Εργαστηριακή Άσκηση 9 SMTP, DHCP

ΟΝΟΜΑΤΕΠΩΝΥΜΟ: ΚΟΥΣΤΕΝΗΣ ΧΡΙΣΤΟΣ (03120227)

ΟΜΑΔΑ: 3

ΟΝΟΜΑ PC/ΛΣ: LAPTOP-TK5Q3T95 / WINDOWS 11

ΗΜΕΡΟΜΗΝΙΑ: 07/12/2023

ΔΙΕΥΘΥΝΣΗ IP: 147.102.236.36

ΔΙΕΥΘΥΝΣΗ MAC: B4-B5-B6-79-4B-09

1. Το πρωτόκολλο SMTP

Για την εκτέλεση της άσκησης αυτής θα χρησιμοποιήσετε τη διεύθυνση ηλεκτρονικού σας ταχυδρομείου στο ΕΜΠ elxxxxx@mail.ntua.gr . Εάν δεν το έχετε κάνει στο παρελθόν ενεργοποιήστε την ακολουθώντας τις οδηγίες του ΚΕΔ που θα βρείτε στην ιστοσελίδα http://www.noc.ntua.gr/help/E-mail. Εάν έχετε ενεργό λογαριασμό email, αλλά προωθείτε τα εισερχόμενα μηνύματα σε άλλη διεύθυνση ηλεκτρονικού ταχυδρομείου, ακυρώστε προσωρινά το σχετικό φίλτρο προώθησης. Για τη χρήση της υπηρεσίας ηλεκτρονικού ταχυδρομείου η επικοινωνία με τον εξυπηρετητή SMTP θα γίνει απευθείας από ένα παράθυρο εντολών μέσω TELNET και όχι με κάποιο πρόγραμμα πελάτη. Θα πρέπει να είστε συνδεδεμένοι στο εσωτερικό δίκτυο του ΕΜΠ ώστε να σας επιτραπεί η πρόσβαση στη θύρα 25 του εξυπηρετητή SMTP. Στη συνέχεια, ανοίξτε ένα παράθυρο εντολών και, πληκτρολογήστε με προσοχή το κείμενο που ακολουθεί. Κάθε γραμμή τερματίζεται πατώντας το πλήκτρο . Εάν κάνετε λάθος στην εισαγωγή των χαρακτήρων θα πρέπει να επαναλάβετε την εντολή2 . Ο εξυπηρετητής SMTP αποκρίνεται σε κάθε εντολή θετικά ή αρνητικά.

telnet smtp.ntua.gr 25

HELP

HELO cn.ntua.gr

EHLO cn.ntua.gr

HELP EHLO

QUIT

1.1 Ποια είναι η σημασία του παραπάνω τρόπου κλήσης της εντολής telnet; [Υπόδειξη: Δείτε τεκμηρίωση telnet.]

```
C:\Users\koust>telnet/?

telnet [-a][-e escape char][-f log file][-l user][-t term][host [port]]
 -a      Attempt automatic logon. Same as -l option except uses
         the currently logged on user's name.
 -e      Escape character to enter telnet client prompt.
 -f      File name for client side logging
 -l      Specifies the user name to log in with on the remote system.
         Requires that the remote system support the TELNET ENVIRON option.
 -t      Specifies terminal type.
         Supported term types are vt100, vt52, ansi and vtnt only.
 host    Specifies the hostname or IP address of the remote computer
         to connect to.
 port    Specifies a port number or service name.
```

Προσδιορισμός τόσο του host(smtp.ntua.gr) στον οποίο θα συνδεθεί ο υπολογιστής μας μέσω της υπηρεσίας telnet όσο και του port που θα χρησιμοποιηθεί (25).

Με την εγκατάσταση σύνδεσης στον εξυπηρετητή SMTP, ο εξυπηρετητής αποστέλλει ένα μήνυμα χαιρετισμού αποτελούμενο από ένα κωδικό απόκρισης συνοδευόμενο από το DNS όνομά του και κάποιο αναγνωριστικό κείμενο.

1.2 Ποιος είναι ο κωδικός απόκρισης (Reply code) που αποστέλλει ο εξυπηρετητής SMTP μετά την εγκατάσταση σύνδεσης και ποιο το νόημά του; [Υπόδειξη: Αναζητήστε Reply Codes in Numeric Order στο RFC 5321.]

> *Υπάρχουν τέσσερις τιμές για το πρώτο ψηφίο του reply code:*
>
> *[…]*
>
> ***2yz Θετική απάντηση** ολοκλήρωσης : Η ενέργεια που ζητήθηκε ολοκληρώθηκε με επιτυχία. Μπορεί να υποβληθεί νέο αίτημα.*
>
> *[…]*
>
> *Το δεύτερο ψηφίο κωδικοποιεί τις απαντήσεις σε συγκεκριμένες κατηγορίες:*
>
> *[…]*
>
> ***Συνδέσεις x2z** : Αυτές είναι απαντήσεις που αναφέρονται στο κανάλι μετάδοσης.*
>
> *[…]*
>
> *Το τρίτο ψηφίο δίνει μια αναλυτικότερη διαβάθμιση του νοήματος σε κάθε κατηγορία που καθορίζεται από το δεύτερο ψηφίο. Ο κατάλογος των απαντήσεων το δείχνει αυτό. Κάθε κείμενο απάντησης είναι προτενόμενο και όχι υποχρεωτικό και μπορεί ακόμη και να αλλάξει ανάλογα με την εντολή με την οποία συσχετίζεται. Από την άλλη, οι κωδικοί απάντησης πρέπει να ακολουθούν αυστηρά τις προδιαγραφές που ορίζονται. Οι υλοποιήσεις δεκτών δεν πρέπει να εφευρίσκουν νέους κώδικες για ελαφρώς διαφορετικές καταστάσεις από αυτές που περιγράφονται εδώ, αλλά μάλλον να προσαρμόζουν κώδικες που έχουν ήδη καθοριστεί.*
>
> RFC 5321 - Simple Mail Transfer Protocol (ietf.org)

Έτσι στην περίπτωση μας ισχύει:

220 <domain> Service ready

1.3 Ποιο το DNS όνομα του εξυπηρετητή;
Το DNS όνομα του εξυπηρετητή είναι: smtp3.ntua.gr

1.4 Ποιο είναι το αναγνωριστικό κείμενο;
ESMTP Sendmail 8.15.2/8.15.2; Wed, 6 Dec 2023 15:25:26 +0200 (EET)

1.5 Ποιος είναι ο κωδικός απόκρισης στην εντολή HELP του πρωτοκόλλου SMTP;
Reply code: 214

1.6 Με βάση την απόκριση στην παραπάνω εντολή καταγράψτε το πλήθος των υποστηριζόμενων εντολών από τον εξυπηρετητή καθώς και τα ονόματα τριών από αυτών.

#εντολών = 16

3 από αυτές :

- MAIL
- RCPT
- DATA

1.7 Η απόκριση περιλαμβάνει πολλές γραμμές. Πώς διακρίνεται η τελευταία γραμμή της; [Υπόδειξη: Αναζητήστε multiline replies στην παράγραφο 4.2.1 του RFC 5321.]

Η μορφή για απαντήσεις πολλών γραμμών απαιτεί κάθε γραμμή, εκτός από την τελευταία, να ξεκινάει με τον κωδικό απάντησης, ακολουθούμενο αμέσως από παύλα, "-" (γνωστό και ως μείον), ακολουθούμενο από κείμενο. Η τελευταία γραμμή θα ξεκινάει με τον κωδικό απάντησης, ακολουθούμενο αμέσως από <SP>, προαιρετικά κάποιο κείμενο, και <CRLF>. Οι διακομιστές ΠΡΕΠΕΙ να στείλουν το <SP> εάν δεν αποσταλεί επόμενο κείμενο, αλλά οι πελάτες ΠΡΕΠΕΙ να είναι προετοιμασμένοι για το αν αυτό παραλειφθεί.

1.8 Ποιος είναι ο κωδικός απόκρισης στην εντολή HELO του πρωτοκόλλου SMTP;

Reply code : 250

1.9 Εμφανίζεται στην απόκριση το όνομα υπολογιστή που δηλώνει η εντολή HELO; Εάν όχι, τι περιέχει η απόκριση;

Όχι, η απόκριση περιέχει την IPv4 διεύθυνση του υπολογιστή μας.

```
HELO cn.ntua.gr
250 smtp3.ntua.gr Hello vpn-131-204.vpn.ntua.gr [147.102.131.204], pleased to meet you
```

1.10 Πόσες γραμμές περιλαμβάνει η απόκριση του εξυπηρετητή στην εντολή EHLO του πρωτοκόλλου SMTP;

```
EHLO cn.ntua.gr
250-smtp3.ntua.gr Hello vpn-131-204.vpn.ntua.gr [147.102.131.204], pleased to meet you
250-ENHANCEDSTATUSCODES
250-PIPELINING
250-8BITMIME
250-SIZE
250-ETRN
250-STARTTLS
250-DELIVERBY
250 HELP
```

Η απόκριση περιλαμβάνει 9 γραμμές.

1.11 Τι επιπλέον περιέχει η απόκριση του εξυπηρετητή στην εντολή EHLO του πρωτοκόλλου SMTP σε σχέση με την εντολή HELO; [Υπόδειξη: Δείτε σημείωση για SMTP Service Extensions στην ιστοσελίδα MAIL Parameters (iana.org).]

Η απόκριση διακομιστή σε μια εντολή EHLO υπολογιστή-πελάτη περιλαμβάνει μια λέξη-κλειδί για κάθε επέκταση υπηρεσίας που υλοποιεί ο διακομιστής. Μερικές από αυτές τις λέξεις-κλειδιά έχουν παραμέτρους.

1.12 Είναι προφανές ότι ο εξυπηρετητής smtp.ntua.gr υποστηρίζει το ESMTP. Πότε έγινε αυτό εμφανές για πρώτη φορά;

Στην αρχή της σύνδεσης

```
220 smtp3.ntua.gr ESMTP Sendmail 8.15.2/8.15.2; Wed, 6 Dec 2023 19:13:19 +0200 (EET)
```

Στη συνέχεια στο παράθυρο εντολών πληκτρολογήστε προσεκτικά το κείμενο που ακολουθεί, όπου elxxxxx είναι το όνομα χρήστη που χρησιμοποιείτε για πρόσβαση στις δικτυακές υπηρεσίες του ΕΜΠ. Κάθε γραμμή εντολών τερματίζεται πατώντας το πλήκτρο . Προσοχή στην κενή γραμμή μετά τις επικεφαλίδες και στις διευθύνσεις ηλεκτρονικού ταχυδρομείου που θα πρέπει να περικλείονται από τους χαρακτήρες «<» «>». Όπως και πριν εάν κάνετε λάθος στην εισαγωγή των χαρακτήρων θα πρέπει να επαναλάβετε την εντολή, οπότε καλό θα ήταν να ετοιμάσετε ένα αρχείο κειμένου με τις εντολές και μετά να τις αντιγράφετε μία κάθε φορά στο παράθυρο εντολών.

telnet relay.ntua.gr 25

HELO example.com

MAIL FROM:<a_guru@of.net>

RCPT TO: <el20227@mail.ntua.gr>

DATA

From: netwoking@guru.org

To: netwoking@apprentice.org

Subject: Test Message

This is a test message.

1

2

3

.

QUIT

```
220 achilles.noc.ntua.gr ESMTP Sendmail 8.15.2/8.15.2; Wed, 6 Dec 2023 19:33:38 +0200 (EET)
HELO example.com
250 achilles.noc.ntua.gr Hello vpn-131-204.vpn.ntua.gr [147.102.131.204], pleased to meet you
MAIL FROM:<a_guru@of.net>
250 2.1.0 <a_guru@of.net>... Sender ok
RCPT TO: <el20227@mail.ntua.gr>
250 2.1.5 <el20227@mail.ntua.gr>... Recipient ok
DATA
354 Enter mail, end with "." on a line by itself
From: netwoking@guru.org
To: netwoking@apprentice.org
Subject: Test Message
This is a test message.
1
2
3
.
250 2.0.0 3B6HXcHG022832 Message accepted for delivery
QUIT
221 2.0.0 achilles.noc.ntua.gr closing connection


Connection to host lost.
```

1.13 Καταγράψτε την ημερομηνία και ώρα που δηλώνει στην απόκρισή του ο εξυπηρετητής relay.ntua.gr μόλις συνδεθήκατε σε αυτόν.

Date : Wed, 6 Dec 2023

Time : 19:33:38 +0200 (EET)

1.14 Ποια είναι η απόκριση του εξυπηρετητή και ο αντίστοιχος κωδικός απόκρισης στην εντολή DATA του πρωτοκόλλου SMTP;

Response : 354 Enter mail, end with "." on a line by itself

Reply code ; 354

1.15 Ποιος είναι ο ρόλος της τελείας που πληκτρολογείτε πριν την εντολή QUIT κατά την επικοινωνία SMTP με τον εξυπηρετητή;

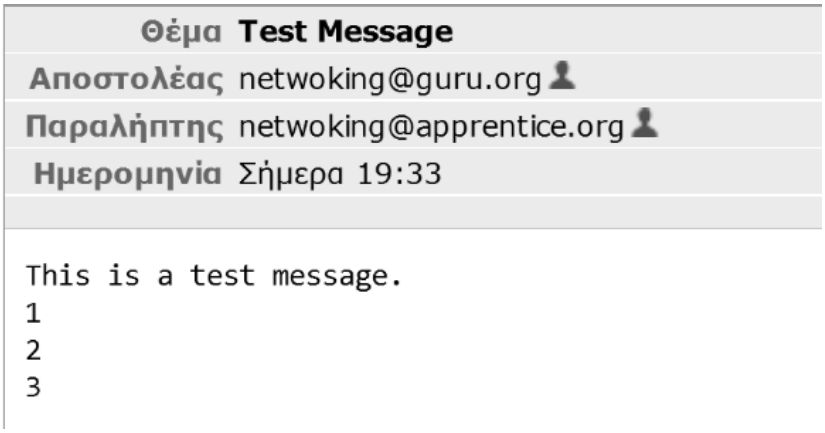
Η τελεία που πληκτρολογούμε πριν την εντολή QUIT δηλώνει το τέλος της εισαγωγής δεδομένων.

1.16 Ποια είναι η απόκριση του εξυπηρετητή και ο αντίστοιχος κωδικός απόκρισης μετά το τέλος της εισαγωγής δεδομένων;

```
Response of Server : 250 2.0.0 3B6HXcHG022832 Message accepted for delivery

Reply code : 250
```

Στη συνέχεια ανοίξτε το ηλεκτρονικό σας ταχυδρομείο μέσω της ιστοσελίδας https://webmail.ntua.gr/, επιλέγοντας τον εξυπηρετητή mail.ntua.gr, για να επιβεβαιώσετε ότι λάβατε το μήνυμα που στείλατε.



1.17 Ποιος εμφανίζεται ως αποστολέας του μηνύματος που λάβατε; Αυτός του φακέλου ή αυτός του κειμένου της επικεφαλίδας From: του μηνύματος;

```
Ως αποστολέας του μηνύματος εμφανίζεται ο <netwoking@guru.org>. Άρα αυτός του
κειμένου της επικεφαλίδας From.
```

1.18 Αφού το ανοίξετε, ποιος εμφανίζεται ως παραλήπτης του μηνύματος; Αυτός του φακέλου ή αυτός του κειμένου της επικεφαλίδας To: του μηνύματος;

```
Ως παραλήπτης του μηνύματος εμφανίζεται ο <netwoking@apprentice.org>. Άρα αυτός του
κειμένου της επικεφαλίδας To.
```

Κάντε κλικ στον οδοντωτό τροχό “Περισσότερες ενέργειες…” και επιλέξτε “Προβολή πηγαίου κώδικα” προκειμένου να εξετάσετε τις επικεφαλίδες του μηνύματος που λάβατε.

1.19 Σε ποια επικεφαλίδα του μηνύματος εμφανίζεται η διεύθυνση αποστολέα του φακέλου που ορίσατε με την εντολή MAIL FROM;

```
Στην επικεφαλίδα Return path ως εξής:

Return-Path: <a_guru@of.net>
```

1.20 Σε ποιες επικεφαλίδες του μηνύματος εμφανίζεται η διεύθυνση παραλήπτη του φακέλου που ορίσατε με την εντολή RCPT TO;

Received: from achilles.noc.ntua.gr (achilles.noc.ntua.gr [147.102.222.210])
by f1.mail.ntua.gr (8.15.2/8.15.2) with ESMTP id 3B6HZhRP000838
for <el20227@mail.ntua.gr>; Wed, 6 Dec 2023 19:35:43 +0200 (EET)
(envelope-from a_guru@of.net)
Received: from example.com (vpn-131-204.vpn.ntua.gr [147.102.131.204])
by achilles.noc.ntua.gr (8.15.2/8.15.2) with SMTP id 3B6HXcHG022832
for <el20227@mail.ntua.gr>; Wed, 6 Dec 2023 19:34:16 +0200 (EET)
(envelope-from a_guru@of.net)

Στις 2 παραπάνω επικεφαλίδες Received.

1.21 Σε ποια επικεφαλίδα εμφανίζεται το αναγνωριστικό που επέστρεψε ο εξυπηρετητής και καταγράψατε στην ερώτηση 1.16;

Στις επικεφαλίδες Message-Id και Received όπως φαίνεται παρακάτω:

Message-Id: <202312061734.3B6HXcHG022832@achilles.noc.ntua.gr>
Received: from example.com (vpn-131-204.vpn.ntua.gr [147.102.131.204])
by achilles.noc.ntua.gr (8.15.2/8.15.2) with SMTP id 3B6HXcHG022832
for <el20227@mail.ntua.gr>; Wed, 6 Dec 2023 19:34:16 +0200 (EET)
(envelope-from a_guru@of.net)

1.22 Σε ποιες επικεφαλίδες εμφανίζεται το δηλωθέν στην εντολή HELO όνομα υπολογιστή;

Στις επικεφαλίδες Received και X-Authentication-Warning όπως φαίνεται παρακάτω:

Received: from example.com (vpn-131-204.vpn.ntua.gr [147.102.131.204])
by achilles.noc.ntua.gr (8.15.2/8.15.2) with SMTP id 3B6HXcHG022832
for <el20227@mail.ntua.gr>; Wed, 6 Dec 2023 19:34:16 +0200 (EET)
(envelope-from a_guru@of.net)
X-Authentication-Warning: achilles.noc.ntua.gr: Host vpn-131-204.vpn.ntua.gr [147.102.131.204] claimed to be example.com

1.23 Εντοπίστε την ακολουθία επικεφαλίδων Received:. Ποια είναι τα ονόματα των MTA που χειρίσθηκαν το μήνυμα;

achilles.noc.ntua.gr ---> f1.mail.ntua.gr(Cyrus v2.3.16) ---> f1.mail.ntua.gr ([unix socket]) ---> m3.mail.ntua.gr

1.24 Ποια πρωτόκολλα χρησιμοποιήθηκαν για την προώθηση του μηνύματος; [Υπόδειξη: Δείτε σημείωση για Mail Transmission Types στην ιστοσελίδα MAIL Parameters(iana.org).]

LMTPA : Local Mail Transfer Protocol

ESMTP : SMTP with Service Extensions

SMTP : Simple Mail Transfer Protocol

1.25 Καταγράψτε την ημερομηνία και ώρα που αναφέρει το κείμενο της επικεφαλίδας Date:. Πώς προέκυψε αυτή αφού δεν την ορίσατε ρητά;

Date: Wed, 6 Dec 2023 19:33:38 +0200 (EET)

Προκύπτει από το response του εξυπηρετητή τη στιγμή που συνδεθήκαμε με την εντολή

telnet relay.ntua.gr 25

Στη συνέχεια με τη βοήθεια του Wireshark καταγράψτε την κίνηση ενώ κάνετε χρήση των υπηρεσιών ηλεκτρονικού ταχυδρομείου του κεντρικού εξυπηρετητή SMTP του ΕΜΠ. Εφαρμόστε φίλτρο σύλληψης για να παρατηρείτε μόνο την κίνηση που σχετίζεται με τη διεύθυνση IPv4 του κεντρικού εξυπηρετητή relay.ntua.gr. Κατόπιν πληκτρολογήστε το κείμενο που ακολουθεί. Κάθε γραμμή τερματίζεται πατώντας το πλήκτρο <Enter>.

telnet relay.ntua.gr 25

NOOP

QUIT

Αφού σταματήσετε την καταγραφή της κίνησης, εφαρμόστε ένα φίλτρο απεικόνισης ώστε να παραμείνουν μόνο μηνύματα σχετικά με την υπηρεσία SMTP και απαντήστε στα εξής:

1.26 Ποιο είναι το φίλτρο σύλληψης που εφαρμόσατε;

Capture filter : ***host relay.ntua.gr***

1.27 Ποιο είναι το φίλτρο απεικόνισης που εφαρμόσατε;

Display filter : ***smtp***

1.28 Ποιο πρωτόκολλο μεταφοράς χρησιμοποιεί το πρωτόκολλο εφαρμογής SMTP;

Το πρωτόκολλο μεταφοράς TCP

1.29 Καταγράψτε τις θύρες (προέλευσης και προορισμού) του πρωτοκόλλου μεταφοράς που χρησιμοποιούνται για την επικοινωνία.

Source port : 54404 (147.102.236.36) ---> Destination port : 25 (147.102.222.210)

Source port : 25 (147.102.222.210) ---> Destination port : 54404 (147.102.236.36)

1.30 Ποια από τις παραπάνω θύρες αντιστοιχεί στο πρωτόκολλο εφαρμογής SMTP;

Port 25

1.31 Πόσα τεμάχια TCP απαιτήθηκαν για τη μεταφορά των δύο εντολών προς τον εξυπηρετητή;

NOOP

5 TCP Segments (6 bytes): #6(1), #8(1), #10(1), #12(1), #14(2)

QUIT

5 TCP Segments (6 bytes): #17(1), #19(1), #21(1), #23(1), #25(2)

1.32 Ποια είναι η απόκριση του εξυπηρετητή και ο αντίστοιχος κωδικός απόκρισης στην εντολή QUIT του πρωτοκόλλου SMTP;

Response: 221 2.0.0 achilles.noc.ntua.gr closing connection\r\n

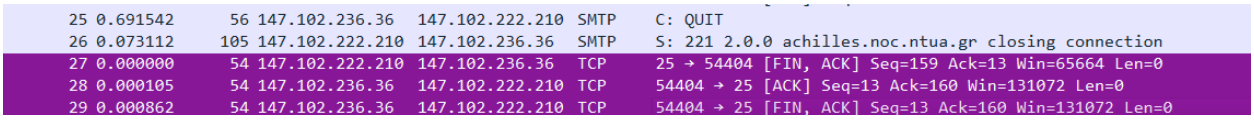
Reply code: 221

1.33 Προκαλεί η εντολή QUIT του πρωτοκόλλου SMTP την άμεση απόλυση της σύνδεσης με τον εξυπηρετητή; Γιατί; [Υπόδειξη: Αναζητήστε εντολή QUIT στο RFC 821.]

> *The receiver should not close the transmission channel until it receives and replies to a QUIT command (even if there was an error). The sender should not close the transmission channel until it send a QUIT command and receives the reply (even if there was an error response to a previous command).*
>
> RFC 821

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. Ο αποστολέας της εντολής QUIT, στην προκειμένη περίπτωση ο υπολογιστής μας, κλείνει το κανάλι μετάδοσης μόνο αφού λάβει την απάντηση του εξυπηρετητή στο QUIT που έστειλε νωρίτερα.

1.34 Ακυρώστε το φίλτρο απεικόνισης. Από ποια πλευρά ξεκινά η απόλυση της σύνδεσης;



25	0.691542	56	147.102.236.36	147.102.222.210	SMTP	C: QUIT
26	0.073112	105	147.102.222.210	147.102.236.36	SMTP	S: 221 2.0.0 achilles.noc.ntua.gr closing connection
27	0.000000	54	147.102.222.210	147.102.236.36	TCP	25 → 54404 [FIN, ACK] Seq=159 Ack=13 Win=65664 Len=0
28	0.000105	54	147.102.236.36	147.102.222.210	TCP	54404 → 25 [ACK] Seq=13 Ack=160 Win=131072 Len=0
29	0.000862	54	147.102.236.36	147.102.222.210	TCP	54404 → 25 [FIN, ACK] Seq=13 Ack=160 Win=131072 Len=0

Όπως φαίνεται στην παραπάνω εικόνα η απόλυση της σύνδεσης ξεκινά από την πλευρά του εξυπηρετητή(πακέτο 27) ο οποιός αφού στείλει reply στο QUIT πακέτο του υπολογιστή μας αρχίζει την απόλυση.

2. Το πρωτόκολλο DHCP

Στη συνέχεια με τη βοήθεια του Wireshark θα καταγράψετε την κίνηση στο τοπικό δίκτυο του εργαστηρίου ενώ κάνετε χρήση της υπηρεσίας DHCP. Για τον λόγο αυτό, προτού ξεκινήσετε την καταγραφή, δείτε τις τρέχουσες ρυθμίσεις της κάρτας δικτύου του υπολογιστή σας. Προς τούτο, σε περιβάλλον Windows ανοίξτε ένα παράθυρο εντολών και εκτελέστε την εντολή ipconfig /all. Σε περιβάλλον Unix χρησιμοποιήστε τις εντολές ifconfig και route, ενώ σε Linux τις εντολές ip addr και ip route (ή την nmcli device show).

```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : MediaTek Wi-Fi 6 MT7921 Wireless LAN Card
   Physical Address. . . . . . . . . : B4-B5-B6-79-4B-09
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::f47c:cb85:e619:df1c%25(Preferred)
   IPv4 Address. . . . . . . . . . . : 147.102.236.36(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.252.0
   Lease Obtained. . . . . . . . . . : Πέμπτη, 7 Δεκεμβρίου 2023 10:06:19 πμ
   Lease Expires . . . . . . . . . . : Πέμπτη, 7 Δεκεμβρίου 2023 12:31:49 μμ
   Default Gateway . . . . . . . . . : 147.102.236.200
   DHCP Server . . . . . . . . . . . : 147.102.236.230
   DHCPv6 IAID . . . . . . . . . . . : 179615158
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-28-E4-22-72-7C-8A-E1-A2-9F-DD
   DNS Servers . . . . . . . . . . . : 2001:4860:4860::8888
                                       2001:4860:4860::8844
                                       8.8.8.8
                                       8.8.4.4
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

2.1. Καταγράψτε τη διεύθυνση MAC της κάρτας δικτύου, τη διεύθυνση IPv4, τη μάσκα υποδικτύου και τη διεύθυνση IPv4 του εξυπηρετητή DHCP που είναι υπεύθυνος για τις ρυθμίσεις αυτές.

```
Physical Address(Mac Address) : B4-B5-B6-79-4B-09

IPv4 Address : 147.102.236.36

Subnet Mask : 255.255.252.0
```

DHCP Server IPv4 Addresss: 147.102.236.230

Με τη βοήθεια του Wireshark ξεκινήστε μια νέα καταγραφή της κίνησης με φίλτρο σύλληψης τη διεύθυνση MAC της κάρτας δικτύου του υπολογιστή σας προκειμένου να μελετήσετε τα μηνύματα DHCP που ανταλλάσσονται κατά την εκχώρηση/αποδέσμευση των ρυθμίσεων IPv4. Κατόπιν σε περιβάλλον Windows εκτελέστε την εντολή ipconfig /release (σε Linux sudo dhclient-r), που θα προκαλέσει την αποδέσμευση των ρυθμίσεων της κάρτας δικτύου του υπολογιστή σας. Έπειτα εκτελέστε την εντολή ipconfig /renew (σε Linux sudo dhclient), προκειμένου να εκχωρηθούν νέες δικτυακές ρυθμίσεις στον υπολογιστή σας. Περιμένετε έως ότου ολοκληρωθεί η εκχώρηση και εκτελέστε πάλι την εντολή ipconfig /renew (σε Linux sudo dhclient), ώστε να ανανεώσετε τις ρυθμίσεις. Όταν ολοκληρωθεί και η εκτέλεση της δεύτερης εντολής, σταματήστε την καταγραφή μηνυμάτων από το Wireshark.

2.2. Ποιο είναι το φίλτρο σύλληψης που εφαρμόσατε;
Capture filter : ***ether host B4-B5-B6-79-4B-09***

2.3. Εφαρμόστε κατάλληλο φίλτρο απεικόνισης ώστε να εμφανίζονται μόνο μηνύματα DHCP. Ποια είναι η σύνταξή του;
Display filter : ***dhcp***

2.4. Ποια είδη μηνυμάτων DHCP παρήχθησαν από την αλληλουχία εντολών απόλυσης (release), εκχώρησης (πρώτο renew) και ανανέωσης (δεύτερο renew) δικτυακών ρυθμίσεων;

- DHCP Release
- DHCP Discover
- DHCP Offer
- DHCP Request
- DHCP ACK

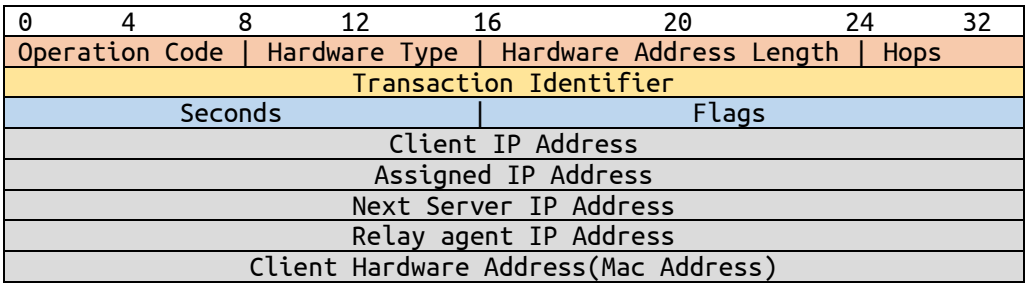
2.5. Ποιο πρωτόκολλο μεταφοράς χρησιμοποιεί το DHCP;
UDP

2.6. Καταγράψτε τις θύρες πηγής και προορισμού των παραπάνω μηνυμάτων.
Source port: 68(147.102.236.36 ή 0.0.0.0) ---> Destination port: 67(147.102.236.230)

Source port: 67(147.102.236.230) ---> Destination port: 68(147.102.236.36)

2.7. Ποιες από τις παραπάνω θύρες αντιστοιχούν στις συνήθεις θύρες (well-known ports) της υπηρεσίας DHCP; [Υπόδειξη: Συμβουλευτείτε τις τιμές των πασίγνωστων θυρών στην ιστοσελίδα https://en.wikipedia.org/wiki/Well_known_ports.]
Και οι δύο θύρες που χρησιμοποιούνται, δηλαδή και η 67 και η 68 είναι συνήθεις θύρες για τον server και τον client αντίστοιχα της υπηρεσίας DHCP.

2.8. Το DHCP ως επέκταση του πρωτοκόλλου BOOTP έχει την ίδια δομή επικεφαλίδων με αυτό. Σημειώστε στο σχήμα τα ονόματα των πεδίων της επικεφαλίδας του μηνύματος BOOTP μέχρι και αυτό που περιέχει τη διεύθυνση MAC πελάτη.



2.9. Πώς γίνεται κατανοητό ότι το μήνυμα BOOTP μεταφέρει επιλογές DHCP, δηλαδή, πρόκειται για μήνυμα DHCP; [Υπόδειξη: Δείτε παράγραφο 3. The Client-Server Protocol στο RFC 2131.]
Πηγαίνοντας στις πληροφορίες της επικεφαλίδας DHCP, βλέπουμε στα Options ***Option: (53) DHCP Message Type***, οπότε και συμπεραίνουμε ότι πρόκειται για DHCP μήνυμα.
Επιπλέον, το πεδίο ***Magic Cookie έχει τιμή DHCP***.

2.10. Ποια είδη μηνυμάτων BOOTP μεταφέρουν τα μηνύματα DHCP που καταγράψατε προηγουμένως;
Μεταφέρονται τα **Boot Request (1)** και **Boot Reply (2).**

2.11. Ποια άλλα πεδία της επικεφαλίδας BOOTP, πλην αυτών που σημειώσατε στο σχήμα, υπάρχουν πριν τις επιλογές DHCP;
Client hardware address padding

Server host name

Server host name

2.12. Ποιος είναι ο κωδικός της επιλογής (option) που δηλώνει τον τύπο του μηνύματος DHCP (DHCP Message Type);
Ο τύπος μηνύματος DHCP δηλώνεται από το μήνυμα DHCP Message Type με κωδικό 53.

2.13. Καταγράψτε το μήκος και την τιμή του πεδίου της επιλογής (option) που προσδιορίζει τον τύπο μηνύματος DHCP. [Υπόδειξη: Στο παράθυρο λεπτομερειών πακέτου του Wireshark αναπτύξτε το περιεχόμενο της επιλογής DHCP Message Type.]

Length: 1

DHCP: Discover (1) / Offer (2) / Request (3) / ACK (5) / Release (7)

2.14. Ποιο είναι το πρώτο μήνυμα DHCP που έστειλε ο υπολογιστής σας; Ποιος ο σκοπός του;
Ένα μήνυμα τύπου DHCP Release. Σκοπός του είναι να αποδεσμεύσει την IP που του είχε δοθεί από τον DHCP.

2.15. Πού ανήκουν οι διευθύνσεις MAC και IPv4 του αποστολέα και του παραλήπτη του παραπάνω μηνύματος;

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

Όπως προαναφέρθηκε, η διεύθυνση IPv4 που εκχωρείται στον υπολογιστή σας, επιβεβαιώνεται στο τέλος της ανταλλαγής των μηνυμάτων DHCP Discover/Offer/Request/ACK μεταξύ του υπολογιστή σας και του εξυπηρετητή DHCP.

2.16. Καταγράψτε τις MAC διευθύνσεις πηγής και προορισμού που χρησιμοποιήθηκαν στα μηνύματα DHCP Discover/Offer/Request/ACK.

- Discover
  Source : b4:b5:b6:79:4b:09, Destination : ff:ff:ff:ff:ff:ff

- Offer
  Source : 00:50:56:b5:aa:aa, Destination: b4:b5:b6:79:4b:09

- Request
  Source: b4:b5:b6:79:4b:09, Destination : 00:50:56:b5:aa:aa

- ACK
  Source : 00:50:56:b5:aa:aa, Destination: b4:b5:b6:79:4b:09

2.17. Καταγράψτε τις διευθύνσεις IPv4 αποστολέα και παραλήπτη των παραπάνω μηνυμάτων.

- Discover
  Source : 0.0.0.0, Destination : 255.255.255.255

- Offer
  Source : 147.102.236.230, Destination : 147.102.236.36

- Request
  1st -> Source: 0.0.0.0, Destination : 255.255.255.255

  2nd -> Source: 147.102.236.36, Destination : 147.102.236.230

  3rd -> Source: 147.102.236.36, Destination : 147.102.236.230

- ACK
  Source : 147.102.236.230, Destination : 147.102.236.36

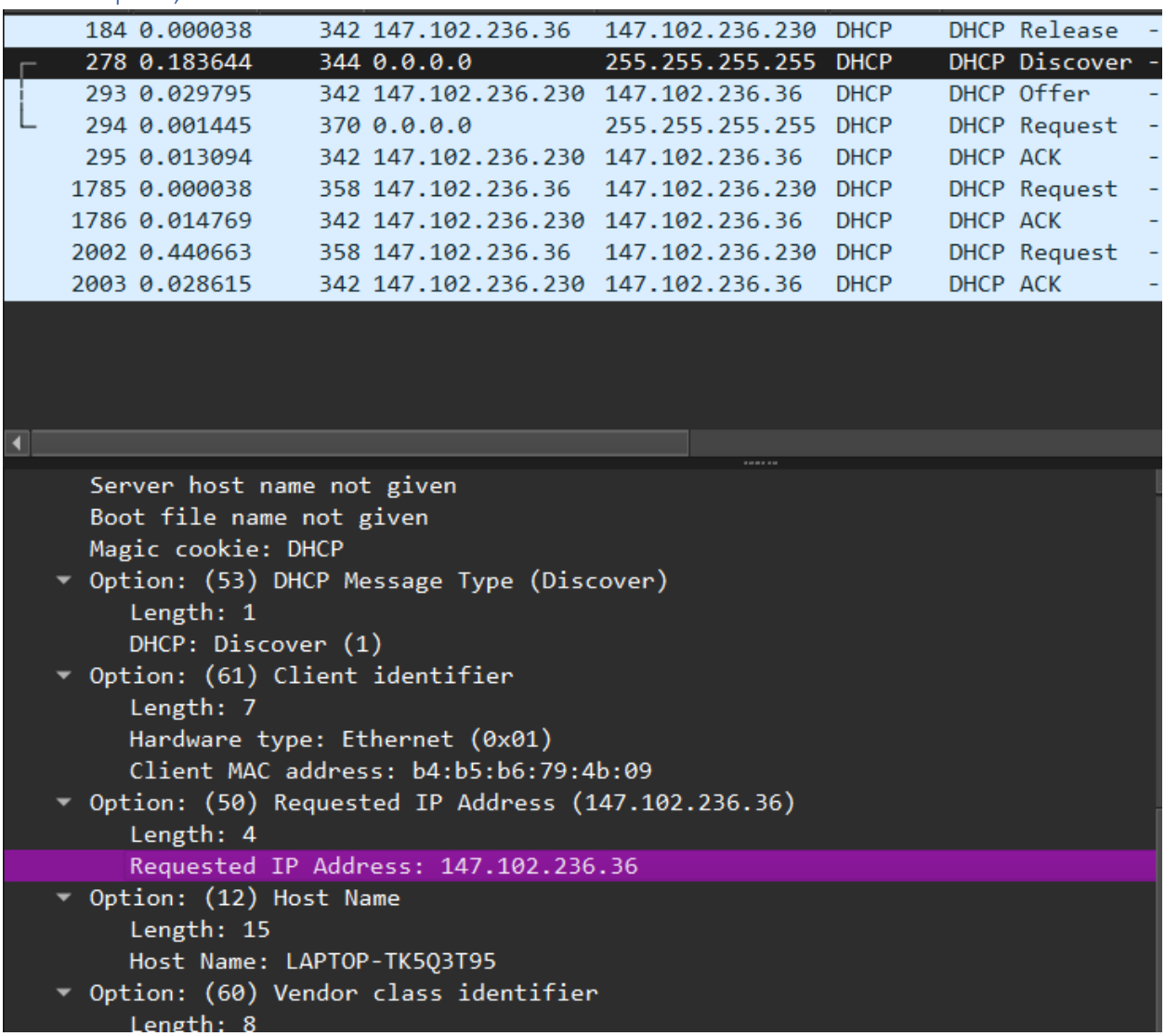
2.18. Τι υποδηλώνει η διεύθυνση IPv4 του παραλήπτη του μηνύματος DHCP Discover;

Παραλήπτης του μηνύματος DHCP Discover είναι η διεύθυνση 255.255.255.255, γνωστή ως broadcast address. Ο υπολογιστής μας επιχειρεί να μεταδωσεί το request του σε όλες τις συσκευές του δικτύου ώστε να βρει κάποιον κόμβο να του αναθέσει IP.

2.19. Δεδομένου ότι το παραπάνω μήνυμα προέρχεται από τον υπολογιστή σας, αιτιολογήστε τη χρήση της διεύθυνσης 0.0.0.0 ως IPv4 διεύθυνσης αποστολέα.

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

2.20. Εκφράζει ο υπολογιστής σας κάπου στο μήνυμα DHCP Discover προτίμηση για τη ζητούμενη διεύθυνση IPv4;



Στο πεδίο Requested IP Address ο υπολογιστής μας κάνει request να του αποδοθεί η διεύθυνση 147.102.236.36

2.21. Πόσα μηνύματα DHCP Offer παρατηρείτε και από ποιες IPv4 διευθύνσεις αποστολέα;
Ένα μόνο μήνυμα DHCP Offer παρατηρείται και η IPv4 του αποστολέα αντιστοιχεί στο default gateway.

2.22. Σε περίπτωση που παρατηρήσατε πάνω από ένα μήνυμα DHCP Offer, εντοπίστε αυτό που έστειλε ο εξυπηρετητής DHCP της ερώτησης 2.1. Ποια είναι η διεύθυνση IPv4 που προτείνει ο εξυπηρετητής DHCP στον υπολογιστή σας και σε ποιο πεδίο της επικεφαλίδας περιέχεται η τιμή της;
Είναι η προηγούμενη τιμή που είχε ο υπολογιστής μας πριν γίνει Release.

Your (client) IP address: 147.102.236.36

2.23. Προς ποια διεύθυνση (MAC και IPv4) στάλθηκε το προηγούμενο μήνυμα DHCP Offer;
Destination

IPv4 : 147.102.236.36

MAC Address : b4:b5:b6:79:4b:09

2.24. Ο πελάτης DHCP δηλώνει στην επικεφαλίδα Bootp flags των αιτημάτων του το κατά πόσο μπορεί να δεχθεί απαντήσεις με μονοεκπομπή (unicast) ή εκπομπή (broadcast) πακέτων IP, θέτοντας αντίστοιχα την τιμή της σημαίας Broadcast flag σε 0 ή 1. Είναι σύμφωνες οι διευθύνσεις του προηγούμενου ερωτήματος με την τιμή της Broadcast flag στο μήνυμα DHCP Discover;
Ναι, είναι.

2.25. Σε ποια επιλογή (option) του μηνύματος DHCP Offer δηλώνει ο εξυπηρετητής DHCP την ταυτότητά του;
Option: (54)

DHCP Server Identifier : 147.102.236.230

2.26. Ποια είναι η IPv4 διεύθυνση πηγής του μηνύματος DHCP Request με το οποίο ο υπολογιστής σας ζητά από τον εξυπηρετητή DHCP την εκχώρηση διεύθυνσης IPv4; Γιατί;
Ισχύει,

Source IPv4 address: 0.0.0.0

Γιατί δεν έχει γίνει ανάθεση διεύθυνσης ακόμα.

2.27. Ποια είναι η διεύθυνση IPv4 που ζητά ο υπολογιστής σας από τον εξυπηρετητή DHCP και σε ποια επικεφαλίδα ή επιλογή (option) του DHCP Request περιέχεται η τιμή της;
Ζητά την τιμή 147.102.236.36 και βρίσκεται στην επιλογή

Option: (50) στο πεδίο Requested IP Address : 147.102.236.36

2.28. Προς ποια διεύθυνση (MAC και IPv4) στάλθηκε το προηγούμενο μήνυμα DHCP Request;
Destination

Mac Address: ff:ff:ff:ff:ff:ff, IPv4 Address: 255.255.255.255

2.29. Πώς αναγνωρίζει ο εξυπηρετητής DHCP ότι το μήνυμα απευθύνεται σε αυτόν και όχι σε κάποιον άλλο; [Υπόδειξη: Δείτε επιλογές (options) και απάντηση στην ερώτηση 2.25.]

Ο κατάλληλος DHCP σέρβερ αναγνωρίζει ότι το μήνυμα απευθύνεται σε εκείνον από το πεδίο Option : (54) DHCP Server Identifier : 147.102.236.230.

2.30. Ποια διεύθυνση IPv4 αποδίδεται τελικά στον υπολογιστής σας με το μήνυμα DHCP ACK και σε ποιο πεδίο της επικεφαλίδας περιέχεται η τιμή της;
Η διεύθυνση 147.102.236.36 και περιέχεται στο πεδίο

Your (client) IP address: 147.102.236.36

2.31. Συμπίπτει η διεύθυνση IPv4 που εκχωρήθηκε με αυτή που είχατε καταγράψει αρχικά στο ερώτημα 2.1;
Ναι, συμπίπτει.

2.32. Ποια είναι η μάσκα υποδικτύου για τη διεύθυνση IPv4 που εκχωρήθηκε και σε ποια επιλογή (option) περιέχεται η τιμή της;
Option: (1) Subnet Mask (255.255.252.0)

2.33. Πόσο διαρκεί η περίοδος δανεισμού αυτής της διεύθυνσης IPv4 και πότε πρέπει να ζητηθεί η ανανέωσή της; Σε ποιες επιλογές (options) περιέχονται οι αντίστοιχες τιμές;
Διαρκεί 10 λεπτά και οι τιμές περιέχονται στα εξής πεδία

Option: (51) IP Address Lease Time

IP Address Lease Time: 10 minutes (600)

Εκτός από τη διεύθυνση IPv4, ο υπολογιστής σας χρησιμοποιεί το DHCP για να λάβει και άλλες δικτυακές παραμέτρους αναγκαίες για τη λειτουργία του. Παρατηρώντας τα περιεχόμενα του μηνύματος DHCP Discover του υπολογιστή σας, θα βρείτε την επιλογή (option) Parameter Request List που περιλαμβάνει τη λίστα των ζητούμενων δικτυακών παραμέτρων.

2.34. Να καταγραφεί ο κωδικός της επιλογής (option) Parameter Request List.
Option: (55) Parameter Request List

2.35. Να καταγραφούν οι κωδικοί, τα ονόματα, καθώς και η σημασία τριών παραμέτρων που ζητάει ο υπολογιστής σας (π.χ. 15 – Domain Name – Το όνομα της περιοχής DNS που ανήκει ο υπολογιστής). [Υπόδειξη: Για μια σύντομη περιγραφή της σημασίας των παραμέτρων συμβουλευτείτε την ιστοσελίδα https://www.iana.org/assignments/bootp-dhcp-parameters.]

1 - Subnet Mask - Η τιμή της μάσκας υποδικτύου

3 - Router - Λίστα IP διευθύνσεων των router εντός του υποδικτύου του client

15 - Domain Name - The DNS domain name of the client

119 - Domain Search - DNS domain search list

2.36. Πόσες παραμέτρους ζήτησε ο υπολογιστής σας με το μήνυμα DHCP Discover και ποιες προσδιορίζει τελικά ο εξυπηρετητής στο μήνυμα DHCP Offer; [Υπόδειξη: Εμφανίστε το ένα εκ των δύο πακέτων σε νέο παράθυρο κάνοντας, στη λίστα των καταγεγραμμένων πακέτων, δεξί κλικ στη γραμμή του και μετά επιλέγοντας Show Packet in New Window.]

Ο υπολογιστής μας ζήτησε 14 παραμέτρους εκ των οποίων προσδιορίστηκαν οι εξής στο DHCP Offer μήνυμα :

- ✓ 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

Μετά τη λήψη της διεύθυνσης IPv4, ο υπολογιστής σας επιβεβαιώνει ότι αυτή είναι πραγματικά διαθέσιμη (δεν χρησιμοποιείται από άλλον).

2.37. Τροποποιήστε το φίλτρο απεικόνισης ώστε εκτός των μηνυμάτων DHCP να εμφανίζονται και πλαίσια ARP που στέλνει ο υπολογιστής σας. Ποια είναι η νέα σύνταξη του φίλτρου απεικόνισης;

Display filter : ***dhcp or (arp and eth.src==b4:b5:b6:79:4b:09)***

2.38. Παρατηρείτε την αποστολή πλαισίων ARP από τον υπολογιστή σας αμέσως μετά το μήνυμα DHCP ACK;

Ναι.

294	0.001445	370	0.0.0.0	255.255.255.255	DHCP	DHCP Request - Transaction ID 0x6
295	0.013094	342	147.102.236.230	147.102.236.36	DHCP	DHCP ACK - Transaction ID 0x6
299	0.111553	42	b4:b5:b6:79:4b…	ff:ff:ff:ff:ff…	ARP	Who has 169.254.208.207? (ARP Prob
305	0.029655	42	b4:b5:b6:79:4b…	ff:ff:ff:ff:ff…	ARP	Who has 147.102.236.200? Tell 147.
308	0.000443	42	b4:b5:b6:79:4b…	ff:ff:ff:ff:ff…	ARP	Who has 147.102.236.200? Tell 147.
334	0.001844	42	b4:b5:b6:79:4b…	ff:ff:ff:ff:ff…	ARP	Who has 147.102.236.200? Tell 147.
427	0.008746	42	b4:b5:b6:79:4b…	ff:ff:ff:ff:ff…	ARP	Who has 147.102.236.200? Tell 147.
452	0.015471	42	b4:b5:b6:79:4b…	ff:ff:ff:ff:ff…	ARP	Who has 147.102.236.36? (ARP Probe
507	0.000810	42	b4:b5:b6:79:4b…	ff:ff:ff:ff:ff…	ARP	Who has 147.102.239.14? Tell 147.1
508	0.000271	42	b4:b5:b6:79:4b…	ff:ff:ff:ff:ff…	ARP	Who has 147.102.239.222? Tell 147.
661	0.018144	42	b4:b5:b6:79:4b…	ff:ff:ff:ff:ff…	ARP	Who has 147.102.236.36? (ARP Probe
749	0.072296	42	b4:b5:b6:79:4b…	ff:ff:ff:ff:ff…	ARP	Who has 147.102.239.222? Tell 147.
926	0.000221	42	b4:b5:b6:79:4b…	ff:ff:ff:ff:ff…	ARP	Who has 147.102.236.36? (ARP Probe
1051	0.005715	42	b4:b5:b6:79:4b…	ff:ff:ff:ff:ff…	ARP	Who has 147.102.239.222? Tell 147.
1085	0.004629	42	b4:b5:b6:79:4b…	ff:ff:ff:ff:ff…	ARP	ARP Announcement for 147.102.236.3
1198	0.012415	42	b4:b5:b6:79:4b…	ff:ff:ff:ff:ff…	ARP	Who has 147.102.239.222? Tell 147.
1269	0.035874	42	b4:b5:b6:79:4b…	ff:ff:ff:ff:ff…	ARP	Who has 147.102.239.222? Tell 147.
1287	0.093861	42	b4:b5:b6:79:4b…	ff:ff:ff:ff:ff…	ARP	ARP Announcement for 147.102.236.3
1304	0.030940	42	b4:b5:b6:79:4b…	ff:ff:ff:ff:ff…	ARP	Who has 147.102.239.222? Tell 147.
1424	0.159594	42	b4:b5:b6:79:4b…	ff:ff:ff:ff:ff…	ARP	Who has 147.102.239.222? Tell 147.
1426	0.653207	42	b4:b5:b6:79:4b…	ff:ff:ff:ff:ff…	ARP	Who has 147.102.239.222? Tell 147.
1445	0.628404	42	b4:b5:b6:79:4b…	ff:ff:ff:ff:ff…	ARP	Who has 147.102.239.222? Tell 147.
1475	0.001423	42	b4:b5:b6:79:4b…	ff:ff:ff:ff:ff…	ARP	Who has 147.102.239.222? Tell 147.
1488	0.015640	42	b4:b5:b6:79:4b…	ff:ff:ff:ff:ff…	ARP	Who has 147.102.239.222? Tell 147.

2.39. Εάν ναι, πόσα τέτοια πλαίσια ARP στάλθηκαν; Εάν όχι, αγνοήστε τις επόμενες δύο ερωτήσεις.

Μετά το πρώτο ACK --> 34

Μετά το δεύτερο --> 13

Μετά το τρίτο --> 19

2.40. Παρατηρείτε πλαίσια ARP με τα οποία αναζητείται ή ανακοινώνεται η διεύθυνση IPv4 του υπολογιστή σας;
Ναι.

2.41. Εξηγήστε τη χρησιμότητα αυτών των πλαισίων ARP [Υπόδειξη: Δείτε “ARP probe and ARP Announcement” και “Gratuitous ARP”.];

Τόσο το **ARP Probe** όσο και το **ARP Announcement** χρησιμοποιούνται σε μια διαδικασία γνωστή ως εντοπισμός διπλότυπων διευθύνσεων. Αν ένας υπολογιστής αποκτήσει και χρησιμοποιήσει μια διεύθυνση IP που τυχαίνει να χρησιμοποιείται ήδη στο δίκτυο, θα προκαλέσει προβλήματα συνδεσιμότητας και για τους δύο υπολογιστές. Ως εκ τούτου, είναι επωφελές για έναν υπολογιστή να δοκιμάσει πρώτα μια διεύθυνση IP πριν τη χρησιμοποιήσει για να διασφαλίσει ότι είναι πράγματι μοναδική. Η διαδικασία είναι αρκετά απλή, στέλνει μερικά ARP probe πακέτα (συνήθως 3) και αν κανείς δεν απαντήσει, διεκδικεί επίσημα τη διεύθυνση IP με ένα ARP Announcement πακέτο.

Ένα **gratuitous ARP** είναι μια απάντηση ARP που δεν ζητήθηκε από ένα ARP request. Το gratuitous ARP αποστέλλεται ως broadcast, ως ένας τρόπος για έναν κόμβο να ανακοινώσει ή να ενημερώσει την αντιστοίχιση IP με το MAC address του σε ολόκληρο το δίκτυο.

Με τη δεύτερη εκτέλεση της εντολής ipconfig /renew (sudo dhclient), ο υπολογιστής σας ζητά την ανανέωση της διεύθυνσης IPv4 που του εκχωρήθηκε προηγουμένως (κατά την πρώτη εκτέλεση της εντολής).

2.42. Ποια είδη μηνυμάτων DHCP παρήχθησαν με την εκτέλεση της εντολής ανανέωσης (δεύτερο renew);
Request και ACK.

2.43. Διαφέρει το πλαίσιο Ethernet και το αντίστοιχο πακέτο IPv4 που μεταφέρει το μήνυμα DHCP Request της εντολής ανανέωσης από το αντίστοιχο της εντολής εκχώρησης (πρώτο renew); Εάν ναι, σε ποια σημεία; [Υπόδειξη: Περιοριστείτε στις διευθύνσεις MAC και IPv4 που καταγράψατε στις ερωτήσεις 2.26 και 2.28.]
Στις διευθύνσεις MAC Source και Destination. Συγκεκριμένα, στο 1ο (χρονικά) request έχουμε Source : 0.0.0.0 & Destination : 255.255.255.255 και στο 2ο έχουμε Source : 147.102.236.36 & Destination : 147.102.236.230

2.44. Υπάρχει επικεφαλίδα ή επιλογή (option) στο μήνυμα DHCP Request της εντολής ανανέωσης που να προσδιορίζει τον εξυπηρετητή DHCP, όπως βρήκατε στην ερώτηση 2.29;
Όχι, δεν υπάρχει στην επικεφαλίδα DHCP υπάρχει όμως η διεύθυνση του DHCP server στην IPv4 επικεφαλίδα ως Destination Address: 147.102.236.230.

2.45. Σε ποια επικεφαλίδα ή επιλογή (option) του μηνύματος DHCP Request της εντολής ανανέωσης περιλαμβάνεται η διεύθυνση IPv4 την ανανέωση της οποίας αιτείται ο υπολογιστή σας; Υπάρχει διαφορά με την απάντηση στην ερώτηση 2.26;
Περιλαμβάνεται στην επικεφαλίδα DHCP στο πεδίο **Client IP address**, οπότε και διαφέρει σε σχέση με το 2.26 καθώς εκεί ζητούνταν η ίδια διεύθυνση μεν αλλά σε Option.

2.46. Σε ποια επικεφαλίδα του μηνύματος DHCP ACK της εντολής ανανέωσης περιλαμβάνεται η διεύθυνση IPv4 την ανανέωση της οποίας εγκρίνει ο εξυπηρετητής DHCP; Υπάρχει διαφορά με την απάντηση στην ερώτηση 2.30;

Στην επικεφαλίδα DHCP στο πεδίο **Your (client) IP address** με τιμή 147.102.236.36 και όχι δεν υπάρχει διαφορά με την 2.30 ερώτηση.

Παρατηρήστε την τιμή του πεδίου Transaction ID της επικεφαλίδας των μηνυμάτων DHCP που κατέγραψε το Wireshark.

2.47. Ποια είναι η τιμή του για το μήνυμα DHCP που σχετίζεται με την εντολή απόλυσης (release);

Transaction ID (Release): 0x31a6ed6e

2.48. Ποια είναι η τιμή του για τα μηνύματα DHCP που σχετίζονται με την εντολή εκχώρησης (πρώτο renew);

Transaction ID (πρώτο renew): 0x624c0614

2.49. Ποια είναι η τιμή του για τα μηνύματα DHCP που σχετίζονται με την εντολή ανανέωσης (δεύτερο renew);

Transaction ID (δεύτερο renew): 0xfefc5d2f

2.50. Ποιος είναι ο σκοπός του πεδίου Transaction ID;

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.