Εργαστηριακή Άσκηση 10
SMTP, DHCP

Ο σκοπός αυτού του εργαστηρίου είναι η εξέταση των πρωτοκόλλων εφαρμογής SMTP και DHCP, που χρησιμοποιούνται ευρύτατα στο διαδίκτυο, με τη βοήθεια του αναλυτή πρωτοκόλλων Wireshark. Εδώ θα χρησιμοποιήσετε τη λειτουργία *Capture* με φίλτρο, ώστε τα πλαίσια που καταγράφονται να περιέχουν κάποια συγκεκριμένα χαρακτηριστικά. Υπενθυμίζεται ότι το φίλτρο απεικόνισης *(Display)*, που επιλέγετε από το μενού *Analyze,* μπορεί να (απ)ενεργοποιηθεί οποιαδήποτε στιγμή κατά τη διάρκεια της καταγραφής, καθώς επίσης και μετά την ολοκλήρωση αυτής, προκειμένου να αποκρύπτει (αποκαλύπτει) κάποια από τα συλληφθέντα πλαίσια, ενώ το φίλτρο σύλληψης, που επιλέγετε από το μενού *Capture*, ενεργοποιείται πάντοτε **πριν** ξεκινήσει η διαδικασία καταγραφής, με αποτέλεσμα να καταγράφεται μόνο ένα μέρος των διερχόμενων πλαισίων. Προσοχή: η απενεργοποίηση του φίλτρου απεικόνισης γίνεται πιέζοντας το κουμπί Clear (η διαγραφή του φίλτρου στο πεδίο εισαγωγής δεν το ακυρώνει!). Επίσης, αφού ξεκινήσετε το πρόγραμμα Wireshark πηγαίνετε στο *Edit* → *Preferences* και στη λίστα επιλογών στα αριστερά διαλέξτε το *Name Resolution*, βεβαιωθείτε ότι το Enable MAC name resolution και το Enable transport name resolution στα δεξιά είναι επιλεγμένα και πατήστε *OK*.

1. Το πρωτόκολλο SMTP

Το πρωτόκολλο **Simple Mail Transfer Protocol (SMTP)** έχει καθιερωθεί για τη μετάδοση μηνυμάτων ηλεκτρονικού ταχυδρομείου στο διαδίκτυο. Η επίσημη περιγραφή του βρίσκεται στα RFC821 και RFC1123. Το πρωτόκολλο που χρησιμοποιείται σήμερα, γνωστό ως **Enhanced SMTP (ESMTP)** αποτελεί επέκταση του αρχικού προτύπου και περιγράφεται στο έγγραφο RFC 2821. Το SMTP είναι ένα σχετικά απλό πρωτόκολλο ηλεκτρονικής αλληλογραφίας βασισμένο στη μετάδοση χαρακτήρων για την αποστολή μηνυμάτων. Το μήνυμα αποτελείται από κείμενο (χαρακτήρες) και πιθανώς άλλα κωδικοποιημένα (ως κείμενο) αντικείμενα.

Για να την αποστολή ενός ηλεκτρονικού μηνύματος θα πρέπει ο χρήστης (πρόγραμμα πελάτης ηλεκτρονικού ταχυδρομείου - email) να έχει δικτυακή πρόσβαση σε έναν εξυπηρετητή SMTP για την εξερχόμενη αλληλογραφία (outgoing mail server). Ο αποστολέας καθορίζει τους παραλήπτες και το μήνυμά του μεταφέρεται στον εξυπηρετητή SMTP με μια σειρά ερωτήσεων-απαντήσεων. Το SMTP προωθεί τα μηνύματα του αποστολέα προς τον εξυπηρετητή SMTP για την εισερχόμενη αλληλογραφία του παραλήπτη πιθανώς μέσω άλλων εξυπηρετητών SMTP που δρουν ως αναμεταδότες (relay servers). Ο παραλήπτης (πρόγραμμα πελάτης ηλεκτρονικού ταχυδρομείου) για να παραλάβει την εισερχόμενη αλληλογραφία χρησιμοποιεί άλλα πρωτόκολλα, όπως, POP3 ή IMAP, για να διαβάσει τα εισερχόμενα μηνύματα από τον εξυπηρετητή του (incoming mail server). Τα προγράμματα ηλεκτρονικού ταχυδρομείου (πχ Mozilla Thunderbird, Microsoft Outlook κ.α.) θα πρέπει να ρυθμιστούν κατάλληλα από τον χρήστη. Συγκεκριμένα ο χρήστης θα πρέπει να καθορίσει τους εξυπηρετητές[1] SMTP και POP3 (ή IMAP) που θα χρησιμοποιήσει για να αποστείλει και να παραλάβει, αντίστοιχα, ηλεκτρονική αλληλογραφία.

Το πρωτόκολλο SMTP άρχισε ως απλή μεταφορά κειμένου χαρακτήρων ASCII των 7 bit και δεν υποστήριζε τη μεταφορά δυαδικών αρχείων καθώς και χαρακτήρων άλλων (πλην του λατινικού) αλφαβήτων. Αργότερα αναπτύχθηκαν άλλα πρότυπα όπως το **Multipurpose Internet Mail Extensions (MIME)** για τη μεταφορά δυαδικών αρχείων και κειμένου σε μη ASCII χαρακτήρες, ενώ οι εξυπηρετητές SMTP άρχισαν να υποστηρίζουν τη μεταφορά χαρακτήρων των 8 bit. Το

[1] Δεν είναι υποχρεωτικό να ταυτίζονται.

πρωτόκολλο ESMTP που χρησιμοποιείται σήμερα για ηλεκτρονική αλληλογραφία υποστηρίζει τόσο γραφικά όσο και την επισύναψη άλλων αρχείων.

Στη συνέχεια δίνεται ένα παράδειγμα της συνομιλίας μεταξύ προγράμματος πελάτη (C) και του εξυπηρετητή SMTP (S) για την αποστολή ενός απλού μηνύματος ηλεκτρονικού ταχυδρομείου.

```
S: 220 www.mailserver.com Your SMTP Post
C: HELO mydomain.gr
S: 250 Hello mydomain.gr
C: MAIL FROM:<sender>
S: 250 Ok
C: RCPT TO:<friend@example.com>
S: 250 Ok
C: DATA
S: 354 End data with <CR><LF>.<CR><LF>
C: Subject: test message
C: From: sender@mydomain.g
C: To: friend@example.com
C:
C: This is a test.
C: Do not reply.
C: .
S: 250 Ok: queued as 123456789
C: QUIT
S: 221 Bye
```

Στο παράδειγμα φαίνονται τα βήματα που περιλαμβάνει η διαδικασία προώθησης της ηλεκτρονικής αλληλογραφίας. Με την εντολή *HELO* ο πελάτης SMTP προσδιορίζει το όνομα της περιοχής όπου ανήκει. Στην περίπτωση που υποστηρίζεται ESMTP χρησιμοποιείται η εντολή *EHLO* (Extended HELLO) αντί της *HELO* (Hello του αρχικού RFC 821). Η δοσοληψία αποστολής της ηλεκτρονικής αλληλογραφίας ξεκινά με την εντολή *MAIL* που προσδιορίζει την ταυτότητα της ταχυδρομικής θυρίδας του αποστολέα. Ακολουθεί μια σειρά από εντολές *RCPT* για τον προσδιορισμό της ταυτότητας των παραληπτών. Στη συνέχεια η εντολή DATA εκκινεί τη διαδικασία μεταφοράς του μηνύματος ηλεκτρονικής αλληλογραφίας. Αφού τελειώσει το κείμενο, η εντολή *QUIT* κλείνει το κανάλι επικοινωνίας. Περισσότερες λεπτομέρειες για τις εντολές του SMTP θα βρείτε στην ιστοσελίδα http://www.networksorcery.com/enp/protocol/smtp.htm και τις εκεί παραπομπές στα σχετικά RFC.

Για τη χρήση της υπηρεσίας SMTP χρησιμοποιούνται ειδικές εφαρμογές, όπως προαναφέραμε, ωστόσο στην άσκηση αυτή η επικοινωνία με τον εξυπηρετητή SMTP θα γίνει απευθείας από ένα παράθυρο εντολών μέσω TELNET. Ανοίξτε ένα παράθυρο εντολών και, πληκτρολογήστε **με προσοχή** το κείμενο που ακολουθεί. Κάθε γραμμή τερματίζεται πατώντας το πλήκτρο `<Enter>`. Εάν κάνετε λάθος στην εισαγωγή των χαρακτήρων θα πρέπει να επαναλάβετε την εντολή[2]. 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
```

[2] Το πλήκτρο `<Backspace>` δεν εκλαμβάνεται ως διόρθωση του προηγούμενου χαρακτήρα, αλλά ως ένας νέος χαρακτήρας για αποστολή.

1.1 Ποια είναι η σημασία του παραπάνω τρόπου κλήσης της εντολής telnet; *[Υπόδειξη: telnet /?]*

Με την εγκατάσταση σύνδεσης στον εξυπηρετητή SMTP, ο εξυπηρετητής αποστέλλει το αναγνωριστικό του συνοδευόμενο από ένα κωδικό απόκρισης.

1.2 Ποιο είναι το αναγνωριστικό που αποστείλει ο εξυπηρετητής SMTP μετά την εγκατάσταση σύνδεσης;
1.3 Ποιος είναι ο κωδικός της απόκρισης (Response code) και ποιο το νόημά του; *[Υπόδειξη: Ανατρέξτε στην ιστοσελίδα που αναφέρθηκε παραπάνω.]*
1.4 Ποιος είναι ο κωδικός απόκρισης στην εντολή HELP του πρωτοκόλλου SMTP;
1.5 Καταγράψτε το πλήθος των υποστηριζόμενων εντολών από τον εξυπηρετητή καθώς και τα ονόματα τριών από αυτών με βάση την απόκριση στην παραπάνω εντολή.
1.6 Ποιος είναι ο κωδικός απόκρισης στις εντολές HELO και EHLO του πρωτοκόλλου SMTP;
1.7 Παρατηρείτε κάποια διαφορά μεταξύ των αποκρίσεων του εξυπηρετητή στις εντολές HELO και EHLO του πρωτοκόλλου SMTP;
1.8 Τι ακριβώς δηλώνει η απόκριση του εξυπηρετητή στην εντολή EHLO του πρωτοκόλλου SMTP; *[Υπόδειξη: Συμβουλευθείτε την απάντηση της σχετικής εντολής HELP στο παράθυρο εντολών.]*
1.9 Είναι προφανές ότι ο εξυπηρετητής smtp.ntua.gr υποστηρίζει το ESMTP. Πότε έγινε αυτό εμφανές για πρώτη φορά;

Στη συνέχεια στο παράθυρο εντολών πληκτρολογήστε με προσοχή το κείμενο που ακολουθεί. Κάθε γραμμή τερματίζεται πατώντας το πλήκτρο `<Enter>`. *Προσοχή: Οι διευθύνσεις ηλεκτρονικού ταχυδρομείου που εμφανίζονται παρακάτω θα πρέπει να περικλείονται από τους χαρακτήρες "<" και ">".* Όπως και πριν εάν κάνετε λάθος στην εισαγωγή των χαρακτήρων θα πρέπει να επαναλάβετε την εντολή.

```
telnet smtp.ntua.gr 25
HELO example.com
MAIL FROM:<a_guru@of.net>
RCPT TO:<Your_email_address>
DATA
Subject:Test Message

Testing
1
2
3
.
QUIT
```

όπου `<Your_email_address>` είναι η διεύθυνση του ηλεκτρονικού σας ταχυδρομείου π.χ. `<elxxxxx@mail.ntua.gr>`[3]. Στη συνέχεια ανοίξτε το ηλεκτρονικό σας ταχυδρομείο μέσω του https://my.ntua.gr για να επιβεβαιώσετε ότι λάβατε το μήνυμα που στείλατε.

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

[3] Εάν δεν έχετε κωδικό στο mail.ntua.gr χρησιμοποιείστε οποιαδήποτε άλλη διεύθυνση ηλεκτρονικού ταχυδρομείου διαθέτετε εκτός ή εντός ΕΜΠ (πλην του central.ntua.gr) αρκεί να έχετε πρόσβαση σε αυτή μέσω web και να **μπορείτε** να ανακτήσετε τις πληροφορίες που ζητούνται πιο κάτω. Εάν δε διαθέτετε τέτοια διεύθυνση θα πρέπει να αποκτήσετε μία (π.χ. στο Gmail ή Yahoo) προτού κάνετε την άσκηση.

1.11 Ποιος είναι ο ρόλος της τελείας που πληκτρολογείτε πριν την εντολή QUIT κατά την επικοινωνία SMTP με τον εξυπηρετητή;
1.12 Ποια είναι η απόκριση του εξυπηρετητή και ο αντίστοιχος κωδικός απόκρισης μετά το τέλος της εισαγωγής δεδομένων;
1.13 Ποιος εμφανίζεται ως αποστολέας του μηνύματος που λάβατε στην ταχυδρομική σας θυρίδα;
1.14 Ποιος εμφανίζεται ως παραλήπτης του μηνύματος που λάβατε στην ταχυδρομική σας θυρίδα[4];
1.15 Σε ποια επικεφαλίδα του μηνύματος που λάβατε εμφανίζεται η απάντηση του εξυπηρετητή που καταγράψατε στην ερώτηση 1.12; *[Υπόδειξη: Θα πρέπει να εξετάσετε τις επικεφαλίδες που συνοδεύουν το μήνυμα. Στην περίπτωση του MyNTUA κάντε κλικ στο Display Headers δίπλα στο πεδίο Full Headers για να εμφανισθούν[5].]*
1.16 Σε ποια επικεφαλίδα του μηνύματος που λάβατε εμφανίζεται το example.com;
1.17 Σε ποια επικεφαλίδα του μηνύματος που λάβατε εμφανίζεται η διεύθυνση ηλεκτρονικού ταχυδρομείου που δώσατε με την εντολή RCPT;

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 την διεύθυνση IP του υπολογιστή σας. Κατόπιν πληκτρολογήστε το κείμενο που ακολουθεί. Κάθε γραμμή τερματίζεται πατώντας το πλήκτρο `<Enter>`.

```
telnet smtp.ntua.gr 25
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:

1.18 Ποιο είναι το φίλτρο σύλληψης που εφαρμόσατε;
1.19 Ποιο είναι το φίλτρο απεικόνισης που εφαρμόσατε;
1.20 Ποιο πρωτόκολλο μεταφοράς χρησιμοποιεί το πρωτόκολλο εφαρμογής SMTP
1.21 Καταγράψτε τις θύρες (προέλευσης και προορισμού) του πρωτοκόλλου μεταφοράς που χρησιμοποιούνται για την επικοινωνία.
1.22 Ποια από τις παραπάνω θύρες αντιστοιχεί στο πρωτόκολλο εφαρμογής SMTP;
1.23 Πόσα μηνύματα SMTP απαιτούνται για τη μεταφορά της εντολής QUIT προς τον εξυπηρετητή;
1.24 Ποια είναι η απόκριση του εξυπηρετητή και ο αντίστοιχος κωδικός απόκρισης στην εντολή QUIT του πρωτοκόλλου SMTP;
1.25 Ποια εντολή του πρωτοκόλλου SMTP προκαλεί την απόλυση της σύνδεσης TCP;

2. Το πρωτόκολλο DHCP

Το Dynamic Host Control Protocol (DHCP) είναι ένα τυποποιημένο πρωτόκολλο RFC 2131, που δημιουργήθηκε από την ανάγκη απλοποίησης της διαχείρισης δικτύων βασισμένων στο TCP/IP. Παλαιότερα τα περισσότερα τοπικά δίκτυα είχαν περιορισμένο αριθμό σταθερών υπολογιστών κάτι που επέτρεπε τη στατική ανάθεση IP διευθύνσεων. Αυτό προϋπέθετε τη δια χειρός αλλαγή και ρύθμιση των διευθύνσεων οι οποίες αποθηκεύονταν στο δίσκο του υπολογιστή. Αν χρειαζόταν ποτέ ένας υπολογιστής να αλλάξει διεύθυνση τότε αυτό γινόταν από την κονσόλα του και συνήθως

[4] Στην περίπτωση του Gmail σε standard view κάντε κλικ στο Show Details.
[5] Εάν χρησιμοποιείτε Yahoo! Classic Mail κάντε κλικ στο Full Headers. Εάν χρησιμοποιείτε το new Yahoo! Mail, επιλέξτε Full Headers αφού κάνετε κλικ στο Actions. Στην περίπτωση του Gmail σε standard view επιλέξτε Show Original αφού κάνετε κλικ στο βέλος δεξιά από το Reply.

απαιτούσε και επανεκκίνηση. Σχετικά σύντομα, και καθώς άρχισαν να δημιουργούνται όλο και πιο σύνθετα δίκτυα, υπήρξε η ανάγκη για κεντρική διαχείριση των διευθύνσεων IP. Αυτό έγινε γιατί άρχισαν να χρησιμοποιούνται κατά κόρον σταθμοί εργασίας (και αργότερα προσωπικοί υπολογιστές). Ένα ειδικό πρωτόκολλο, το Reverse Address Resolution Protocol (RARP), δημιουργήθηκε για τέτοιες περιπτώσεις (RFC 903). Επέτρεπε σε ένα μηχάνημα να «μάθει» την IP διεύθυνσή του και μετά να ξεκινήσει την κανονική λειτουργία του TCP/IP.

Ένα άλλο πρωτόκολλο, το BOOTstrap Protocol (BOOTP), αναπτύχθηκε για να επιτρέψει σε φτηνούς σταθμούς εργασίας που δε διέθεταν χώρο μόνιμης αποθήκευσης (σκληρό δίσκο) να λαμβάνουν την IP διεύθυνσή τους και την εικόνα του λειτουργικού τους συστήματος κατά την εκκίνηση (RFC951). Το BOOTP στη συνέχεια εμπλουτίστηκε με ένα μηχανισμό επέκτασης (BOOTP extension mechanism) που επέτρεπε επιπλέον δεδομένα και επιλογές μηνυμάτων. Αυτή η έκδοση του BOOTP έμελλε να είναι ο πρόγονος του DHCP. Υπάρχουν δύο κύριες διαφορές μεταξύ των πρωτοκόλλων BOOTP και DHCP. Το DHCP ορίζει μηχανισμούς δυναμικής εκχώρησης διευθύνσεων IP στους σταθμούς εργασίας ως δάνειο για καθορισμένο χρονικό διάστημα. Έτσι επιτυγχάνεται η επαναχρησιμοποίηση ενός αριθμού διευθύνσεων IP από πολλούς σταθμούς εργασίας. Επιπλέον το DHCP παρέχει το μηχανισμό με τον οποίο ο σταθμός εργασίας μπορεί μόνος του να ανασύρει τις πληροφορίες που απαιτούνται προκειμένου να λειτουργήσει στο δίκτυο.

Σε συντομία, η λειτουργία του DHCP είναι η ακόλουθη. Μόλις ο υπολογιστής εκκινήσει εκπέμπει ένα μήνυμα αναζήτησης (*DHCP Discover*) εξυπηρετητή DHCP. Οι εξυπηρετητές DHCP που ακούν αυτό το μήνυμα, απαντούν με μήνυμα προσφοράς (*DHCP Offer*) το οποίο ορίζει διευθύνσεις IP. Ο υπολογιστής επιλέγει μία προσφορά και εκπέμπει αίτηση (*DHCP Request*) προς τον εξυπηρετητή ζητώντας τη συγκεκριμένη διεύθυνση IP. Όλοι οι άλλοι εξυπηρετητές αποχωρούν και ο επιλεχθείς εξυπηρετητής στέλνει επιβεβαίωση (*DHCP ACK*) για την εκχωρούμενη διεύθυνση IP. Η διεύθυνση IP παραχωρείται με δάνειο για συγκεκριμένο χρονικό διάστημα (lease time). Προτού λήξει το διάστημα αυτό, ο υπολογιστής πρέπει να ανανεώσει το δάνειο. Όταν ο υπολογιστής τελειώσει, στέλνει μήνυμα απόλυσης (*DHCP Release*) της διεύθυνσης.

Ουσιαστικά, το DHCP αναλαμβάνει να ορίσει αυτόματα, χωρίς την παρουσία διαχειριστή δικτύου, τις αναγκαίες παραμέτρους λειτουργίας ενός υπολογιστή. Το DHCP υποστηρίζει 3 μηχανισμούς για να αντιστοιχίζει διευθύνσεις:

- Δυναμική αντιστοίχηση (εκχώρηση μιας διεύθυνσης IP για συγκεκριμένο διάστημα)
- Αυτόματη αντιστοίχηση (μόνιμη εκχώρηση μιας διαθέσιμης διεύθυνσης IP)
- Χειροκίνητη αντιστοίχηση (εκχώρηση με βάση τη διεύθυνση MAC του αιτούντος)

Για να δείτε τις τρέχουσες ρυθμίσεις τις κάρτας δικτύου του υπολογιστή σας ανοίξτε ένα παράθυρο εντολών και εκτελέστε την εντολή `ipconfig /all`.

2.1. Καταγράψτε τη διεύθυνση IP, τη μάσκα υπο-δικτύου του υπολογιστή σας καθώς και τη διεύθυνση IP του εξυπηρετητή DHCP που είναι υπεύθυνος για τις ρυθμίσεις αυτές.

Στη συνέχεια με τη βοήθεια του Wireshark ξεκινήστε μια νέα καταγραφή της κίνησης (χωρίς φίλτρο σύλληψης) προκειμένου να μελετήσετε τα μηνύματα DHCP που ανταλλάσσονται κατά την εκχώρηση/αποδέσμευση των ρυθμίσεων IP της κάρτας δικτύου του υπολογιστή σας.

Κατόπιν εκτελέστε την εντολή `iprelease`[6] που θα προκαλέσει την αποδέσμευση των ρυθμίσεων της κάρτας δικτύου του υπολογιστή σας. Έπειτα εκτελέστε την εντολή `iprenew`[7] προκειμένου να εκχωρηθούν νέες δικτυακές ρυθμίσεις στον υπολογιστή σας. Περιμένετε έως ότου ολοκληρωθεί η εκχώρηση και εκτελέστε πάλι την εντολή `iprenew` ώστε να ανανεώσετε τις ρυθμίσεις. Όταν

[6] Ταυτόσημη με την `ipconfig /release`, την οποία, όμως, ο χρήστης labuser δε μπορεί να εκτελέσει ελλείψει κατάλληλων δικαιωμάτων.
[7] Ισοδυναμεί με την εντολή `ipconfig /renew`.

ολοκληρωθεί και η εκτέλεση της δεύτερης `iprenew`, σταματήστε την καταγραφή μηνυμάτων από το Wireshark.

2.2. Εφαρμόστε κατάλληλο φίλτρο απεικόνισης ώστε να εμφανίζονται μόνο μηνύματα DHCP. Ποια είναι η σύνταξή του; *[Υπόδειξη: Υπενθυμίζεται ότι το πρωτόκολλο DHCP αποτελεί επέκταση του BOOTP.]*
2.3. Ποιο πρωτόκολλο μεταφοράς χρησιμοποιεί το DHCP;
2.4. Ποια είδη μηνυμάτων DHCP παρήχθησαν από την αλληλουχία εντολών απόλυσης (`iprelease`), εκχώρησης και ανανέωσης (`iprenew`) δικτυακών ρυθμίσεων; *[Υπόδειξη: Ο τύπος μηνύματος DHCP αναφέρεται και στο πεδίο Info του παράθυρου με τη λίστα καταγεγραμμένων πακέτων του Wireshark.]*
2.5. Ποιος είναι ο σκοπός του πρώτου μηνύματος DHCP που παρατηρείτε;
2.6. Πού ανήκουν οι διευθύνσεις IP του αποστολέα και του παραλήπτη του παραπάνω μηνύματος;
2.7. Παρατηρώντας το περιεχόμενο των πεδίων της επικεφαλίδας όλων των μηνυμάτων DHCP, να καταγραφούν: η αριθμητική ετικέτα (tag) και το μήκος (length) της επιλογής (option) που καθορίζει τον τύπο του εκάστοτε μηνύματος (DHCP Message Type). *[Υπόδειξη: Το Wireshark εμφανίζει την ετικέτα και το μήκος (t=x, l=y) στην πρώτη γραμμή δίπλα από κάθε επιλογή που περιλαμβάνεται στις επικεφαλίδες των μηνυμάτων DHCP]*
2.8. Ποια είναι η τιμή (value) που αντιστοιχεί στην αριθμητική ετικέτα που καταγράψατε στην ερώτηση 2.7 για κάθε είδος μηνύματος DHCP που καταγράψατε; *[Υπόδειξη: Στο παράθυρο λεπτομερειών πακέτου του Wireshark αναπτύξτε όλες τις γραμμές που αντιστοιχούν στην επιλογή DHCP με τη συγκεκριμένη αριθμητική ετικέτα]*

Όπως προαναφέρθηκε, η διεύθυνση IP 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.

2.9. Καταγράψτε τις θύρες πηγής και προορισμού που χρησιμοποιήθηκαν κατά την ανταλλαγή των μηνυμάτων *DHCP Discover/Offer/Request/ACK* μεταξύ του υπολογιστή σας και του εξυπηρετητή DHCP.
2.10. Ποιες από τις παραπάνω θύρες αντιστοιχούν στις συνήθεις θύρες (well-known ports) της υπηρεσίας DHCP; *[Υπόδειξη: Συμβουλευτείτε την ιστοσελίδα http://en.wikipedia.org/wiki/Well_known_ports.]*
2.11. Ποιες είναι οι διευθύνσεις IP αποστολέα και παραλήπτη των παραπάνω τεσσάρων μηνυμάτων;
2.12. Τι υποδηλώνει η διεύθυνση IP του παραλήπτη του μηνύματος *DHCP Discover*;
2.13. Δεδομένου ότι το παραπάνω μήνυμα προέρχεται από τον υπολογιστή σας, να αιτιολογήσετε τη χρήση της διεύθυνσης `0.0.0.0` ως διεύθυνση IP του αποστολέα.
2.14. Ποια διεύθυνση IP αποδίδεται τελικά στον υπολογιστής σας;
2.15. Για πόσο χρόνο διαρκεί η εκχώρηση της IP διεύθυνσης αυτής; *[Υπόδειξη: Αναζητείστε την τιμή του lease time στο μήνυμα DHCP Offer.]*
2.16. Συμπίπτει η διεύθυνση IP που εκχωρήθηκε με αυτή που είχατε καταγράψει αρχικά στο ερώτημα 2.1; Αιτιολογήστε.

Εκτός από τη διεύθυνση IP, 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.

2.17. 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 θα ανήκει ο υπολογιστής). *[Υπόδειξη: Συμβουλευτείτε την ιστοσελίδα http://www.iana.org/assignments/bootp-dhcp-parameters.]*
2.18. Πόσες παραμέτρους ζήτησε ο υπολογιστής σας με το μήνυμα *DHCP Discover* και πόσες προσδιορίζει τελικά ο εξυπηρετητής DHCP στο μήνυμα *DHCP Offer*; *[Υπόδειξη: Εμφανίστε*

το ένα εκ των δύο πακέτων σε νέο παράθυρο κάνοντας δεξί κλικ στη γραμμή του στη λίστα των καταγεγραμμένων πακέτων και μετά επιλέγοντας Show Packet in New Window.]

Μετά τη λήψη της διεύθυνσης IP, ο υπολογιστής σας επιβεβαιώνει ότι αυτή είναι πραγματικά διαθέσιμη (δε χρησιμοποιείται από άλλον) και αμέσως μετά ζητά την ανανέωσή της.

2.19. Τροποποιείστε το φίλτρο απεικόνισης ώστε εκτός των μηνυμάτων DHCP να εμφανίζονται και πλαίσια ARP. Ποια είναι η νέα σύνταξη του φίλτρου απεικόνισης;
2.20. Παρατηρείτε την αποστολή πλαισίων που το Wireshark αποκωδικοποιεί ως gratuitous ARP αμέσως μετά το μήνυμα *DHCP ACK*;
2.21. Εάν ναι, πόσα τέτοια πλαίσια στάλθηκαν;
2.22. Ποιος υπολογιστής (δηλαδή, ποια διεύθυνση IP) τα παράγει και ποιου υπολογιστή τη διεύθυνση MAC αναζητεί;
2.23. Εξηγείστε τη χρησιμότητα αυτών των πλαισίων ARP *[Υπόδειξη: Αναζητείστε το "gratuitous ARP" στο google.]*;

Με τη δεύτερη εκτέλεση της εντολής `iprenew`, ο υπολογιστής σας ζητά την ανανέωση της διεύθυνσης IP που του εκχωρήθηκε προηγουμένως (κατά την πρώτη εκτέλεση της εντολής `iprenew`).

2.24. Ποια είδη μηνυμάτων DHCP παρήχθησαν μετά τη δεύτερη εκτέλεση της εντολής `iprenew`;
2.25. Ποια είναι η βασική διαφορά του μηνύματος *DHCP Request* της δεύτερης εκτέλεσης της εντολής `iprenew`, σε σχέση με το *DHCP Request* της πρώτης εκτέλεσης της εντολής; *[Υπόδειξη: Περιορισθείτε στις βασικές παραμέτρους που εμφανίζονται στο παράθυρο με τη λίστα των καταγεγραμμένων πακέτων του Wireshark.]*

Παρατηρείστε την τιμή του πεδίου Transaction ID των μηνυμάτων DHCP που κατέγραψε το Wireshark.

2.26. Ποια είναι η τιμή του για το μήνυμα DHCP που σχετίζεται με την εκτέλεση της εντολής `iprelease`;
2.27. Ποια είναι η τιμή του για τα μηνύματα DHCP που σχετίζονται με την πρώτη εκτέλεση της εντολής `iprenew`;
2.28. Ποια είναι η τιμή του για τα μηνύματα DHCP που σχετίζονται με τη δεύτερη εκτέλεση της εντολής `iprenew`;
2.29. Ποιος είναι ο σκοπός του πεδίου Transaction ID;

Ονοματεπώνυμο:	**Όνομα PC:**
Ομάδα:	**Ημερομηνία:**
Διεύθυνση IP: . . .	**Διεύθυνση MAC: - - - - -**

Εργαστηριακή Άσκηση 10
SMTP, DHCP

Απαντήστε στα ερωτήματα στον χώρο που σας δίνεται παρακάτω και στην πίσω σελίδα εάν δεν επαρκεί. Το φυλλάδιο αυτό θα παραδοθεί στον επιβλέποντα.

1

1.1 .....

.....

1.2 .....

.....

1.3 .....

.....

1.4 .....

1.5 .....

.....

.....

.....

1.6 .....

1.7 .....

.....

1.8 .....

.....

.....

1.9 .....

.....

1.10 .....

.....

1.11 .....

.....

1.12 .....

.....

1.13 .....

1.14 .....

1.15 .....