

Όνοματεπώνυμο:	Ιωάννης Γιαννούκος	Ομάδα:	3
Όνομα PC/ΛΣ:	JohnJohn / Windows 11	Ημερομηνία:	11/1/2023
Διεύθυνση IP:	147.102.200.49	Διεύθυνση MAC:	3C-6A-A7-9A-B3-CF

## 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.

#### Άσκηση 1

1.1) Με την εντολή “telnet smtp.ntua.gr 25” συνδεόμαστε με τον εξυπηρετητή smtp.ntua.gr στην θύρα 25.

1.2) Reply code: 220

1.3) DNS όνομα εξυπηρετητή: smtp3.ntua.gr

1.4) “smtp3.ntua.gr ESMTP Sendmail 8.15.2/8.15.2; Thu, 8 Dec 2022 10:49:08 +0200 (EET)”

1.5) 214

1.6) Ο εξυπηρετητής υποστηρίζει 16 εντολές, τρεις εκ των οποίων είναι οι MAIL, DATA και RSET.

1.7) Κάθε απάντηση του εξυπηρετητή περιέχει έναν κωδικό στην αρχή του, μία παύλα “-” ακριβώς μετά και, τέλος μία γραμμή του μηνύματος. Η τελευταία γραμμή περιέχει τον κωδικό, ένα κενό “ ” και του υπόλοιπους χαρακτήρες, σημαίνοντας έτσι το τέλος του μηνύματος που θέλει να αποστείλει.

1.8) 501

1.9) Όχι, δεν δηλώνεται το όνομα του υπολογιστή που έχει ως όρισμα η εντολή HELO. Ωστόσο, το μήνυμα που εμφανίζεται στον πελάτη (εμένα) είναι το εξής: “250 smtp3.ntua.gr Hello [147.102.238.51], pleased to meet you”.

1.10) 9 γραμμές

1.11) Με την εντολή EHLO ανακοινώνονται από τον εξυπηρετητή υπηρεσίες που υποστηρίζει.

1.12) Ναι. Αυτή την πληροφορία μας την φανερώνει ο εξυπηρετητής στο πρώτο μήνυμα που στέλνει, δηλαδή αμέσως μετά τη σύνδεσή μας με αυτόν. Η γραμμή αυτή

περιέχει τα εξής: “220 smtp3.ntua.gr ESMTP Sendmail 8.15.2/8.15.2; Thu, 8 Dec 2022 11:10:08 +0200 (EET)”

1.13) Thu, 8 Dec 2022 11:01:12 +0200 (EET)

1.14) Ο εξυπηρετητής στέλνει το εξής μήνυμα: “354 Enter mail, end with “.” On a line by itself”. Ο κωδικός απόκρισης, επομένως, είναι 354

1.15) Η τελεία έχει τον ρόλο του delimiter, δηλαδή δηλώνει που τελειώνει το κείμενο που στέλνουμε στο μήνυμα ηλεκτρονικού ταχυδρομείου. Στην απάντηση που δίνει ο εξυπηρετητής, που σημειώθηκε στην απάντηση του προηγούμενου υποερωτήματος, αναφέρει ότι η τελεία αυτή πρέπει να βρίσκεται σε μία γραμμή από μόνη της.

1.16) Ο εξυπηρετητής στέλνει το εξής μήνυμα: “250 2.0.0 2B899AXj052476 Message accepted for delivery”.

1.17) Ως αποστολέας εμφανίζεται ο “netwoking@guru.org”, δηλαδή το όνομα του πεδίου Το: του μηνύματος.

1.18) Αυτός της επικεφαλίδας “To:” του μηνύματος.

1.19) Στην επικεφαλίδα “Return-Path”.

1.20) Στην επικεφαλίδα “X-Envelope-To”

1.21) Στην επικεφαλίδα “Received” στην γραμμή  
“by Diomedes.noc.ntua.gr(8.13.0/8.13.0) with SMTP id 2B899AXj052476”.

1.22) Στην επικεφαλίδα “Received” στην γραμμή  
“from example.com [147.102.238.43])”.

1.23) diomedes.noc.ntua.gr

1.24) SMTP

1.25) “Thu, 8 Dec 2022 11:00:38 +0200 (EET)”.

Η ημερομηνία αυτή προέκυψε από την ώρα που ο MTA προσπάθησε να στείλει το μήνυμα στην διεύθυνση [el18918@mail.ntua.gr](mailto:el18918@mail.ntua.gr).

1.26) Φίλτρο σύλληψης: “host relay.ntua.gr”.

1.27) Φίλτρο απεικόνισης: “smtp”

1.28) TCP

1.29) Src Port: 25  
Dst Port: 51999

1.30) Στο πρωτόκολλο εφαρμογής SMTP αντιστοιχεί η θύρα 25.

1.31) 1 τεμάχιο

1.32) Απόκριση εξυπηρετητή: “2.0.0 diomedes.noc.ntua.gr closing connection”  
Κωδικός απόκρισης: 221

1.33) Όχι. Με την εντολή QUIT ο πελάτης ενημερώνει ότι θέλει να διακόψει την επικοινωνία του με τον εξυπηρετητή αφήνοντάς τον να απολύσει πρώτος την σύνδεση. Αυτό λογικά συμβαίνει για να γνωρίζει ο πελάτης ποια μηχανήματα είναι ικανά να λαμβάνουν πληροφορία από αυτόν, αυξάνοντας έτσι την ασφάλειά του.

## ***Άσκηση 2 (IP: 147.102.238.130)***

2.1) MAC Address: 3C – 6A – A7 – 9A – B3 – CF  
IPv4 Address: 147.102.238.130  
Subnet Mask: 255.255.252.0  
DHSP Server: 147.102.236.230

2.2) Φίλτρο Απεικόνισης: “dhcp”

2.3) Από την αλληλουχία αυτών των εντολών παρήχθησαν τα μηνύματα *DHCP Release*, *DHCP Discover* και *DHCP Request*.

2.4) UDP

2.5) Όλα τα μηνύματα έχουν: Src Port → 68 , Dst Port → 67

2.6) Και οι δύο θύρες, 68 και 67, είναι συνήθεις θύρες της υπηρεσίας DHCP.

2.7) (Σχεδιάγραμμα – Πίνακας)

2.8) Την πληροφορία αυτή την λαμβάνουμε από την επικεφαλίδα “Magic cookie”.

2.9) Μεταφέρουν μηνύματα ειδών “Release”, “Discover” και “Request”.

2.10) Message type  
Hardware type  
Hardware address length  
Hops  
Transaction ID  
Seconds elapsed  
Bootp flags  
Client IP address  
Your (client) IP address  
Next server IP address  
Relay agent IP address  
Client MAC address  
Client hardware address padding  
Server host name not given

Boot file name not given  
Magic cookie

2.11) DHCP Message Type  
Κωδικός: 53

2.12)

Message Type [1 byte]	Hardware Type [1 byte]	Hardware Address Length [1 byte]	Hops [1 byte]
Transaction ID [4 bytes]			
Seconds elapsed [2 bytes]		Bootp flags [2 bytes]	
Client IP Address [4 bytes]			
Your (client) IP address [4 bytes]			
Next server IP address [4 bytes]			
Relay agent IP address [4 bytes]			
Client MAC address [4 bytes]			

2.13) Το πρώτο μήνυμα που έστειλε ο υπολογιστής μου στον DHCP Server είναι το *DHCP Release* με σκοπό να αποδεσμεύσει την διεύθυνση IP που δόθηκε αρχικά στον υπολογιστή μου.

2.14) Η διεύθυνση MAC του αποστολέα ανήκει στον υπολογιστή μου και η διεύθυνση IP του αποστολέα ανήκε στον υπολογιστή μου, μέχρι που έγινε αίτηση για να αφηθεί. Οι διευθύνσεις MAC και IP του παραλήπτη ανήκουν στον DHCP server.

2.15) Σε όλη τη διαδικασία ανταλλαγής μηνυμάτων η MAC διεύθυνση του υπολογιστή μου έμεινε (προφανώς) αμετάβλητη και, έτσι, χρησιμοποιείτο η ίδια διεύθυνση σε όλα τα μηνύματα. Η MAC που χρησιμοποιείτο για τον εξυπηρετητή DHCP, ωστόσο, άλλαζε, καθώς αρχικά δεν έχει ορισθεί από ποιον θα ληφθεί η διεύθυνση IP. Έτσι, ίσχυσαν τα παρακάτω:

Κατά την διαδικασία <i>Discover</i> :	MAC DHCP Server = ff:ff:ff:ff:ff:ff
Κατά την διαδικασία <i>Offer</i> :	MAC DHCP Server = 00:50:56:b5:aa:aa
Κατά την διαδικασία <i>Request</i> :	MAC DHCP Server = ff:ff:ff:ff:ff:ff
Κατά την διαδικασία <i>ACK</i> :	MAC DHCP Server = 00:50:56:b5:aa:aa

2.16)

Κατά την διαδικασία *Discover*:  
Source IP Address → 0.0.0.0  
Destination IP Address → 255.255.255.255  
Κατά την διαδικασία *Offer*:  
Source IP Address → 147.102.236.230  
Destination IP Address → 147.102.238.130

Κατά την διαδικασία *Request*:

Source IP Address → 0.0.0.0

Destination IP Address → 255.255.255.255

Κατά την διαδικασία *ACK*:

Source IP Address → 147.102.236.230

Destination IP Address → 147.102.238.130

2.17) Η τιμή 255.255.255.255 ως διεύθυνση IP προορισμού δηλώνει ότι το πακέτο θα πρέπει να σταλεί σε όλους τους εξυπηρετητές και όχι σε κάποιον συγκεκριμένο.

2.18) Το μήνυμα *DHCP Discover* περιέχει ως διεύθυνση IP αποστολέα 0.0.0.0, διότι ο υπολογιστής μου δεν έχει λάβει ακόμα κάποια διεύθυνση IP.

2.19) Ναι, ο υπολογιστής μου κάνει αίτηση στον εξυπηρετητή να του δώσει την διεύθυνση 147.102.238.130 στο πεδίο Option: Requested IP Address της επικεφαλίδας DHCP.

2.20) Η διεύθυνση που προτείνει ο εξυπηρετητής είναι η διεύθυνση που αιτήθηκε προηγουμένως (στο μήνυμα *DHCP Discover*) και μπορεί να αντληθεί από το μήνυμα *DHCP Offer* από το πεδίο Your (client) IP address.

2.21) Το μήνυμα *DHCP Offer* έχει διεύθυνση αποστολής IP την διεύθυνση την οποία θα δοθεί στον υπολογιστή μου, δηλαδή 147.102.238.130, και φυσική διεύθυνση την διεύθυνση MAC του υπολογιστή μου.

2.22) Η τιμή της σημαίας Broadcast flag είναι 0, και έτσι θα στείλει το μήνυμα *DHCP Offer* με μονοεκπομπή (unicast), πράγμα που συμβαίνει, καθώς από το προηγούμενο ερώτημα βλέπουμε ότι θέτει συγκεκριμένες διευθύνσεις IP και MAC ως διευθύνσεις προορισμού.

2.23) Η διεύθυνση του εξυπηρετητή DHCP είναι 147.102.236.230 και η τιμή αυτή μπορεί να αντληθεί από το πεδίο Option: DHCP Server Identifier.

2.24) Ο υπολογιστής μου αιτείται για την διεύθυνση IP 147.102.238.130, και η τιμή αυτή μπορεί να αντληθεί από το πεδίο Option: Requested IP Address.

2.25) Το προηγούμενο μήνυμα *DHCP Request* έχει διεύθυνση IP και MAC προορισμού 255.255.255.255 και ff:ff:ff:ff:ff:ff, αντιστοίχως.

2.26) Ο εξυπηρετητής μπορεί να αντιληφθεί ότι το μήνυμα *DHCP Request* απευθύνεται σε αυτόν κοιτώντας το πεδίο Option: DHCP Server Identifier, το οποίο θα περιέχει την διεύθυνση IP του.

2.27) Τελικά, η διεύθυνση που αποδίδεται στον υπολογιστή μου είναι η 147.102.238.130, για την οποία έγινε και η αίτηση στο μήνυμα *DHCP Request*, και η διεύθυνση αυτή μπορεί να αντληθεί από το πεδίο «Your (client) IP address».

2.28) Ναι, η διεύθυνση που δίνεται στον υπολογιστή μου είναι η ίδια με αυτήν του ερωτήματος 2.1.

2.29) Η μάσκα υποδικτύου είναι η 255.255.252.0, η τιμή της οποίας μπορεί να αντληθεί από το πεδίο Option: Subnet Mask.

2.30) Η διεύθυνση που δόθηκε στον υπολογιστή μου έχει διάρκεια δανεισμού 10 λεπτά (600 δευτερόλεπτα), η ανανέωση της οποίας πρέπει να συμβεί μέσα στα επόμενα 10 λεπτά από την στιγμή του δανεισμού της. Η τιμή αυτή μπορεί να αντληθεί από το πεδίο Option: IP Address Lease Time.

2.31) Ο κωδικός της επιλογής Parameter Request List είναι 55.

2.32) Τρεις παράμετροι που ζητάει ο υπολογιστής μου στο μήνυμα *DHCP Discover* είναι οι εξής:

- 1 – Subnet Mask – Η μάσκα υποδικτύου που θα έχει η υπολογιστής μου.
- 3 – Router – Οι διευθύνσεις των δρομολογητών
- 33 – Static Route – Ο πίνακας στατικής δρομολόγησης

2.33) Ο υπολογιστής μου ζήτησε συνολικά 14 παραμέτρους από τον εξυπηρετητή DHCP, από τον οποίο τελικά έλαβε 6, και μάλιστα μόνο 3 από όσες ζήτησε, και συγκεκριμένα τις εξής: Subnet Mask, Router, Domain Name Server. Οι επιπλέον παράμετροι που έστειλε ο εξυπηρετητής με το μήνυμα *DHCP Offer* είναι οι IP Address Lease Time, DHCP Message Type και DHCP Server Identifier.

2.34) Φίλτρο απεικόνισης: “dhcp or (arp and eth.src == 3c:6a:a7:9a:b3:cf)”

2.35) Ναι, ο υπολογιστής μου έστειλε πακέτα ARP αφού έλαβε το μήνυμα *DHCP ACK*.

2.36) Στάλθηκαν 11 πακέτα ARP από τον υπολογιστή μου.

2.37) Με τα πακέτα ARP αναζητείται αν υπάρχει κάποιος άλλος χρήστης στο δίκτυο που να έχει την διεύθυνση IP που έλαβε ο υπολογιστής μου, έτσι ώστε, αν άλλος χρήστης χρησιμοποιεί την διεύθυνση IP αυτή, ο υπολογιστής μου να μην αποδεχθεί εν τέλει την διεύθυνση αυτή.

2.38) Κατά την διαδικασία που έπεται από ένα μήνυμα *DHCP ACK* στέλνονται πακέτα ARP Probe με τιμή Opcode 1 (request) που σκοπό έχουν να ρωτήσουν τους υπόλοιπους χρήστες του δικτύου (γενικά τερματικούς χρήστες και εξυπηρετητές) αν χρησιμοποιούν την υποψήφια διεύθυνση IP. Αν κανένας χρήστης δεν απαντήσει στα πακέτα ARP request, τότε είναι σίγουρο ότι είναι ασφαλές ο υπολογιστής μου να υιοθετήσει την διεύθυνση IP που συμφώνησε με τον εξυπηρετητή DHCP. Αφού, λοιπόν, γίνει γνωστό ότι η υποψήφια διεύθυνση IP δεν χρησιμοποιείται από δεύτερο χρήστη/εξυπηρετητή, ο υπολογιστής μου στέλνει πακέτα ARP Announcement με στόχο να ανακοινώσει σε όλους τους κόμβους του δικτύου για την αντιστοίχιση της φυσικής διεύθυνσης με την IP που έχει ο υπολογιστής μου.

2.39) Παρήχθη μήνυμα *DHCP Request*, με το οποίο με τη σειρά του προκάλεσε τον εξυπηρετητή DHCP να στείλει μήνυμα *DHCP ACK*.

2.40) Όσων αφορά το πλαίσιο Ethernet, στην αρχική περίπτωση η τιμή του πεδίου Destination είναι ff:ff:ff:ff:ff:ff, ενώ στην δεύτερη είναι 00:50:56:b5:aa:aa.

Όσων αφορά το πακέτο IPv4, στην αρχική περίπτωση η τιμή του πεδίου Source Address είναι 0.0.0.0, ενώ στην δεύτερη είναι 147.102.238.130, και η τιμή του πεδίου Destination Address στην πρώτη περίπτωση είναι 255.255.255.255, ενώ στην δεύτερη είναι 147.102.236.230.

Κατά τ' άλλα όλες οι τιμές των πεδίων είναι ίδιες.

2.41) Όχι, δεν υπάρχει πεδίο στο οποίο να αναγράφεται οποιαδήποτε διεύθυνση του εξυπηρετητή DHCP στον οποίο θέλει να απευθυνθεί ο υπολογιστής μου. Ωστόσο, αυτό δεν είναι απαραίτητο, καθώς ξέρει σε ποιον εξυπηρετητή να απευθυνθεί, και έτσι μπορεί να συμπληρώσει το πεδίο Destination Address της επικεφαλίδας IPv4 με την διεύθυνσή του.

2.42) Η πληροφορία αυτή μπορεί να αντληθεί από το πεδίο της επικεφαλίδας DHCP Client IP address. Στο ερώτημα 2.24 είδαμε ότι η πληροφορία αυτή υπήρχε στο πεδίο Option: Requested IP Address, ενώ στο πεδίο Client IP Address υπήρχε η τιμή 0.0.0.0.

2.43) Στην επικεφαλίδα DHCP στο πεδίο Client IP Address. Είδαμε ότι στο ερώτημα 2.27 την πληροφορία αυτή την αντλούσαμε από το πεδίο Your (client) IP address, ενώ στο πεδίο Client IP Address υπήρχε η τιμή 0.0.0.0.

2.44) Στο μήνυμα *DHCP Release* η τιμή του πεδίου Transaction ID είναι 0x64091a47.

2.45) Στα μηνύματα που σχετίζονται με την εντολή εκχώρησης η τιμή του πεδίου Transaction ID είναι σε όλα 0xf804b44e.

2.46) Στα μηνύματα που σχετίζονται με την εντολή εκχώρησης η τιμή του πεδίου Transaction ID είναι σε όλα 0xdf1d7310.

2.47) Το πεδίο Transaction ID έχει σκοπό να κάνει δυνατή την διαφοροποίηση των διαδικασιών εύρεσης/εκχώρησης διευθύνσεων IP σε τερματικούς χρήστες. Κάθε φορά, λοιπόν, που ξεκινά μια διαδικασία ανάθεσης διεύθυνσης IP σε χρήστη, όλα τα μηνύματα DHCP σχετιζόμενα με αυτήν θα έχουν κοινή τιμή στο πεδίο τους Transaction ID.