Ονοματεπώνυμο: Ζευγολατάκος Παναγιώτης		Ομάδα: 3
Όνομα PC/ΛΣ: panos-PC / Windows 10		Ημερομηνία: 7/11/2020
Διεύθυνση IP: 192.168.2.11	Διεύθυνση MAC: D0-50-99-75-F8-F8	

Εργαστηριακή Άσκηση 6
Πρωτόκολλο ICMP

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 ether host d0:50:99:75:f8:f8

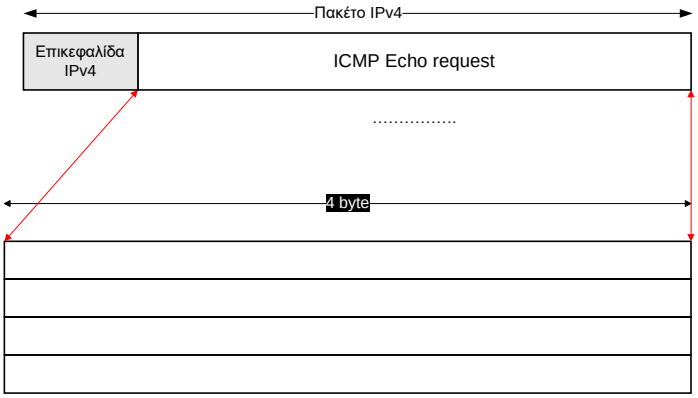
1.2 arp or icmp

1.3 Ένα ζευγάρι πακέτων πρωτοκόλλου ARP ανταλλάσσεται στο τοπικό δίκτυο (LAN) προκειμένου να βρεθεί η MAC Address μιας ζητούμενης διεύθυνσης IPv4. Χρησιμοποιείται έτσι ώστε να αποθηκευτεί στην cache η ζητούμενη διεύθυνση και να συνεχιστεί η επικοινωνία στο μέλλον.

1.4 Protocol: ICMP (1)

1.5 8 Bytes

1.6 Type, Code, Checksum, Identifier, Sequence Number



(Για κάποιο λόγο δεν μπορώ να γράψω στο παραπάνω σχήμα, οπότε το αντιγράφω από κάτω)

Type	Code	Checksum
Identifier		Sequence Number

1.7 Type: 8 (Echo (ping) request)

Code: 0

1.8

Identifier (BE): 1 (0x0001)

Identifier (LE): 256 (0x0100)

Sequence Number (BE): 1 (0x0001)

Sequence Number (LE): 256 (0x0100)

1.9 Το μήκος είναι 32 Bytes και το περιεχόμενο είναι το παρακάτω:

Data: 6162636465666768696a6b6c6d6e6f707172737475767761626364656667686 9

1.10 Το μήκος είναι 8 Bytes και έχει την ίδια δομή με αυτή του Echo request.

1.11 Type: 0 (Echo (ping) reply)

Code: 0

1.12 Το πεδίο Type.

1.13

Identifier (BE): 1 (0x0001)

Identifier (LE): 256 (0x0100)

Sequence Number (BE): 1 (0x0001)

Sequence Number (LE): 256 (0x0100)

1.14 Είναι οι ίδιες

1.15 Τα πεδία ταυτότητας και αύξοντα αριθμού χρησιμοποιούνται για να μπορεί να αναγνωριστεί το ζεύγος request-reply, αφού παραμένουν ίδια.

1.16 Το μήκος είναι 32 Bytes και το περιεχόμενο είναι το παρακάτω:

Data: 61626364656667686 96a6b6c6d6e6f707172737475767761626364656667686 9

(ίδια συμβολοσειρά με το 1.9)

1.17 Όχι, είναι το ίδιο.

1.18 Η γραμμή **Reply from 192.168.2.1: bytes=32 time<1ms TTL=64** στο παράθυρο εντολών αντιστοιχεί σε ένα μήνυμα ICMP Echo reply στο Wireshark.

Στις γραμμές:

Ping statistics for 192.168.2.1:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Βλέπουμε τον αριθμό των μηνυμάτων ICMP που στάλθηκαν και λήφθηκαν (φαίνονται και στο Wireshark).

1.19 Στάλθηκαν 12 πακέτα ARP request.

1.20 Στέλνονται περίπου κάθε ένα δευτερόλεπτο.

1.21 Κανένα.

1.22 Στο παράθυρο εντολών παίρνουμε τη γραμμή:

Reply from 192.168.2.11: Destination host unreachable.

Η οποία υποδεικνύει πως στάλθηκαν πακέτα ARP προκειμένου να βρεθεί η διεύθυνση MAC που αντιστοιχεί στην διεύθυνση IPv4 που δώσαμε. Εφόσον δε βρέθηκε, δεν ανταλλάχθηκαν και μηνύματα ICMP.

2

2.1 Internet Address Physical Address Type

192.168.2.1 e0-19-54-25-47-58 dynamic

192.168.2.255 ff-ff-ff-ff-ff-ff static

224.0.0.22 01-00-5e-00-00-16 static

224.0.0.251 01-00-5e-00-00-fb static

224.0.0.252 01-00-5e-00-00-fc static

239.255.255.250 01-00-5e-7f-ff-fa static

255.255.255.255 ff-ff-ff-ff-ff-ff static

2.2 Αποστολέας: d0:50:99:75:f8:f8,

Παραλήπτης: e0:19:54:25:47:58

2.3 Src: 192.168.2.11, Dst: 147.102.1.1

2.4 Η διεύθυνση MAC του αποστολέα αντιστοιχεί στη διεύθυνση IPv4 του υπολογιστή μου και η διεύθυνση MAC του παραλήπτη αντιστοιχεί στη διεύθυνση IPv4 στο router μου.

2.5 Ναι.

2.6 Ο σκοπός τους ήταν η ενημέρωση του router για τη διεύθυνση MAC που αντιστοιχεί στη διεύθυνση IP του υπολογιστή μου.

2.7 icmp.type == 0

2.8 Παρατηρούμε πως ο αποστολέας είναι η διεύθυνση που κάναμε ping και ο παραλήπτης είναι η τοπική διεύθυνση IPv4, επομένως καταλαβαίνουμε πως το μήνυμα διέσχισε ένα μονοπάτι για να φτάσει στον προορισμό του, συνεπώς το TTL έχει μειωθεί τόσο όσο ο αριθμός των ενδιάμεσων κόμβων (γεγονός που μπορούμε να επαληθεύσουμε αν χρησιμοποιήσουμε την εντολή **tracert 147.102.1.1**).

2.9 ICMP Echo Requests.

2.10 Δεν υπάρχουν πακέτα ARP, εφόσον η διεύθυνση βρίσκεται εκτός του τοπικού δικτύου και είναι ανήκει σε ανενεργό υπολογιστή, επομένως υπάρχουν μόνο πακέτα ICMP Echo request (δεν λαμβάνουμε replies).

3

3.1 64 Bytes

3.2 Είναι το διπλάσιο.

3.3 Παρατηρούμε το μήνυμα λάθους: Time to live exceeded in transit.

3.4 Type: 8 (Echo (ping) request)

Code: 0

3.5 Checksum (2 Bytes), Identifier (2 Bytes), Sequence (2 Bytes).

Παρατηρούμε πως υπάρχει και ένα πεδίο Unused μεγέθους 4 Bytes και αφού λάβουμε το πρώτο μήνυμα "Destination Unreachable", έχουμε το πεδίο Unused μεγέθους (σύνολο) 3 Bytes (1+2), ενώ παρευρίσκεται και ένα πεδίο Length μεγέθους 1 Bytes, έναντι των πεδίων Identifier και Sequence Number.

3.6 Το πακέτο που διάλεξα έχει συνολικό μέγεθος 70 Bytes, αλλά το μέγεθος των δεδομένων είναι 28 Bytes.

3.7 Το περιεχόμενο του πεδίου δεδομένων είναι η επικεφαλίδα IPv4 που προκάλεσε το μήνυμα (28 Bytes) και τα πρώτα 8 Bytes του δεδομενογράμματος του πακέτου αυτού δηλαδή την επικεφαλίδα ICMP.

4

4.1 Από τα συνήθη μεγέθη MTU, αφαίρεσα 20 και 8 Bytes, για τις επικεφαλίδες IPv4 και ICMP αντίστοιχα. Επομένως έκανα ping για τα μεγέθη: 1472, 1464, 978 και 548, όπου έλαβα και απάντηση.

4.2 Ναι.

4.3 Η πηγή του είναι η διεύθυνση 192.168.2.1, δηλαδή το router μου.

4.4 Type: 3 (Destination unreachable)

Code: 4 (Fragmentation needed)

4.5 Το πεδίο Code δηλώνει ότι το λάθος οφείλεται στην απαίτηση μη θρυμματισμού με την τιμή 4 και η τιμή του MTU of next hop είναι 1492.

4.6 Το πεδίο των δεδομένων περιέχει τις επικεφαλίδες IPv4 και ICMP του αρχικού μηνύματος και δεδομένα μήκους 520 Bytes.

4.7 Η MTU είναι 1492 (δηλαδή ping 1464).

4.8 Δεν απαντάει και για MTU ίση με 1006 (δηλαδή ping 978).

4.9 Η τιμή 576 (δηλαδή ping 548).

4.10 Αυτή η MTU είναι σίγουρα μικρότερη ή ίση της ελάχιστης MTU κάποιου κόμβου της διαδρομής, διότι λαμβάνουμε reply, επομένως γνωρίζουμε πως το μήνυμα κατάφερε και έφτασε στον προορισμό του.

4.11 Προκειμένου να παραχθεί ICMP Destination Unreachable πρέπει η διεπαφή να λάβει το μήνυμα, το οποίο δε συμβαίνει, εφόσον το μέγεθος του πακέτου ξεπερνάει την MTU κάπου στην πορεία.

4.12 Δεν παρατηρώ θραύσματα. Βλέπω μόνο το τελικό πακέτο.

.....

5

5.1 host 147.102.40.15

5.2 nslookup edu-dy.cn.ntua.gr 147.102.40.15

5.3 Έλαβα το μήνυμα:

DNS request timed out.

timeout was 2 seconds.

Επομένως δεν έλαβα απάντηση στο αίτημα DNS.

5.4 Ναι, 5 μηνύματα.

5.5 Είναι UDP Datagram και η θύρα προορισμού τους είναι η θύρα 53.

5.6 Ναι.

5.7 Type: 3 (Destination unreachable)

Code: 3 (Port unreachable)

5.8 Το πεδίο Code.

5.9 Το μήνυμα λάθους περιέχει τα δεδομένα που περιέχουν το 53 ως Destination Port του αρχικού μηνύματος.

5.10 Χρησιμοποιώ Windows.

6

6.1 ping 2001:648:2000:329::101, tracert 2001:648:2000:329::101

6.2 Φίλτρο σύλληψης: ip6

Φίλτρο απεικόνισης: icmpv6

6.3 Έχει την τιμή: 0x86dd

6.4 40 Bytes.

6.5 Version (4 bits), Traffic Class (8 bits), Flow Label (20 bits), Payload Length (16 bits), Next Header (8 bits), Hop Limit (8 bits), Source IPv6 Address (128 bits), Destination IPv6 Address (128 bits).

6.6 Η επικεφαλίδα Hop Limit.

6.7 Η επικεφαλίδα Next Header και για το ICMPv6 έχει την τιμή 58.

6.8 Ναι.

6.9 Type: Echo (ping) request (128)

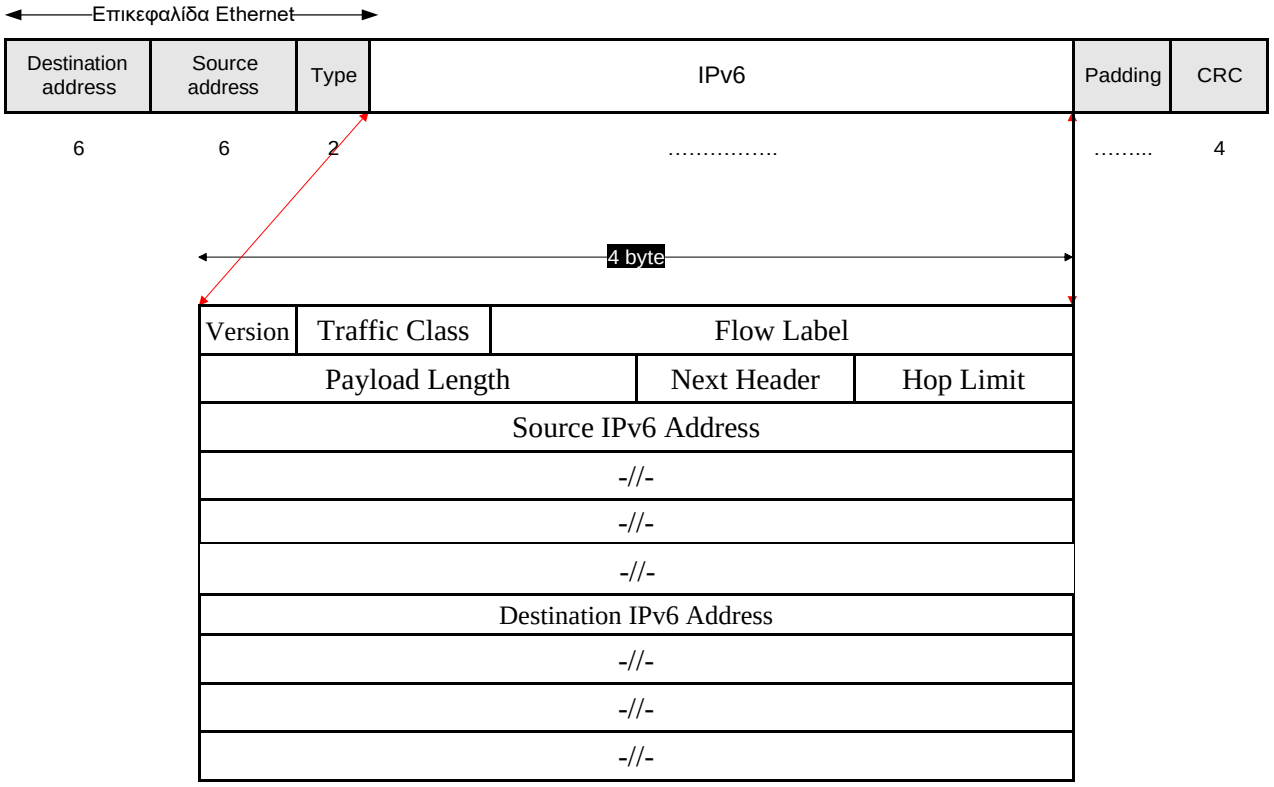
Data (32 bytes)

6.10 Ναι.

6.11 Type: Echo (ping) reply (129)

Data (32 bytes)

.....



6.12 Η διαφορά είναι πως τα δεδομένα είναι 64 bytes μόνο μηδενικά.

6.13 Ναι.

6.14 Το Type έχει την τιμή 3 και μεταφέρει δεδομένα μήκους 112 Bytes.

6.15 Περιέχει το IPv6 Header της πηγής (40 Bytes) και το ICMPv6 μήνυμά του (72 Bytes).