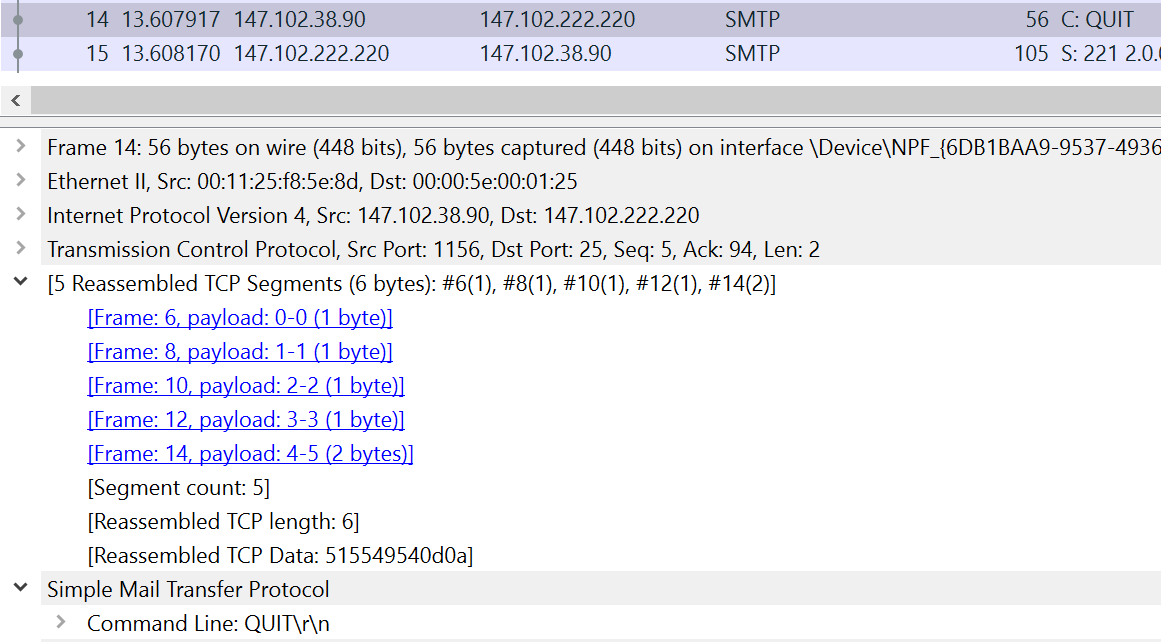
***1.29***

Χρησιμοποιούνται οι θύρες 25 και 1156.

***1.30***

Η θύρα 25 αντιστοιχεί στο πρωτόκολλο εφαρμογής SMTP.

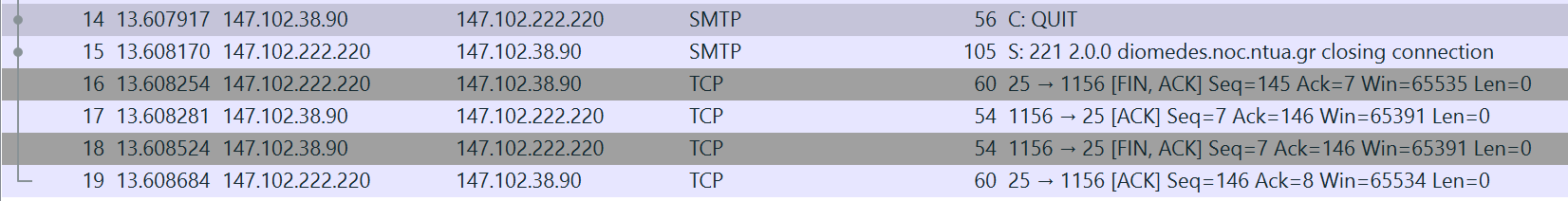
***1.31***

 Η εντολή QUIT απαιτεί 5 TCP τεμάχια, τα 6, 8, 10, 12 και 14.

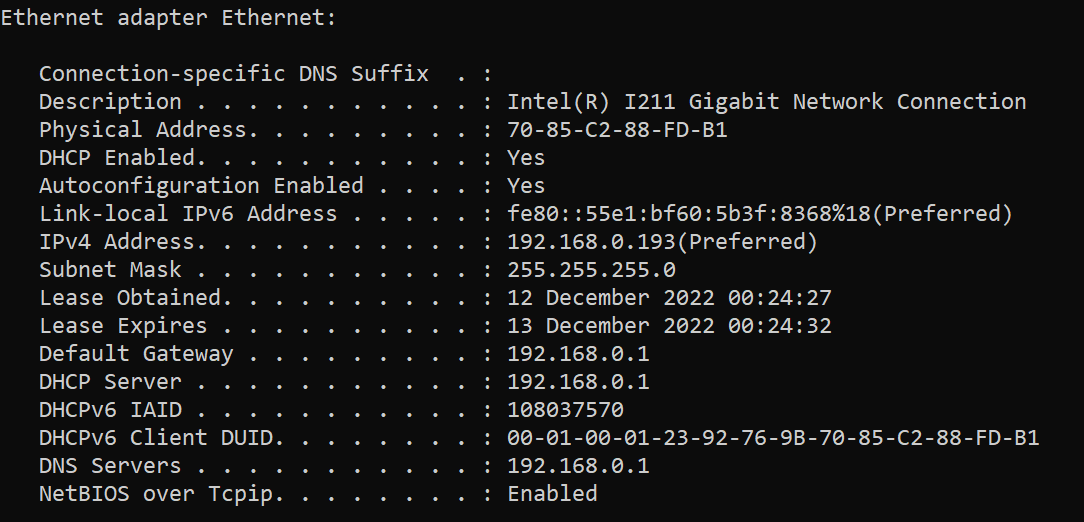
***1.32***

Η απόκριση του εξυπηρετητή στο QUIT είναι η παρακάτω με κωδικό απόκρισης το 221:

***1.33***

Η εντολή QUIT ειδοποιεί τον server πως θέλει να τερματίσει τη σύνδεση. Ο σέρβερ στη συνέχεια απαντά με κατάλληλο μήνυμα τερματισμού σύνδεσης και εν συνεχεία γίνεται η απόλυση TCP συνδέσεων.

**Άσκηση 2: Το πρωτόκολλο DHCP**

Τρέχουμε την εντολή «ipconfig /all»:

***2.1***

Καταγράφουμε τα εξής (Ethernet Adapter):

* ***MAC address της κάρτας δικτύου***: 70-85-C2-88-FD-B1
* ***IPv4 address***: 192.168.0.193
* ***Μάσκα Υποδικτύο***υ: 255.255.255.192
* ***DHCP Server IPv4***: 147.102.136.62

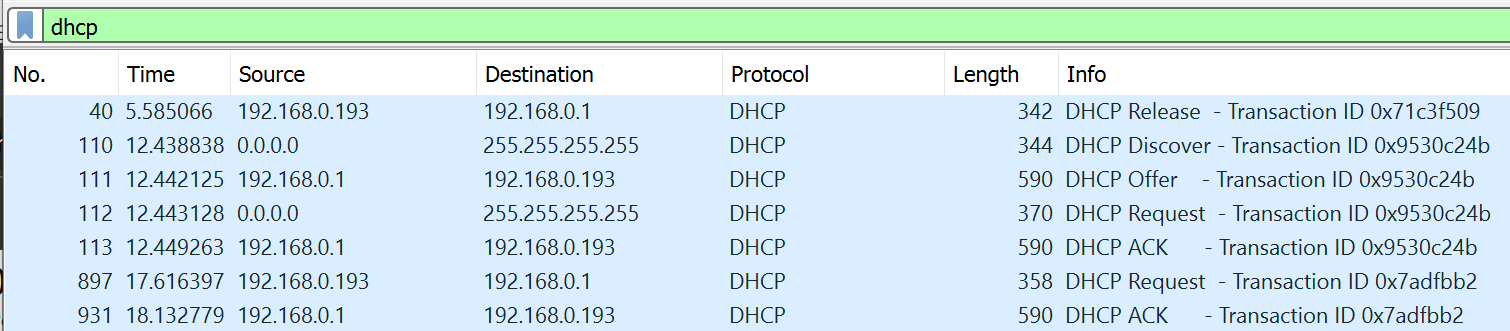
***2.2***

Το φίλτρο απεικόνισης είναι: «dhcp».

***2.3***

Όπως βλέπουμε στο παρακάτω στιγμιότυπο παρήχθησαν τα παρακάτω είδη:

* DHCP Release
* DHCP Discover
* DHCP Offer
* DHCP Request
* DHCP ACK



***2.4***

Χρησιμοποιεί το UDP.

***2.5***

Καταγράφονται οι θύρες 67 και 68.

***2.6***

Οι 2 θύρες αυτές αντιστοιχούν: η 67 στη θύρα Bootstrap Protocol Server, ενώ η 68 στη θύρα Bootstrap Protocol Client.

***2.7***

|  |  |  |  |
| --- | --- | --- | --- |
| **Message Type**  **(1 Byte)** | **Hardware Type**  **(1 Byte)** | **Hardware Address (1 Byte)** | **Hops**  **(1 Byte)** |
| **Transaction ID (4 Bytes)** | | | |
| **Seconds Elapsed (2 Bytes)** | | **Bootp Flags (2 Bytes)** | |
| **Client IP address (4 Bytes)** | | | |
| **Your (client) IP address (4 Bytes)** | | | |
| **Next server IP address (4 Bytes)** | | | |
| **Relay agent IP address (4 Bytes)** | | | |
| **Client MAC address (6 Bytes)** | | | |

***2.8***

Πηγαίνοντας στις πληροφορίες της επικεφαλίδας DHCP, βλέπουμε στα Options, το Option: (53) DHCP Message Type, οπότε και συμπεραίνουμε ότι πρόκειται για DHCP μήνυμα. Επιπλέον, το πεδίο Magic Cookie έχει τιμή DHCP.

***2.9***

Μεταφέρονται τα Boot Request (1) και Boot Reply (2).

***2.10***

Υπάρχουν επιπλέον τα πεδία:

* **Client hardware address padding**
* **Server host name not given**
* **Boot file name not given**
* **Magic Cookie**

***2.11***

Ο τύπος μηνύματος DHCP δηλώνεται από το μήνυμα DHCP Message Type με κωδικό 53.

***2.12***

Καταγράφηκαν τα παρακάτω:

* Πακέτο 40 → Length: 0x01 / DHCP: Release (0x07)
* Πακέτο 110 → Length: 0x01 / DHCP: Discover (0x01)
* Πακέτο 111 → Length: 0x01 / DHCP: Offer (0x02)
* Πακέτο 112 → Length: 0x01 / DHCP: Request (0x03)
* Πακέτο 113 → Length: 0x01 / DHCP: ACK (0x05)
* Πακέτο 897 → Length: 0x01 / DHCP: Request (0x03)
* Πακέτο 931 → Length: 0x01 / DHCP: ACK (0x05)

***2.13***

Το πρώτο DHCP μήνυμα που έστειλε ο υπολογιστής μας είναι ένα DHCP Release μήνυμα, ώστε να αποδεσμεύσει την IP που του είχε δοθεί από τον DHCP.

***2.14***

Τα στοιχεία του αποστολέα ανήκουν στον υπολογιστή μας, ενώ του παραλήπτη ανήκουν στον DHCP server (default gateway).

***2.15***

Στα πακέτα 110, 111, 112, 113 καταγράφονται οι εξής MAC διευθύνσεις:

* Discover (packet 110), Request (packet 111):

***Πηγή***: 70:85:c2:88:fd:b1

***Προορισμός***: ff:ff:ff:ff:ff:ff

* Offer (packet 112), ACK (packet 113):

***Πηγή***: 58:d9:d5:5a:99:50

***Προορισμός***: 70:85:c2:88:fd:b1

***2.16***

Καταγράφονται οι εξής IPv4 διευθύνσεις για τα παρακάτω μηνύματα:

* **Πακέτο 110** **(Discover)** → Αποστολέας: 0.0.0.0 / Παραλήπτης: 255.255.255.255
* **Πακέτο 111** **(Request)**→Αποστολέας: 192.168.0.1/Παραλήπτης: 255.255.255.255
* **Πακέτο 112** **(Offer)** → Αποστολέας: 0.0.0.0 / Παραλήπτης: 255.255.255.255
* **Πακέτο 113** **(ACK)** → Αποστολέας: 192.168.0.1 / Παραλήπτης: 255.255.255.255

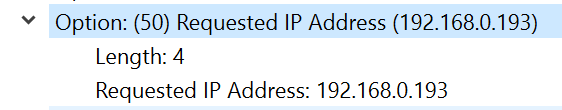
***2.17***

Παραλήπτης του μηνύματος DHCP Discover είναι η διεύθυνση 255.255.255.255, κοινώς γνωστή ως broadcast. Αυτό συμβαίνει καθώς ο υπολογιστής μας “ψάχνει” να βρει κάποιον να του δώσει IP, επομένως ρωτάει κάθε πιθανό κόμβο του υποδικτύου στο οποίο ανήκει.

***2.18***

Στο παραπάνω μήνυμα, ο υπολογιστής μας εμφανίζεται να έχει ως IP το 0.0.0.0, αφού δε του έχει αποδοθεί ακόμα κάποια διεύθυνση.

***2.19***

Στα Options της επικεφαλίδας DHCP βλέπουμε την επιλογή με κωδικό 50 και όνομα Requested IP Address, όπου και ζητείται (προτιμάται) η IP 192.168.0.193 από εμάς.

***2.20***

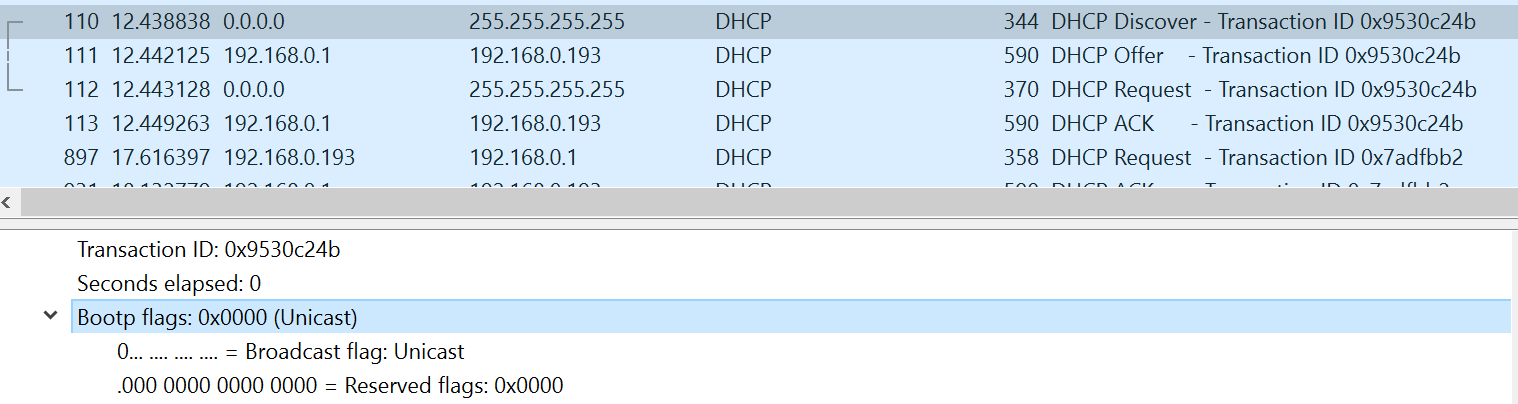
Προτείνεται στον υπολογιστή μας η διεύθυνση 192.168.0.193, η οποία και εμφανίζεται στο πεδίο Your (client) IP address.

***2.21***

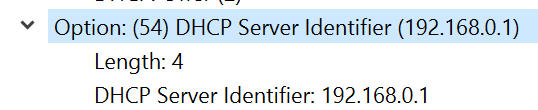
Το προηγούμενο μήνυμα στάλθηκε στην MAC/IP address:

70:85:c2:88:fd:b1/192.168.0.193 αντίστοιχα.

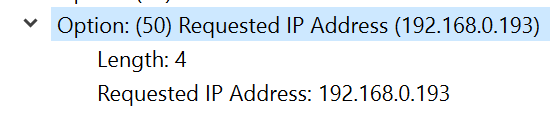
***2.22***

Όπως βλέπουμε στο παραπάνω μήνυμα έχουμε unicast με προορισμό την διεύθυνση IP μας. Πράγματι η bootp flag είναι 0 (unicast) οπότε συμφωνούν οι τιμές.

***2.23***

Η IPv4 διεύθυνση του DHCP server είναι 192.168.0.1 και εμφανίζεται στο Option: (54) DHCP Server Identifier (192.168.0.1).

***2.24***

ΗIPv4 διεύθυνση που ζητάει ο υπολογιστής μας από τον DHCP server στο μήνυμα DHCP Request είναι η 192.168.0.193 και εμφανίζεται στο Option: (50) Requested IP Address (192.168.0.193).

***2.25***

Το προηγούμενο μήνυμα στάλθηκε στην MAC/IP address:

ff:ff:ff:ff:ff:ff/255.255.255.255 αντίστοιχα.

***2.26***

Ο εξυπηρετητής DHCP αναγνωρίζει ότι το μήνυμα απευθύνεται σε εκείνον από το πεδίο Option: DHCP Server Identifier (193.168.0.1) της επικεφαλίδας DHCP του μηνύματος DHCP Request.

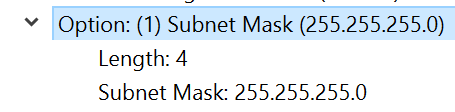
***2.27***

Μας αποδίδεται τελικά η 193.168.0.193, η οποία και φαίνεται στο πεδίο Your (client) IP address.

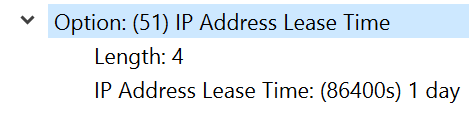
***2.28***

Ναι, συμπίπτει.

***2.29***

Στο ACK πακέτο, στο πεδίο Option: (1) Subnet Mask περιέχεται η τιμή 255.255.255.0, η οποία είναι η μάσκα υποδικτύου για την IPv4 που εκχωρήθηκε.

***2.30***

Η εκχώρηση της IP διεύθυνσης διαρκεί 1 μέρα και αυτό φαίνεται στο πεδίο Option: (51) IP Address Lease Time.

***2.31***

Ο κωδικός είναι ο 55.

***2.32***

* 1 – Subnet Mask – Η τιμή της μάσκας υποδικτύου
* 3 – Router – Λίστα IP διευθύνσεων των router εντός του υποδικτύου του client
* 6 – Domain Name Server – Λίστα διαθέσιμων ονομάτων DNS εξυπηρετητών

***2.33***

Ο υπολογιστής μας ζήτησε 14 παραμέτρους και ο DHCP προσδιόρισε 3 από αυτές, συγκεκριμένα αυτές που αναφέρθηκαν στο ερώτημα 2.32.

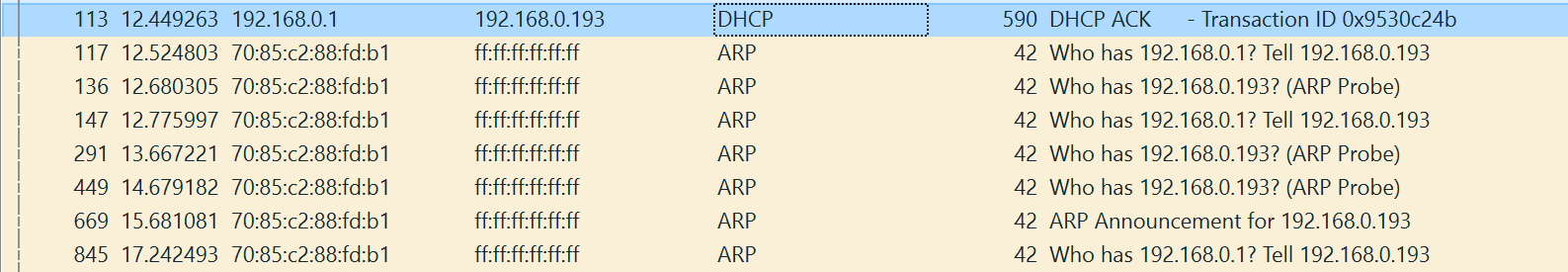
***2.34***

Εφόσον ο υπολογιστής μας καθ’ όλη τη διάρκεια της άσκησης δεν έχει σταθερή IP, χρησιμοποιούμε για το φίλτρο τη MAC address του. Επομένως, συντάσσουμε το «dhcp or (arp and eth.src==70:85:c2:88:fd:b1)».

***2.35***

Ναι.

***2.36***

Παρατηρούνται 7 πλαίσια ARP.

***2.37***

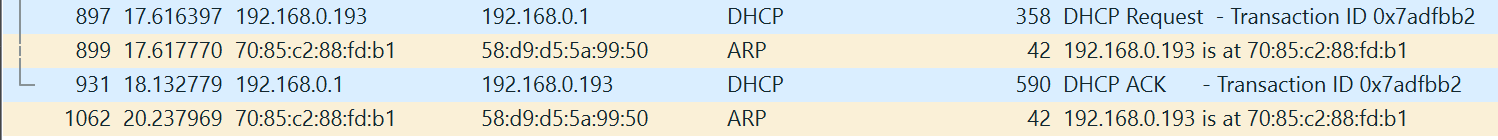
Ναι, τα πλαίσια 136, 291 και 449 αναζητούν την IPv4 του υπολογιστή μας (ARP Probe). Ακόμη ανακοινώνεται στο πλαίσιο 669 (ARP Announcement for 192.168.0.193)

***2.38***

Όπως ξέρουμε, με τα ARP Probe μηνύματα ο υπολογιστής μας ρωτάει συνέχεια το υποδίκτυο (τυπικά στέλνονται 3 ARP Probe) για να βεβαιωθεί πως δε χρησιμοποιεί κανείς άλλος την IP για την οποία ρωτάει, αυτήν που ο ίδιος δηλαδή χρησιμοποιεί. Το ARP Announcement δηλώνει πως ο υπολογιστής μας κατοχυρώνει επίσημα αυτήν την IP (αφού δεν έλαβε απάντηση στα ARP Probe μηνύματα που έστειλε προηγουμένως).

***2.39***

Παρήχθησαν ένα DHCP Request και ένα DHCP ACK.



***2.40***

Διαφέρουν στα παρακάτω πεδία:

* Transaction ID
* Client IP address (0.0.0.0 – 10.3.20.47)
* ΜAC address παραλήπτη (ff:ff:ff:ff:ff:ff – 04:d5:90:da:67:b0)

***2.41***

Όχι, δεν υπάρχει.

***2.42***

Περιλαμβάνεται στην επικεφαλίδα Client IP address, οπότε και διαφέρει σε σχέση με το 2.23 καθώς εκεί ζητούνταν η ίδια διεύθυνση μεν αλλά σε Option.

***2.43***

Περιλαμβάνεται στην επικεφαλίδα Your (client) IP address, όπως και στο 2.27.

***2.44***

***Transaction ID (Release)***: 0x71c3f509

***2.45***

***Transaction ID (πρώτο renew)***: 0x9530c24b

***2.46***

***Transaction ID (δεύτερο renew)***: 0x7adfbb2

***2.47***

Το πεδίο Transaction ID είναι ένας τυχαίος αριθμός επιλεγμένος από τον client, ο οποίος χρησιμοποιείται από τον client και τον server ώστε να συσχετιστούν κατάλληλα τα μηνύματα κατά την μεταξύ τους επικοινωνία.