

Όνοματεπώνυμο: Πυλιώτης Αθανάσιος		Ομάδα: 3
Όνομα PC/ΛΣ: DESKTOP-5DLG3IF		Ημερομηνία: 06/12/2022
Διεύθυνση IP: 147.102.216.3	Διεύθυνση MAC: 40:b0:34:70:96:da	

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 Αρχικά προσδιορίζει τον τρόπο που θέλουμε να επικοινωνήσουμε (TELNET), στη συνέχεια το πρωτόκολλο με το οποίο θέλουμε να συνδεθούμε και σε πιο domain (SMTP στο ntua.gr) και μέσω ποιας θύρας θέλουμε να συνδεθούμε (την 25), δηλαδή τη παλιά θύρα για SMTP. Ελέγχουμε αν μπορούμε να συνδεθούμε με τον τρόπο που ζητάμε και στη θύρα 25 αντί για 23 που είναι η προκαθορισμένη.

1.2 Ο κωδικός είναι ο 220 και η σημασία του είναι <domain> service ready, πρακτικά πως έγινε επιτυχώς η σύνδεση με την υπηρεσία.

1.3 smtp3.ntua.gr είναι το domain name.

1.4 smtp3.ntua.gr ESMTP Sendmail 8.15.2/8.15.2; Mon, 5 Dec 2022 11:21:50 +0200 (EET)

1.5 κωδικός του HELP: 214

1.6 16 διαφορετικές εντολές με 3 να είναι AUTH, DATA, VRFY

1.7 Όπως και στη προηγούμενη εργασία, αντί να έχει «214-» στην αρχή της γραμμής, έχει «214 », δηλαδή αντί για παύλα έχει κενό.

1.8 κωδικός του HELO: 250

1.9 όχι δεν εμφανίζεται, αλλά δείχνει «κάπως» τη διεύθυνση IPv6 του αντί για το όνομα.

250 smtp3.ntua.gr Hello [IPv6:20EHLO cn.ntua.gr"0f3:8297:29b4:a592], pleased to meet you

1.10 9 γραμμές.

1.11 Εντολές που μπορεί να χρησιμοποιήσει παραπάνω. Πιθανότατα ονόματα παραμέτρων enhance SMTP.

1.12 Από την επιβεβαίωση όταν συνδεθήκαμε στην υπηρεσία που για όνομα service γράφει ESMTP αλλά και στο EHLO 250-ENHANCEDSTATUSCODES

1.13 Mon, 5 Dec 2022 12:26:55 +0200 (EET)

1.14 DATA

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

Στέλνει τον κωδικό του DATA και πως να τελειώσει το μήνυμα.

1.15 Η τελεία σηματοδοτεί το τέλος του email που στέλνουμε.

1.16 **250** 2.0.0 2B5AQitMA031771 Message accepted for delivery

Ο κωδικός 250 δηλώνει message accepted.

1.17 Αυτός του κειμένου επικεφαλίδας From, networking@guru.org

1.18 Αυτός του κειμένου επικεφαλίδας To, networking@apprentice.org

1.19 Return-Path:

1.20 Received:

1.21 Message-Id:

1.22 X-Authentication-Warning:, Received:

1.23 Τα ονόματα των MTA είναι diomedes.noc.ntua.gr, f1.mail.ntua.gr, m2.mail.ntua.gr

1.24 LMTPA, SMTP, ESMTP

1.25 Date: Mon, 5 Dec 2022 12:26:55 +0200 (EET) Είναι η ώρα που συνδέθηκα στην υπηρεσία SMTP και όχι η ώρα που στάλθηκε το email, από εκεί πήρε το Date:

1.26 Capture filter: host 147.102.222.220

1.27 Display filter: smtp

1.28 Το πρωτόκολλο TCP

1.29 Transmission Control Protocol, Src Port: 25, Dst Port: 54430

1.30 Η θύρα νούμερο 25, την οποία διευκρινίζουμε και όταν συνδεόμαστε στην υπηρεσία.

1.31 [5 Reassembled TCP Segments (6 bytes): #6(1), #8(1), #10(1), #12(1), #14(2)], άρα 5 reassembled τεμάχια

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

Κωδικός το 221 και απόκριση 2.0.0 diomedes.noc.ntua.gr closing connection, service closing transmission channel

1.33 όχι, καθώς περιμένει για επιβεβαίωση από τον εξυπηρετητή για την εντολή. Πρέπει να σταλούν τα τελευταία πακέτα TCP για την επιβεβαίωση της απόλυσης σύνδεσης από τον SMTP server.

2

2.1 Physical Address. : 40-B0-34-70-96-DA

IPv4 Address. : 147.102.216.3

Subnet Mask : 255.255.255.0

DHCP Server : 147.102.216.252

2.2 Display filter: dhcp

2.3 DHCP Release, DHCP Discover, DHCP Offer, DHCP Request, DHCP ACK

2.4 UDP

2.5 User Datagram Protocol, Src Port: 68, Dst Port: 67

User Datagram Protocol, Src Port: 67, Dst Port: 68

2.6 67 (server) και 68 (client)

2.7 Dynamic Host Configuration Protocol (Release)

Message type: Boot Request (1)

Hardware type: Ethernet (0x01)

Hardware address length: 6

Hops: 0

Transaction ID: 0x371e3dba

Length: 4

DHCP Server Identifier: 147.102.216.252

Option: (61) Client identifier

Length: 7

Hardware type: Ethernet (0x01)

Client MAC address: 40:b0:34:70:96:da

Server ανήκει στο default gateway που συμπίπτει με το DHCP Server και client στο ethernet μου, δηλαδή στον υπολογιστή μου.

2.15 Request: Ethernet II, Src: 40:b0:34:70:96:da, Dst: ff:ff:ff:ff:ff:ff

ACK: Ethernet II, Src: 00:50:56:b5:aa:aa, Dst: ff:ff:ff:ff:ff:ff

Discover: Ethernet II, Src: 40:b0:34:70:96:da, Dst: ff:ff:ff:ff:ff:ff

Offer: Ethernet II, Src: 00:50:56:b5:aa:aa, Dst: 40:b0:34:70:96:da

2.16 Request: Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255

ACK: Internet Protocol Version 4, Src: 147.102.216.252, Dst: 255.255.255.255

Discover: Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255

Offer: Internet Protocol Version 4, Src: 147.102.216.252, Dst: 147.102.216.3

2.17 255.255.255.255 is the broadcast IP Address στο τοπικό δίκτυο.

2.18 η 0.0.0.0 είναι unspecified και θα δοθεί από το offer και το request μετά. Εμείς κάνουμε στα option requested ip address αυτή που θέλουμε.

2.19 ναι, Requested IP Address: 147.102.216.3

2.20 προτείνει στο Your (client) IP address: 147.102.216.3

2.21 Destination Address: 147.102.216.3, Destination: 40:b0:34:70:96:da, άρα στις δικές μου διευθύνσεις IPv4 and MAC

2.22 0... = Broadcast flag: Unicast, για αυτό και δεν έγινε broadcast, επειδή δεν δέχεται broadcast και δέχεται μόνο unicast. Όλα είναι unicast τα πακέτα. Κανονικά θα έπρεπε να είναι 1, broadcast, όπως γνωρίζουμε από τη θεωρία και να απαντάνε με broadcast (σε άλλη καταγραφή έγινε κάθε φορά broadcast και είχαν flag 1 αντίστοιχα)

2.23 Option: (54) DHCP Server Identifier (147.102.216.252), άρα στο 54 DHCP Server Identifier.

2.24 Option: (50) Requested IP Address (147.102.216.3), άρα στο 50

2.25 broadcast address (ff:ff:ff:ff:ff:ff, 255.255.255.255)

2.26 το γνωρίζει από το DHCP Server Identifier

2.27 Your (client) IP address: 147.102.216.3 αυτή που ζήτησε όντως στο Your (client) IP address.

2.28 Ναι συμπίπτει

2.29 Option: (1) **Subnet Mask** (255.255.255.0) 255.255.255.0 στο Subnet Mask

2.30 Option: (51) IP Address Lease Time,

IP Address Lease Time: (600s) 10 minutes

Διαρκεί 10 λεπτά και βρίσκεται στο IP Address Lease Time

2.31 Code: 55

2.32 Option: (55) Parameter Request List

Length: 14

Parameter Request List Item: (1) Subnet Mask

Η subnet mask που πρέπει να χρησιμοποιηθεί στο interface που ζητάει IP Address

Parameter Request List Item: (3) Router

Default router ή gateway τελευταίας επιλογής που θα χρησιμοποιηθεί για το interface

Parameter Request List Item: (15) Domain Name

Διευκρινίζει το domain name που ο πελάτης θα πρέπει να χρησιμοποιηθεί σαν suffix όταν κάνει resolving hostnames μέσω του DNS

2.33 ζητάει 14 παραμέτρους και παίρνει 4 πίσω (1, 3, 6 και 255 οι αντίστοιχοι κωδικοί)

2.34 Display Filter: dhcp or arp.src.hw_mac == 40:b0:34:70:96:da

2.35 ναι

2.36 4, τα 3 πρώτα είναι ARP Probe και το τελευταίο ARP Announcement for 169.254.86.117

2.37 Ναι.

2.38 Αναζητούμε τη διεύθυνση 169.254.86.117 μέχρι που ανακοινώνεται. Στέλνονται για να εξακριβώσει πως δεν χρησιμοποιείται από κάποιον άλλο υπολογιστή αυτή η διεύθυνση. Η ανακοίνωση γίνεται για να γνωρίζει το δίκτυο την ύπαρξη της και πως μπορεί να χρησιμοποιηθεί.

2.39 Request, ACK (με κατάλληλο έλεγχο του χρόνου βρήκαμε ποια στάλθηκαν νωρίτερα ή αργότερα).

2.40 Ναι, δεν έχει broadcast στο destination MAC and IPv4, αλλά είναι:

Ethernet II, Src: 40:b0:34:70:96:da, Dst: 00:50:56:b5:aa:aa

Internet Protocol Version 4, Src: 147.102.216.3, Dst: 147.102.216.252

Και δεν έχει τη διεύθυνση 169.254.86.117 σαν πηγή του IPv4.

2.41 Ναι υπάρχει. Η DHCP υπάρχει στο Destination Address του IPv4

2.42 Ναι υπάρχει διαφορά, είναι στο Client IP Address τώρα αντί για τα options στο τέλος.

2.43 Your (client) IP address: 147.102.216.3 και όχι, δεν υπάρχει διαφορά σε αυτό.

2.44 Release: Transaction ID: 0x371e3dba

2.45 1st Renew: Transaction ID: 0x67949d13

2.46 2nd Renew: Transaction ID: 0x95445163

2.47 Σκοπός είναι η ταυτοποίηση των πακέτων. Βοηθάει τον εξυπηρετητή και τον πελάτη να γνωρίζουν πως έχουν τον ίδιο σκοπό και κάνουν τη σύνδεση που χρειάζεται οντως. Παρατηρούμε παραπάνω πως αλλάζει κάθε φορά, αλλά το Transaction ID μεταξύ του πρώτου Renew και του αντίστοιχου ACK που επιστρέφεται θα είναι ίδιο επειδή θέλουν το ίδιο πράγμα και διευκολύνει στην επιβεβαίωση.

7277	95.769184	169.254.86.117	255.255.255.255	DHCP	370	DHCP Request - Transaction ID 0x67949d13
7278	95.769360	169.254.86.117	255.255.255.255	DHCP	370	DHCP Request - Transaction ID 0x67949d13
7279	95.771084	147.102.216.252	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0x67949d13
7280	95.771401	147.102.216.252	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0x67949d13
15556	113.706...	147.102.216.126	255.255.255.255	DHCP	342	DHCP Inform - Transaction ID 0x156b2036
16829	117.782...	147.102.216.3	147.102.216.252	DHCP	358	DHCP Request - Transaction ID 0x95445163
16830	117.782...	147.102.216.252	147.102.216.3	DHCP	342	DHCP ACK - Transaction ID 0x95445163