Εργαστηριακή Άσκηση 9
SMTP, DHCP

Ο σκοπός αυτής της εργαστηριακής άσκησης είναι η εξέταση του πρωτοκόλλου εφαρμογής SMTP, που χρησιμοποιείται στο διαδίκτυο για τη μεταφορά ηλεκτρονικής αλληλογραφίας και του πρωτοκόλλου DHCP, που χρησιμοποιείται για την αυτόματη απόδοση διευθύνσεων IP, με τη βοήθεια του αναλυτή πρωτοκόλλων Wireshark. Όπως και στις προηγούμενες ασκήσεις 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 Resolve MAC address και το Resolve transport names στα δεξιά είναι επιλεγμένα και πατήστε *OK*.

Για τις παρακάτω ασκήσεις απαντήστε στο συνοδευτικό φυλλάδιο, το οποίο θα υποβάλλετε ως αρχείο pdf.

1. Το πρωτόκολλο SMTP

Το πρωτόκολλο **Simple Mail Transfer Protocol (SMTP)** έχει καθιερωθεί για τη μετάδοση μηνυμάτων ηλεκτρονικού ταχυδρομείου στο διαδίκτυο. Η επίσημη περιγραφή της αρχικής του έκδοσης βρίσκεται στο RFC 821. Το πρωτόκολλο που χρησιμοποιείται σήμερα, γνωστό ως **Enhanced SMTP (ESMTP)**, αποτελεί επέκταση του αρχικού προτύπου και η πλέον πρόσφατη περιγραφή του περιλαμβάνεται στο έγγραφο RFC 5321. Το SMTP είναι ένα σχετικά απλό πρωτόκολλο βασισμένο στη μετάδοση χαρακτήρων για την αποστολή μηνυμάτων. Το SMTP ξεκίνησε 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 πρωτόκολλο ESMTP που χρησιμοποιείται σήμερα υποστηρίζει την αποστολή μηνυμάτων που αποτελούνται από κείμενο (χαρακτήρες) και πιθανώς άλλα, κωδικοποιημένα ως κείμενο αντικείμενα, όπως γραφικά, καθώς και την επισύναψη αρχείων. Το SMTP ως πρωτόκολλο ορίζει τα της μεταφοράς του μηνύματος, όχι το περιεχόμενό του. Ορίζει τον φάκελο (envelope) του μηνύματος και τις παραμέτρους του, όπως π.χ. τον αποστολέα, παραλήπτη, κα., αλλά όχι τις επικεφαλίδες και το σώμα του μηνύματος. Ένα άλλο πρότυπο το RFC 5322 ορίζει τη σύνταξη των μηνυμάτων, γνωστή και ως Internet Message Format, δηλαδή, τις επικεφαλίδες και το σώμα.

Στην ανταλλαγή μηνυμάτων ηλεκτρονικού ταχυδρομείου εμπλέκονται πολλές οντότητες: ο πράκτορας αλληλογραφίας χρήστη MUA (Mail User Agent), ο πράκτορας υποβολής αλληλογραφίες MSA (Mail Submission Agent), ο πράκτορας μεταφοράς αλληλογραφίας MTA (Mail Transfer Agent), ο πράκτορας παράδοσης αλληλογραφίας MDA (Mail Delivery Agent), ένα τοπικό ή απομακρυσμένο γραμματοκιβώτιο (mailbox) και το σύστημα ονοματοδοσίας περιοχών DNS.

Ο πράκτορας αλληλογραφίας χρήστη (MUA) είναι η εφαρμογή για τη σύνταξη, αποστολή και λήψη μηνυμάτων ηλεκτρονικού ταχυδρομείου, π.χ. το Outlook, Thunderbird, ή πρόγραμμα ιστοσελίδας, π.χ. gmail, yahoo mail. Ο πράκτορας υποβολής αλληλογραφίας MSA (Mail Submission Agent) είναι εφαρμογή (δαίμονας σε εξυπηρετητή) που παραλαμβάνει την αλληλογραφία από τον MUA χρησιμοποιώντας το πρωτόκολλο SMTP, επισήμως στη θύρα 587, αλλά ιστορικά στη θύρα 25. Συνεργάζεται με τον πράκτορα μεταφοράς αλληλογραφίας (MTA) για την παράδοσή της. Ο MTA είναι εφαρμογή που λαμβάνει εισερχόμενη και προωθεί απερχόμενη αλληλογραφία, χρησιμοποιώντας το πρωτόκολλο SMTP στη θύρα 25, όπως sendmail, postfix, Microsoft exchange, κα. Συνήθως, οι λειτουργίες MSA και MTA συνυπάρχουν στο ίδιο λογισμικό. Ο πράκτορας παράδοσης αλληλογραφίας (MDA) είναι εφαρμογή που παραδίδει την αλληλογραφία για μια περιοχή ή δίκτυο. Αποθηκεύει την αλληλογραφία στο γραμματοκιβώτιο (mailbox) των χρηστών, από όπου μπορεί να αντληθεί με διάφορους τρόπους. Συνήθως αποτελεί μέρος της εφαρμογής MTA αν και μπορεί να είναι ανεξάρτητο λογισμικό, όπως π.χ. το dovecot. Η επικοινωνία μεταξύ MTA και MDA μπορεί να γίνει εναλλακτικά μέσω του LMTP (Local Mail Transfer Protocol), μιας παραλλαγής του SMTP, επειδή σε αυτήν την περίπτωση δεν υφίσταται ανάγκη ουρών αναμονής για την προώθηση των μηνυμάτων, παρά μόνο αποθήκευσης αυτών.

Το RFC 5321 ορίζει τη διεύθυνση ηλεκτρονικού ταχυδρομείου (email address) ως μια σειρά χαρακτήρων της μορφής *local-part@domain-name* που προσδιορίζει τον παραλήπτη της αλληλογραφίας ή το γραμματοκιβώτιο παράδοσής της. Το γραμματοκιβώτιο (mailbox) προσδιορίζεται μοναδικά από τη διεύθυνση ηλεκτρονικού ταχυδρομείου. Όμως όλες οι διευθύνσεις email δεν αντιστοιχούν σε κάποιο χώρο αποθήκευσης, π.χ. διευθύνσεις λιστών και ψευδώνυμα (aliases). Το όνομα του γραμματοκιβωτίου είναι το *local-part* της διεύθυνσης ηλεκτρονικού ταχυδρομείου. Έχει μήκος μέχρι 64 χαρακτήρες και συνήθως ταυτίζεται με το όνομα χρήστη (username) του παραλήπτη. Τυπικά επιτρέπεται να περιλαμβάνει λατινικά γράμματα (a-z, A-Z), ψηφία (0-9), τελεία ".", παύλα "– " και υπογράμμιση "_". Το δεύτερο μέρος της διεύθυνσης ηλεκτρονικού ταχυδρομείου, το *domain-name*, είναι το όνομα περιοχής DNS του προορισμού. Μπορεί να έχει μήκος μέχρι 255 χαρακτήρες και η σύνταξή του ακολουθεί αυστηρούς κανόνες. Είναι μια λίστα λέξεων μήκους μέχρι 63 χαρακτήρες που διαχωρίζονται με τελείες (dots). Η κάθε λέξη ακολουθεί τον κανόνα LDH (letters, digits, hyphen), όπου η παύλα δεν μπορεί να είναι ο πρώτος ή τελευταίος χαρακτήρας.

Για να την αποστολή ενός μηνύματος ηλεκτρονικού ταχυδρομείου θα πρέπει το πρόγραμμα πελάτης MUA να έχει δικτυακή πρόσβαση σε έναν MSA, εξυπηρετητή SMTP για την εξερχόμενη αλληλογραφία (outgoing mail server). Ο MUA μορφοποιεί το μήνυμα σύμφωνα με το προφίλ υποβολής (submission) του SMTP. Ο αποστολέας καθορίζει παραμέτρους του φακέλου (envelope), όπως την email διεύθυνση πηγής και προορισμού, και μεταφέρει στον εξυπηρετητή SMTP το μήνυμα ηλεκτρονικού ταχυδρομείου, επικεφαλίδες και σώμα, ως δεδομένα σε μια σειρά ερωτήσεων–απαντήσεων.

Ο MSA προσδιορίζει τον προορισμό από τη διεύθυνση email που παρέχει το SMTP, όχι από τις επικεφαλίδες του μηνύματος ηλεκτρονικού ταχυδρομείου, ερωτώντας το DNS για τον εξυπηρετητή αλληλογραφίας της περιοχής μετά το "@". Εάν ο παραλήπτης δεν είναι τοπικό γραμματοκιβώτιο, το μήνυμα προωθείται με το πρωτόκολλο SMTP στον MTA προορισμού. Αυτός μπορεί να δρα ως αναμεταδότης (relay server) και να προωθεί το μήνυμα σε άλλους MTA προτού αυτό παραδοθεί στον MDA. Κάθε φορά που ένας MTA λαμβάνει ένα μήνυμα ηλεκτρονικού ταχυδρομείου προσθέτει μια επικεφαλίδα ιχνηλάτησης (trace), την "*Received:*". Με αυτόν τον τρόπο δημιουργείται μια σειριακή καταγραφή των MTA που χειρίσθηκαν το μήνυμα.

Με την τελική παράδοση στον MDA προστίθεται η επικεφαλίδα "*Return-Path:*" για την καταγραφή της διαδρομής επιστροφής και αποθηκεύεται η αλληλογραφία στο γραμματοκιβώτιο. Η αποθηκευμένη αλληλογραφία μπορεί να διαβαστεί είτε τοπικά είτε να συλλεχθεί από μακριά μέσω πρωτοκόλλων όπως τα POP3 ή IMAP.

Τα προγράμματα πελάτες ηλεκτρονικού ταχυδρομείου (π.χ. Mozilla Thunderbird, Microsoft Outlook κ.α.) θα πρέπει να ρυθμιστούν κατάλληλα από τον χρήστη για αποστολή και λήψη αλληλογραφίας. Συγκεκριμένα ο χρήστης θα πρέπει να καθορίσει δύο εξυπηρετητές, που δεν είναι υποχρεωτικό να ταυτίζονται, τον εξυπηρετητή SMTP που θα χρησιμοποιήσει για την αποστολή ηλεκτρονικής αλληλογραφίας και τον εξυπηρετητή POP3 ή IMAP την παραλαβή της, αντίστοιχα. 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.gr
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 αποστολής της ηλεκτρονικής αλληλογραφίας. Με την εντολή *HELO* ο πελάτης SMTP προσδιορίζει το DNS όνομα του υπολογιστή του. 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 FROM* που προσδιορίζει τη διεύθυνση αποστολέα του φακέλου. Ακολουθεί μια σειρά από εντολές *RCPT TO* για τον προσδιορισμό των παραληπτών του φακέλου. Στη συνέχεια, η εντολή DATA εκκινεί τη διαδικασία μεταφοράς του περιεχομένου του μηνύματος ηλεκτρονικής αλληλογραφίας. Η μεταφορά του περιεχομένου τερματίζεται με μια μοναδική τελεία "." σε νέα γραμμή. Αφού τελειώσει η μεταφορά, η εντολή *QUIT* δηλώνει το τέλος της σύνδεσης και το κανάλι επικοινωνίας κλείνει.

Το περιεχόμενο του μηνύματος αποτελείται από δύο τμήματα: τις επικεφαλίδες (header) και το σώμα (body). Οι επικεφαλίδες χωρίζονται από το σώμα με μία κενή γραμμή. Κάθε επικεφαλίδα έχει δύο πεδία: το όνομά της και ένα κείμενο και ξεκινά με νέα γραμμή. Το όνομα της επικεφαλίδας είναι εκτυπώσιμοι χαρακτήρες, όχι κενό ή tab. Ο χαρακτήρας ":", η χρήση του οποίου απαγορεύεται στα ονόματα, χρησιμοποιείται για να διαχωρίσει το όνομα της επικεφαλίδας από το κείμενο που την ακολουθεί. Το κείμενο της επικεφαλίδας μπορεί να εκτείνεται σε επόμενες γραμμές. Ο πρώτος χαρακτήρας κάθε γραμμής πρέπει να είναι το κενό ή tab και η σύσταση είναι το μήκος της γραμμής να μην ξεπερνά τους 78 χαρακτήρες.

Κάθε μήνυμα επιβάλλεται να έχει δύο επικεφαλίδες την *From:*, η διεύθυνση ηλεκτρονικού ταχυδρομείου του αποστολέα, και την *Date:*, η ημερομηνία και ώρα σύνταξης του μηνύματος, που συνήθως συμπληρώνεται αυτόματα. Άλλες επικεφαλίδες είναι: *To:*, η διεύθυνση του μοναδικού παραλήπτη ή οι διευθύνσεις ηλεκτρονικού ταχυδρομείου των κύριων παραληπτών, *Subject:*, το θέμα του μηνύματος, *Cc:*, διευθύνσεις δευτερευόντων παραληπτών στους οποίους στέλνεται

αντίγραφο, *Bcc:*, διευθύνσεις άλλων παραληπτών που δεν εμφανίζονται, *Content-Type:*, πληροφορία για το πώς θα εμφανισθεί το μήνυμα, συνήθως κάποιος τύπος MIME, *Message-ID:*, πεδίο που παράγεται αυτόματα για την αποφυγή πολλαπλών παραδόσεων και *Reply-To:*, η διεύθυνση που θα χρησιμοποιηθεί για να απαντηθεί το μήνυμα. Να σημειωθεί ότι το κείμενο της επικεφαλίδας *To:* μπορεί να είναι άσχετο από τη διεύθυνση ηλεκτρονικού ταχυδρομείου *RCPT TO:* όπου παραδίδεται το μήνυμα, παρότι ο προορισμός SMTP μπορεί να εξαχθεί από αυτό. Η λογική είναι αντίστοιχη της συμβατικής αλληλογραφίας όπου το *Προς* της επιστολής μπορεί να διαφέρει από τον παραλήπτη του φακέλου που την περιέχει. Παρόμοια, το *From:* μπορεί να μην είναι ο αποστολέας *MAIL FROM:* του μηνύματος.

Για τη ροή μηνυμάτων κατά την αποστολή ηλεκτρονικής αλληλογραφίας δείτε στην ιστοσελίδα https://www.eventhelix.com/Networking/SMTP_Sequence_Diagram.pdf ένα απλό παράδειγμα. 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. Σημειώστε ότι οι εντολές αφορούν τον φάκελο (envelope) της αλληλογραφίας και δεν σχετίζονται με τις επικεφαλίδες (headers) του ηλεκτρονικού μηνύματος. Για τις επικεφαλίδες του μηνύματος διαβάστε περισσότερα στο RFC 5322. Ειδικά για τις επικεφαλίδες ιχνηλάτησης (trace), που περιγράφουν την πορεία για την παράδοση του μηνύματος, συμβουλευθείτε τις αντίστοιχες παραγράφους του RFC 5321.

Για την εκτέλεση της άσκησης αυτής θα χρησιμοποιήσετε τη διεύθυνση ηλεκτρονικού σας ταχυδρομείου στο ΕΜΠ *elxxxxx@mail.ntua.gr*[1]. 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. Προηγουμένως θα πρέπει να συνδεθείτε με OpenVPN 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 <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
```

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

Με την εγκατάσταση σύνδεσης στον εξυπηρετητή SMTP, ο εξυπηρετητής αποστέλλει ένα μήνυμα χαιρετισμού αποτελούμενο από ένα κωδικό απόκρισης συνοδευόμενο από το DNS όνομα 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.]*

[1] Αφού ολοκληρώσετε την άσκηση με αυτή τη διεύθυνση, μπορείτε να την επαναλάβετε με τη διεύθυνση ηλεκτρονικού ταχυδρομείου που συνήθως χρησιμοποιείτε και να εντοπίσετε διαφορές.

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

1.3 Ποιο το DNS όνομα του εξυπηρετητή;
1.4 Ποιο είναι το αναγνωριστικό κείμενο;
1.5 Ποιος είναι ο κωδικός απόκρισης στην εντολή HELP του πρωτοκόλλου SMTP;
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.
1.7 Η απόκριση περιλαμβάνει πολλές γραμμές. Πώς διακρίνεται η τελευταία γραμμή της; *[Υπόδειξη: Αναζητήστε multiline replies στο RFC 5321.]*
1.8 Ποιος είναι ο κωδικός απόκρισης στην εντολή HELO του πρωτοκόλλου SMTP;
1.9 Εμφανίζεται στην απόκριση το όνομα υπολογιστή που δηλώνει η εντολή HELO; Εάν όχι, τι περιέχει η απόκριση;
1.10 Πόσες γραμμές περιλαμβάνει η απόκριση του εξυπηρετητή στην εντολή EHLO του πρωτοκόλλου SMTP;
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).]*
1.12 Είναι προφανές ότι ο εξυπηρετητής smtp.ntua.gr υποστηρίζει το ESMTP. Πότε έγινε αυτό εμφανές για πρώτη φορά;

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 <Enter>. *Προσοχή στην κενή γραμμή μετά τις επικεφαλίδες και στις διευθύνσεις ηλεκτρονικού ταχυδρομείου που θα πρέπει να περικλείονται από τους χαρακτήρες "<" και ">".* 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:<elxxxxx@mail.ntua.gr>
DATA
From: netwoking@guru.org
To: netwoking@apprentice.org
Subject: Test Message

This is a test message.
1
2
3
.
QUIT
```

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.

1.13 Καταγράψτε την ημερομηνία και ώρα που δηλώνει στην απόκρισή του ο εξυπηρετητής relay.ntua.gr μόλις συνδεθήκατε σε αυτόν.
1.14 Ποια είναι η απόκριση του εξυπηρετητή και ο αντίστοιχος κωδικός απόκρισης στην εντολή DATA του πρωτοκόλλου SMTP;
1.15 Ποιος είναι ο ρόλος της τελείας που πληκτρολογείτε πριν την εντολή QUIT κατά την επικοινωνία SMTP με τον εξυπηρετητή;

1.16 Ποια είναι η απόκριση του εξυπηρετητή και ο αντίστοιχος κωδικός απόκρισης μετά το τέλος της εισαγωγής δεδομένων;
1.17 Ποιος εμφανίζεται ως αποστολέας του μηνύματος που λάβατε; Αυτός του φακέλου ή αυτός του κειμένου της επικεφαλίδας From: του μηνύματος;
1.18 Αφού το ανοίξετε, ποιος εμφανίζεται ως παραλήπτης του μηνύματος; Αυτός του φακέλου ή αυτός του κειμένου της επικεφαλίδας To: του μηνύματος;

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;
1.20 Σε ποιες επικεφαλίδες του μηνύματος εμφανίζεται η διεύθυνση παραλήπτη του φακέλου που ορίσατε με την εντολή RCPT TO;
1.21 Σε ποια επικεφαλίδα εμφανίζεται το αναγνωριστικό που επέστρεψε ο εξυπηρετητής και καταγράψατε στην ερώτηση 1.16;
1.22 Σε ποιες επικεφαλίδες εμφανίζεται το δηλωθέν στην εντολή HELO όνομα υπολογιστή;
1.23 Εντοπίστε την ακολουθία επικεφαλίδων Received:. Ποια είναι τα ονόματα των MTA που χειρίσθηκαν το μήνυμα;
1.24 Ποια πρωτόκολλα χρησιμοποιήθηκαν για την προώθηση του μηνύματος; *[Υπόδειξη: Δείτε σημείωση για Mail Transmission Types στην ιστοσελίδα MAIL Parameters (iana.org).]*
1.25 Καταγράψτε την ημερομηνία και ώρα που αναφέρει το κείμενο της επικεφαλίδας Date:. Πώς προέκυψε αυτή αφού δεν την ορίσατε ρητά;

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
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;
1.27 Ποιο είναι το φίλτρο απεικόνισης που εφαρμόσατε;
1.28 Ποιο πρωτόκολλο μεταφοράς χρησιμοποιεί το πρωτόκολλο εφαρμογής SMTP;
1.29 Καταγράψτε τις θύρες (προέλευσης και προορισμού) του πρωτοκόλλου μεταφοράς που χρησιμοποιούνται για την επικοινωνία.
1.30 Ποια από τις παραπάνω θύρες αντιστοιχεί στο πρωτόκολλο εφαρμογής SMTP;
1.31 Πόσα τεμάχια TCP απαιτούνται για τη μεταφορά της εντολής QUIT προς τον εξυπηρετητή;
1.32 Ποια είναι η απόκριση του εξυπηρετητή και ο αντίστοιχος κωδικός απόκρισης στην εντολή QUIT του πρωτοκόλλου SMTP;
1.33 Προκαλεί η εντολή QUIT του πρωτοκόλλου SMTP την άμεση απόλυση της σύνδεσης TCP; Γιατί;

2. Το πρωτόκολλο DHCP

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

κονσόλα του και συνήθως απαιτούσε 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, αργότερα προσωπικοί υπολογιστές και σήμερα πληθώρα φορητών συσκευών.

Αρχικά, για τέτοιες περιπτώσεις χρησιμοποιήθηκε ένα ειδικό πρωτόκολλο, το Reverse Address Resolution Protocol (RARP). Το RARP που ορίζεται στο RFC 903 επέτρεπε σε ένα μηχάνημα να «μάθει» την IP διεύθυνσή του, μέσω της παγκοσμίως μοναδικής διεύθυνσης MAC της κάρτας δικτύου του, και μετά να ξεκινήσει την κανονική λειτουργία του TCP/IP. Ένα άλλο πρωτόκολλο, το BOOTstrap Protocol (BOOTP), ορίζεται στο RFC 951, αναπτύχθηκε αργότερα για να επιτρέψει σε φτηνούς σταθμούς εργασίας που δεν διέθεταν χώρο μόνιμης αποθήκευσης (σκληρό δίσκο) να λαμβάνουν κατά την εκκίνηση την IP διεύθυνσή τους, το όνομα του αρχείου με την εικόνα του λειτουργικού τους συστήματος και τον εξυπηρετητή όπου αυτό είναι αποθηκευμένο. Το BOOTP στη συνέχεια εμπλουτίστηκε με ένα μηχανισμό επέκτασης (Vendor Information Extensions), ώστε να επιτρέπονται επιπλέον δεδομένα, ως προαιρετικές επιλογές (options) στο τελευταίο μέρος της επικεφαλίδας BOOTP που μέχρι τότε παρέμενε αχρησιμοποίητο. Αυτή η έκδοση του BOOTP έμελλε να είναι ο πρόγονος του DHCP. Ο τύπος μηνύματος DHCP είναι μια τέτοια επιλογή και ορίζονται επιπλέον επιλογές DHCP πέραν αυτών που προϋπήρξαν. Οι επιλογές, πλην των 0 (pad) και 255 (end) που έχουν μήκος ένα byte, είναι τριάδες κωδικός/μήκος/τιμή. Για την πλήρη λίστα αυτών δείτε στο http://www.networksorcery.com/enp/protocol/bootp/options.htm.

Το DHCP χρησιμοποιεί το πρωτόκολλο BOOTP προσθέτοντας δύο κύριες λειτουργίες σε αυτό. Ορίζει μηχανισμούς δυναμικής εκχώρησης διευθύνσεων IPv4 και ανάκτησης επιπλέον δικτυακών ρυθμίσεων. Οι διευθύνσεις IPv4 εκχωρούνται στους σταθμούς εργασίας ως δάνειο για καθορισμένο χρονικό διάστημα. Έτσι επιτυγχάνεται η επαναχρησιμοποίηση ενός πλήθους διευθύνσεων IPv4 από πολλούς σταθμούς εργασίας. Πέραν των διευθύνσεων IPv4, ο σταθμός εργασίας μπορεί να ανασύρει τις επιπλέον πληροφορίες διάρθρωσης που απαιτούνται προκειμένου να λειτουργήσει στο δίκτυο, όπως π.χ. την προκαθορισμένη πύλη και τις διευθύνσεις των εξυπηρετητών DNS. Ουσιαστικά, το DHCP αναλαμβάνει να ορίσει αυτόματα, χωρίς την παρουσία διαχειριστή δικτύου, τις αναγκαίες παραμέτρους λειτουργίας ενός υπολογιστή.

Σε συντομία, η λειτουργία του DHCP είναι η ακόλουθη. Μόλις ο υπολογιστής εκκινήσει εκπέμπει ένα μήνυμα αναζήτησης εξυπηρετητή DHCP (*DHCP Discover*). Οι εξυπηρετητές DHCP που ακούν αυτό το μήνυμα, απαντούν με μήνυμα προσφοράς (*DHCP Offer*) το οποίο ορίζει διευθύνσεις IPv4. Ο υπολογιστής επιλέγει μία προσφορά και εκπέμπει αίτηση (*DHCP Request*) προς όλους τους εξυπηρετητές δηλώνοντας τη συγκεκριμένη διεύθυνση IPv4 που επέλεξε. Όλοι οι άλλοι εξυπηρετητές αποχωρούν και ο επιλεχθείς εξυπηρετητής στέλνει επιβεβαίωση (*DHCP ACK*) για την εκχωρούμενη διεύθυνση IPv4.

Το DHCP υποστηρίζει 3 μηχανισμούς για να αντιστοιχίζει διευθύνσεις:

- Δυναμική αντιστοίχηση (εκχώρηση μιας από τις διαθέσιμες διευθύνσεις IPv4 για συγκεκριμένο διάστημα)
- Αυτόματη αντιστοίχηση (μόνιμη για απεριόριστο χρόνο εκχώρηση μιας από τις διαθέσιμες διευθύνσεις IPv4)
- Χειροκίνητη αντιστοίχηση (εκχώρηση συγκεκριμένης διεύθυνσης IPv4 που ορίζει ο διαχειριστής με βάση τη διεύθυνση MAC του αιτούντος)

Όταν η διεύθυνση IPv4 παραχωρείται με δάνειο για συγκεκριμένη περίοδο δανεισμού (lease time), ο υπολογιστής πρέπει να ανανεώσει το δάνειο προτού λήξει η περίοδος αυτή. Αυτό γίνεται με μήνυμα *DHCP Request* που περιέχει την ήδη εκχωρημένη διεύθυνση. Όταν τελειώσει με τη χρήση της εκχωρημένης διεύθυνσης, ο υπολογιστής στέλνει μήνυμα απόλυσής της (*DHCP Release*) προκειμένου αυτή να απελευθερωθεί προς χρήση από άλλο μηχάνημα. Εάν δεν το πράξει, η διεύθυνση απελευθερώνεται με τη λήξη της περιόδου δανεισμού.

Στην ιστοσελίδα https://www.eventhelix.com/Networking/Dhcp.pdf θα βρείτε ένα πλήρες παράδειγμα της διαδικασίας ανταλλαγής μηνυμάτων DHCP για τέσσερις διαφορετικές περιστάσεις

δυναμικής εκχώρησης διεύθυνσης IPv4 σε έναν φορητό υπολογιστή. Επιπλέον πληροφορίες για τα πεδία και τις επιλογές (options) των μηνυμάτων DHCP που ανταλλάσσονται θα βρείτε στην ιστοσελίδα https://www.eventhelix.com/Networking/dhcp-flow/dhcp-sequence-diagram.pdf.

Στο IPv6 οι σταθμοί εργασίας ανακαλύπτουν τον πλησιέστερο δρομολογητή μέσω της λήψης μηνυμάτων RA (Router Advertisement) και με την πληροφορία που λαμβάνουν από αυτά μπορούν να παράγουν αυτόματα την IPv6 διεύθυνσή τους χρησιμοποιώντας τη διαδικασία Stateless Address Autoconfiguration (SLAAC). Το πρωτόκολλο Dynamic Host Configuration Protocol version 6 (DHCPv6) που ορίζεται στο RFC 8415 χρησιμοποιείται για να παρέχει μόνο για όποια επιπλέον πληροφορία ζητηθεί (stateless DHCPv6), όπως π.χ. τους εξυπηρετητές DNS. Μπορεί όμως να χρησιμοποιηθεί και για την απόδοση διευθύνσεων (stateful DHCPv6) όταν θέλουμε συγκεκριμένες διευθύνσεις IPv6 και όχι τυχαίες ή βασισμένες στη MAC διεύθυνση της κάρτας δικτύου, όπως γίνεται στο SLAAC.

Στη συνέχεια με τη βοήθεια του Wireshark θα καταγράψετε την κίνηση στο τοπικό σας δίκτυο ενώ κάνετε χρήση της υπηρεσίας DHCP, οπότε εάν είστε συνδεδεμένοι με OpenVPN στο εσωτερικό δίκτυο του ΕΜΠ, αποσυνδεθείτε. Επειδή δεν θα εφαρμόσετε φίλτρο σύλληψης κατά την καταγραφή, ίσως συλλάβετε μηνύματα DHCP που αφορούν άλλους υπολογιστές του τοπικού σας δικτύου. Για τον λόγο αυτό, προτού ξεκινήσετε την καταγραφή, δείτε τις τρέχουσες ρυθμίσεις της κάρτας δικτύου του υπολογιστή σας ώστε να είστε σε θέση να ξεχωρίσετε μηνύματα που δεν αφορούν τον 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).

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. Υπενθυμίζεται, ότι στο οικιακό δίκτυο, η υπηρεσία DHCP παρέχεται από τον οικιακό δρομολογητή (την προκαθορισμένη πύλη).

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 IPv4 της κάρτας δικτύου του υπολογιστή σας. 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. Εφαρμόστε κατάλληλο φίλτρο απεικόνισης ώστε να εμφανίζονται μόνο μηνύματα DHCP. Ποια είναι η σύνταξή του;
2.3. Ποια είδη μηνυμάτων DHCP παρήχθησαν από την αλληλουχία εντολών απόλυσης (release), εκχώρησης (πρώτο renew) και ανανέωσης (δεύτερο renew) δικτυακών ρυθμίσεων;
2.4. Ποιο πρωτόκολλο μεταφοράς χρησιμοποιεί το DHCP;
2.5. Καταγράψτε τις θύρες πηγής και προορισμού των παραπάνω μηνυμάτων.
2.6. 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.]*
2.7. 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.
2.8. Πώς γίνεται κατανοητό ότι το μήνυμα BOOTP μεταφέρει επιλογές DHCP, δηλαδή, πρόκειται για μήνυμα DHCP; *[Υπόδειξη: Δείτε παράγραφο The Client-Server Protocol στο RFC 2131.]*

2.9. Ποια είδη μηνυμάτων BOOTP μεταφέρουν τα μηνύματα DHCP που καταγράψατε προηγουμένως;
2.10. Ποια άλλα πεδία της επικεφαλίδας BOOTP, πλην αυτών που σημειώσατε στο σχήμα, υπάρχουν πριν τις επιλογές DHCP;
2.11. Ποιο είναι το όνομα και ο κωδικός της επιλογής (option) που δηλώνει τον τύπο μηνύματος DHCP;
2.12. Για κάθε μήνυμα DHCP που παράχθηκε, να καταγράψετε το μήκος και την τιμή του πεδίου της επιλογής (option) που προσδιορίζει τον τύπο του; *[Υπόδειξη: Στο παράθυρο λεπτομερειών πακέτου του Wireshark αναπτύξτε το περιεχόμενο της επιλογής DHCP Message Type.]*
2.13. Ποιο είναι το πρώτο μήνυμα DHCP που έστειλε ο υπολογιστής σας; Ποιος ο σκοπός του;
2.14. Πού ανήκουν οι διευθύνσεις MAC και IPv4 του αποστολέα και του παραλήπτη του παραπάνω μηνύματος;

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.

2.15. Καταγράψτε τις MAC διευθύνσεις πηγής και προορισμού που χρησιμοποιήθηκαν κατά την ανταλλαγή των μηνυμάτων *DHCP Discover/Offer/Request/ACK* μεταξύ του υπολογιστή σας και του εξυπηρετητή DHCP.
2.16. Καταγράψτε τις διευθύνσεις IPv4 αποστολέα και παραλήπτη των παραπάνω τεσσάρων μηνυμάτων.
2.17. Τι υποδηλώνει η διεύθυνση IPv4 του παραλήπτη του μηνύματος *DHCP Discover*;
2.18. Δεδομένου ότι το παραπάνω μήνυμα προέρχεται από τον υπολογιστή σας, αιτιολογήστε τη χρήση της διεύθυνσης 0.0.0.0 ως διεύθυνσης IPv4 του αποστολέα.
2.19. Ποια είναι η διεύθυνση IPv4 που προτείνει ο εξυπηρετητής DHCP στον υπολογιστή σας με το μήνυμα *DHCP Offer* και σε ποιο πεδίο της επικεφαλίδας περιέχεται η τιμή της;
2.20. Προς ποια διεύθυνση (MAC και IPv4) στάλθηκε το προηγούμενο μήνυμα *DHCP Offer;*
2.21. 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*;
2.22. Ποια είναι η διεύθυνση IPv4 του εξυπηρετητή DHCP όπως προκύπτει από το μήνυμα *DHCP Offer*; Σε ποιο πεδίο της επικεφαλίδας και/ή σε ποια επιλογή (option) περιέχεται η τιμή της;
2.23. Ποια είναι η διεύθυνση IPv4 που ζητά ο υπολογιστής σας από τον εξυπηρετητή DHCP με το μήνυμα *DHCP Request* και σε ποια επιλογή (option) περιέχεται η τιμή της;
2.24. Προς ποια διεύθυνση (MAC και IPv4) στάλθηκε το προηγούμενο μήνυμα *DHCP Request* και πώς αναγνωρίζει ο εξυπηρετητής DHCP ότι το μήνυμα απευθύνεται σε αυτόν; *[Υπόδειξη: Δείτε απάντηση στην ερώτηση 2.22.]*
2.25. Ποια διεύθυνση IPv4 αποδίδεται τελικά στον υπολογιστής σας με το μήνυμα *DHCP ACK* και σε ποιο πεδίο της επικεφαλίδας περιέχεται η τιμή της;
2.26. Συμπίπτει η διεύθυνση IPv4 που εκχωρήθηκε με αυτή που είχατε καταγράψει αρχικά στο ερώτημα 2.1;
2.27. Ποια είναι η μάσκα υποδικτύου για τη διεύθυνση IPv4 που εκχωρήθηκε και σε ποια επιλογή (option) περιέχεται η τιμή της;
2.28. Για πόσο χρόνο διαρκεί η εκχώρηση αυτής της διεύθυνσης IPv4 και σε ποια επιλογή (option) περιέχεται η τιμή του;

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.

2.29. Να καταγραφεί ο κωδικός της επιλογής (option) Parameter Request List.
2.30. 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.]*
2.31. Πόσες παραμέτρους ζήτησε ο υπολογιστής σας με το μήνυμα *DHCP Discover* και ποιες προσδιορίζει τελικά ο εξυπηρετητής DHCP 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.]*

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

2.32. 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;
2.33. Παρατηρείτε την αποστολή ARP Request από τον υπολογιστή σας αμέσως μετά το μήνυμα *DHCP ACK*;
2.34. Εάν ναι, πόσα τέτοια ARP Request στάλθηκαν; Εάν όχι, αγνοήστε τις επόμενες δύο ερωτήσεις.
2.35. Ποιου υπολογιστή (δηλαδή, για ποια διεύθυνση IPv4) αναζητεί ο υπολογιστής σας τη διεύθυνση MAC;
2.36. Εξηγήστε τη χρησιμότητα αυτών των πλαισίων ARP *[Υπόδειξη: Αναζητήστε το "gratuitous ARP"ή "ARP probe"στο google.]*;

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).

2.37. Ποια είδη μηνυμάτων DHCP παρήχθησαν με την εκτέλεση της εντολής ανανέωσης (δεύτερο renew);
2.38. 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 2.15 και 2.16.]*
2.39. 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 2.23;
2.40. Σε ποια επικεφαλίδα ή επιλογή (option)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 2.25;

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

2.41. Ποια είναι η τιμή του για το μήνυμα DHCP που σχετίζεται με την εντολή απόλυσης (release);
2.42. Ποια είναι η τιμή του για τα μηνύματα DHCP που σχετίζονται με την εντολή εκχώρησης (πρώτο renew);
2.43. Ποια είναι η τιμή του για τα μηνύματα DHCP που σχετίζονται με την εντολή ανανέωσης (δεύτερο renew);
2.44. Ποιος είναι ο σκοπός του πεδίου Transaction ID;

Ονοματεπώνυμο: Νικόλας Μπέλλος	**Ομάδα:** 3
Όνομα PC/ΛΣ: BELLOS-DELL-G3	**Ημερομηνία:** 27 / 12 / 2021
Διεύθυνση IP: 192 . 168 . 1 . 9	**Διεύθυνση MAC:** 7C - 2A - 31 - 40 - C9 - AF

Εργαστηριακή Άσκηση 9
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 Η πρόσβαση στον εξυπηρετητή smtp.ntua.gr μέσω της πόρτας 25

1.2 Reply Code: 220. Σημαίνει οτι ο εξυπηρετητής είναι ανοιχτός και έτοιμος για τη σύνδεση.

1.3 DNS name: smtp2.ntua.gr

1.4 Αναγνωριστικό κείμενο : ESMTP Sendmail 8.15.2/8.15.2; Mon, 27 Dec 2021 11:49:50 +0200 (EET)

1.5 Κωδικός απόκρισης : 214

1.6 16 υποστηριζόμενες εντολές. 3 από αυτές : HELO, EHLO, MAIL

1.7 Μετά το κωδικό της υπάρχει space " " αντί για παύλα "-"

1.8 Κωδικός απόκρισης : 250

1.9 Η απόκριση περιέχει την IP του υπολογιστή που δηλώνει η εντολή HELO

1.10 Περιέχει 9 γραμμές

1.11 Περιέχει και ονόματα παραμέτρων που συνοδεύουν την εντολή

1.12 Έγινε εμφανές μετά την εντολή EHLO λόγω της παραμέτρου ENHANCEDSTATUSCODES

1.13 Mon, 27 Dec 2021 00:02:35

1.14 Κωδικός απόκρισης : 354, η απόκριση ήταν θετική

1.15 Η εντολή DATA μας λέει να συμπληρώσουμε μία τελεία "." μετά το τέλος του email.

1.16 Κωδικός απόκρισης : 250, η απόκριση μας λέει ότι το μήνυμα έγινε δεκτό για αποστολή (Message accepted for delivery)

1.17 networking@guru.org → αυτός της επικεφαλίδας From :

1.18 netwoking@apprentice.org → αυτός της επικεφαλίδας To :

1.19 Στην επικεφαλίδα : Return-Path

1.20 Στις επικεφαλίδες : Received

1.21 Στην επικεφαλίδα : Message-Id

1.22 Στις επικεφαλίδες : Received και X-Authentication-Warning

1.23 Ονόματα MTA : f0.mail.ntua.gr και achilles.noc.ntua.gr

1.24 Πρωτόκολλα : ESMTP, SMTP, LMTPA

1.25 Date: Mon, 27 Dec 2021 00:02:35 +0200 (EET). Προέκυψε από την ώρα που είναι καταγεγραμένη στο server με τον οποίο συνδεθήκαμε με telnet

1.26 Capture filter : host 147.102.222.210

1.27 Display filter : smtp

1.28 Το πρωτόκολλο TCP

1.29 Source Port: 25, Destination Port: 51072

1.30 Η θύρα 25

1.31 1 τεμάχιο

1.32 Κωδικός απόκρισης : 221. Απόκριση : 2.0.0 achilles.noc.ntua.gr closing connection

1.33 Όχι, δεν υπάρχει άμεση απόλυση σύνδεσης. Πρέπει να σταλθούν ακόμα κάποια πακέτα TCP για την επιβεβαίωση απόλυσης σύνδεσης

2

2.1 MAC : 7C-2A-31-40-C9-AF, IPv4 : 192.168.1.9, Subnet Mask : 255.255.255.0, DHCP Server : 192.168.1.1

2.2 Display filter : dhcp

2.3 Release, Discover, Offer, Request, ACK

2.4 Το πρωτόκολλο UDP

2.5 Source Port: 68, Destination Port: 67

2.6 Και η 68 και η 67 είναι well-known ports για το DHCP

2.7 ..... (σημειώστε ονόματα στο σχήμα στην επόμενη σελίδα)

2.8 Από το πεδίο ‘Magic Cookie

Message type	Hardware type	Hardware address	Hops
Transaction ID			
Seconds elapsed		Bootp flags	
Client IP address			
Your IP address			
Next Server IP address			
Relay agent IP address			
Client MAC address			

2.9 Boot request, Boot reply

2.10 Client hardware address padding, Server host name, Boot file name, Magic cookie

2.11 (53) DHCP Message Type

2.12 Release - Length: 1, Code: 7, Discover - Length: 1, Code: 1, Offer - Length: 1, Code: 2 Request - Length: 1, Code: 3, ACK - Length: 1, Code: 5

2.13 Το DHCP Release και έχει σκοπό την αποδέσμευση των ρυθμίσεων δικτύου

2.14 Οι MAC, IPv4 του αποστολέα ανήκουν στον υπολογιστή μου και του παραλήπτη στο default gateway του οικειακού δικτύου μου (συμπίπτει με το DHCP Server)

2.15 Discover - Source: 7c:2a:31:40:c9:af, Destination: ff:ff:ff:ff:ff:ff. Offer - Source: 50:78:b3:cd:48:fa, Destination: 7c:2a:31:40:c9:af. Request - Source: 7c:2a:31:40:c9:af, Destination: ff:ff:ff:ff:ff:ff. ACK - Source: 50:78:b3:cd:48:fa, Destination: 7c:2a:31:40:c9:af

2.16 Discover - Source Address: 0.0.0.0, Destination Address: 255.255.255.255. Offer - Source Address: 192.168.1.1, Destination Address: 255.255.255.255. Request - Source Address: 0.0.0.0, Destination Address: 255.255.255.255. ACK - Source Address: 192.168.1.1, Destination Address: 255.255.255.255

2.17 Ότι το πακέτο μετατίδεται σε όλες τις συσκευές του τοπικού δικτύου (broadcast)

2.18 Ο υπολογιστής μου τη δεδομένη στιγμή δεν έχει πάρει κάποια IPv4 διεύθυνση και άρα αυτή αναπαριστάται από τη 0.0.0.0

2.19 Προτείνει τη διεύθυνση 192.168.1.9 στο πεδίο 'Your (client) IP address'

2.20 Προς τη διεύθυνση MAC του υπολογιστή μου (Client MAC address πεδίο) και στην IPv4 255.255.255.255 (broadcast)

2.21 Η τιμή της διεύθυνσης MAC είναι, αλλά η IPv4 διεύθυνση είναι broadcasting οπότε δεν είναι

2.22 Στο option 'DHCP Server Identifier'

2.23 Η 192.168.1.9 και βρίσκεται στο option 'Requested IP Address'

2.24 Στάλθηκε στη MAC: ff:ff:ff:ff:ff:ff και IPv4: 255.255.255.255. Το γνωρίζει από το option 'DHCP Server Identifier'

2.25 Η διεύθυνση 192.168.1.9 που βρίσκεται στο πεδιο 'Your (client) IP address'.

2.26 Ναι συμπίπτει

2.27 Subnet Mask: 255.255.255.0 και βρίσκεται στο option 'Subnet Mask'

2.28 Διαρκεί 21 μέρες και βρίσκεται στο option 'IP Address Lease Time'.

2.29 Code: 55

2.30 (1) Subnet Mask: είναι η μάσκα υποδικτύου, (3) Router: είναι ο δρομολογητής του τοπικού δικτύου, (6) Domain Name Server: Είναι ο υπολογιστής που αναλαμβάνει τη μετάφραση των διευθύνσεων

2.31 Ζήτησε 14 παραμέτρους και ο εξυπηρετητής προσδιορίζει 3 (τις (1), (3) και (6))

2.32 Display filter: dhcp or arp

2.33 Ναι παρατηρώ

2.34 Στέλνονται 3 τέτοια requests

2.35 Αναζητά τη διεύθυνση 192.168.1.9

2.36 Στέλνονται για να επιβεβαιώσει ο υπολογιστής ότι η διεύθυνση IPv4 δεν χρησιμοποιείται από άλλο υπολογιστή

2.37 Request και ACK

2.38 Διαφέρει ναι, στην εντολή εγχώρησης η IP του αποστολέα είναι 0.0.0.0 και η MAC του παραλήπτη είναι ff:ff:ff:ff:ff:ff, ενώ στην εντολή ανανέωσης αυτές οι τιμές είναι ανανεωμένες στις 192.168.1.9 και 50:78:b3:cd:48:fa

2.39 Στο πεδίο 'Client IP address'. Ναι υπάρχει στο ότι στην 2.23 η διεύθυνση βρισκόταν σε option, ενώ τώρα σε πεδίο.

2.40 Στο πεδίο 'Your (client) IP address'. Όχι δεν υπάρχει κάποια διαφορά.

2.41 Transaction ID: 0x4f785ec7

2.42 Transaction ID: 0x02da8f21

2.43 Transaction ID: 0x30272ff2

2.44 Ο σκοπός του είναι η ταυτοποίηση και η ομαδοποίηση των dhcp requests και responses