

Όνοματεπώνυμο: Ναυσικά Αμπατζή		Ομάδα: 2
Όνομα PC/ΛΣ: Dell XPS 15-7590 Windows		Ημερομηνία: 10 /11 /2020
Διεύθυνση IP: 192.168.1.9	Διεύθυνση MAC:24-41-8C-65-26-BF	

Μέρος 1

1.1 Φίλτρο : ether host 24-41-8C-65-26-BF

1.2 Φίλτρο απεικόνισης : arp or icmp

1.3 Δεν καταγράφηκαν πακέτα ARP, διότι η default gateway υπήρχε στον ARP πίνακα.

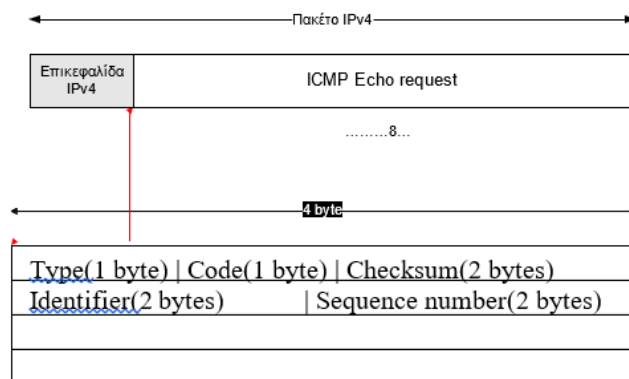
1.4 Το πεδίο Protocol και έχει τιμή 1.

1.5 Το μήκος της επικεφαλίδας μηνυμάτων(Header Length) ICMP Echo Request είναι 8 bytes.

1.6 Επικεφαλίδα του μηνύματος ICMP Echo Request:

- Type : 1byte
- Code : 1 byte
- Checksum : 2 byte
- Identifier : 2 byte
- Sequence number : 2 byte

Ακολουθεί το σχήμα:



1.7 Type : 8

Code: 0

1.8 Identifier (BE):1

Identifier (LE) : 256

Sequence number(BE): 540

Sequence number(LE):7170

1.9 Το μήκος του πεδίου δεδομένων (Data) είναι 32bytes και το περιεχόμενό του 6162636465666768696a6b6c6d6e6f70717273747576776162636465666766869.

1.10 Το μήκος της επικεφαλίδας ενός μηνύματος Echo Reply είναι 8 bytes, ίδιο δηλαδή με αυτό ενός μηνύματος Echo Request και η δομή του είναι επίσης η ίδια.

1.11 Type:0

Code:0

1.12 Το είδος του μηνύματος το καθορίζει το πεδίο Type.Η τιμή 8 αντιστοιχεί σε Request και η τιμή 0 σε Reply.

Type: 8 (Echo (ping) request)

Type: 0 (Echo (ping) reply)

1.13 Identifier (BE):1

Identifier (LE) : 256

Sequence number(BE): 540

Sequence number(LE):7170

1.14 Οι τιμές Identifier και Αύξοντα αριθμού είναι οι ίδιες για το Request και το Reply:

Identifier (BE):1

Identifier (LE) : 256

Sequence number(BE): 541

Sequence number(LE):7476

1.15 Τα δύο αυτά πεδία χρησιμοποιούνται ώστε να συσχετίζουν κάθε αίτηση με την αντίστοιχη απάντησή της.

1.16 Το μήκος και ποιο το περιεχόμενο του πεδίου δεδομένων(Data) των μηνυμάτων ICMP *Echo reply* είναι: 32 byte και 6162636465666768696a6b6c6d6e6f70717273747576776162636465666766869

1.17 Το περιεχόμενο του περιεχομένου είναι το ίδιο και στο Request Και στο Reply.

1.18 Το πεδίο cmd αναφέρει τον προορισμό των μηνυμάτων(192.168.1.1) και περιέχει επίσης και τον αριθμό των requests και replies.

1.19 Για την επίλυση της διεύθυνσης του μη ενεργού υπολογιστή στάλθηκαν 12 ARP request μηνύματα.

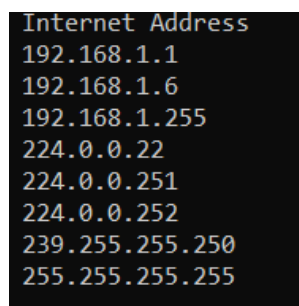
1.20 Στέλνονται περίπου κάθε 1 sec

1.21 Δεν στάλθηκαν πακέτα icmp.

1.22 Μία εγγραφή στο παράθυρο εντολών δημιουργεί 3 ερωτήσεις στο wireshark.

Μέρος 2

2.1 Οι διευθύνσεις του πίνακα arp μετά την καταγραφή είναι οι εξής:



Internet Address
192.168.1.1
192.168.1.6
192.168.1.255
224.0.0.22
224.0.0.251
224.0.0.252
239.255.255.250
255.255.255.255

2.2 Διεύθυνση MAC αποστολέα: 24:41:8c:65:26:bf

Διεύθυνση MAC παραλήπτη: ec:f0:fe:e3:87:7a

2.3 IPV4 αποστελέα : 192.168.1.5

IPV4 παραλήπτη : 147.102.1.1

2.4 Οι παραπάνω MAC διευθύνσεις αντιστοιχούν στις IPV4 διευθύνσεις του παραπάνω ερωτήματος(2.3).

2.5 Όχι δεν παρατήρησα πακέτα ARP κατά την καταγραφή.

2.6 Αυτό συμβαίνει διότι η διεύθυνση IPV4 147.102.1.1 που έκανα ping είναι διεύθυνση υπολογιστή που δεν βρίσκεται στο τοπικό μου δίκτυο, αλλά είναι ενεργή. Για να μπορέσω να την φτάσω θα πρέπει να χρησιμοποιήσω την default gateway. Εάν αυτό βρίσκεται ήδη στον πίνακα arp δεν πρόκειται να δούμε τέτοια πακέτα.

2.7 Φίλτρο απεικόνισης: icmp.type==0

2.8 Το TTL είναι 57. Στην επικεφαλίδα στο wireshark αυτό μπορούμε να το βρούμε από το πεδίο time to live.

2.9 Εμφανίζονται μόνο τα request ICMP μηνύματα.

2.10 Το Ping σε ανενεργή διεύθυνση σε υπολογιστή εκτός του τοπικού μου υποδικτύου παρατηρώ ότι δίνει μόνο icmp μηνύματα(όχι arp), σε αντίθεση με ανενεργή διεύθυνση

εντός του τοπικού μου υποδικτύου. Αυτό συμβαίνει διότι η πρόσβαση στη διεύθυνση εκτός του τοπικού μου δικτύου θα γίνει μέσω δρομολογητή, ο οποίος υπάρχει ήδη στον πίνακα arp.

Μέρος 3

3.1 Το μήκος του πεδίου δεδομένων των μηνυμάτων ICMP Echo Request είναι 64 bytes και το περιεχόμενο του 000...00.

3.2 Το μήκος στο αντίστοιχο ερώτημα 1.9 είναι το μισό (32 Bytes).

3.3 Παρατηρώ το μήνυμα λάθους Time to live exceeded in transit.

3.4 Type: 11

Code: 0

3.5 Πριν το πεδίο δεδομένων (Data) υπάρχουν στην επικεφαλίδα τα πεδία : Type (1 byte), Code(1 byte), Checksum(2 bytes), Unused(1 byte)

3.6 20 bytes header + 68 bytes Length of original datagram = 88 bytes

3.7 Το περιεχόμενο Data του μηνύματος αυτού είναι η επικεφαλίδα του διαδικτύου συν τα 8 αρχικά bytes από τα Data του μηνύματος Request που επιστρέφονται στον αποστολέα. Χρησιμοποιούνται από τον host ώστε να αντιστοιχεί το μήνυμα στην κατάλληλη διεργασία. Σε περίπτωση που ένα πρωτόκολλο υψηλότερου επιπέδου χρησιμοποιεί port numbers, τα δεδομένα αυτά θεωρείται ότι είναι τα πρώτα 64 Bytes του αρχικού μηνύματος.

Μέρος 4

4.1 Τιμές μήκους : 1472, 1464, 978,548

4.2 Ναι παρατηρώ το μήνυμα αυτό και στο wireshark.

4.3 Το παρήγαγε ο κόμβος 192.168.1.1 (default gateway).

4.4 Type: 3, Code:4

4.5 Το πεδίο Code οφείλεται στην απαίτηση μη θρυμματισμού πακέτου και η επικεφαλίδα Next – Hop MTU έχει τιμή 1492.

4.6 Το πεδίο δεδομένων(Data) περιέχει επικεφαλίδες IPV4 και ICMP και τα πρώτα 520 bytes των δεδομένων του πακέτου που στάλθηκε από τον υπολογιστή μου.

4.7 MTU = 1492 bytes

4.8 Το 147.102.40.15 δεν απαντά επίσης για τιμές MTU 1006 bytes.

4.9 Έλαβα απάντηση από το 147.102.40.15 για τιμή MTU 576 bytes.

4.10 Είναι η MTU της διεπαφής του προορισμού.

4.11 Το 147.102.40.15 δεν παράγει μήνυμα λάθους καθώς είναι ο τελικός κόμβος. Τέτοια μηνύματα παράγουν μόνο οι δρομολογητές όταν δεν μπορούν να προωθήσουν σε επόμενο κόμβο κάποιο μήνυμα, όχι όμως οι τελικοί κόμβοι.

4.12 Το μήκος βγαίνει ίσο με: 572 bytes

Total Length: 572

Ωστόσο το μήκος που περιμέναμε είναι 576 bytes, δηλαδή όσο και το μήκος της MTU του παραλήπτη. Αυτό συμβαίνει διότι το μήκος του fragment offset πρέπει να είναι πολλαπλάσιο του 8 πάντα. Έτσι με μήκος 572 έχουμε:

Fragment offset = (Total Length – Header Length) = (572-20) = 552 bytes και fragment offset/8 = 552/8 = 69

Για μήκος 576 bytes : Fragment offset = 576 – 20 = 556 bytes και fragment offset/8 = 556/8 = 69.5(αδύνατο).

Μέρος 5

5.1 Φίλτρο σύλληψης : host 147.102.40.15

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

5.3 Απάντηση από το παράθυρο εντολών:

5.4 Ναι υπάρχουν 3 μηνύματα DNS στην καταγραφή.

5.5 Το πρωτόκολλο μεταφοράς τους είναι το UDP και η θύρα προορισμού τους, η port 53.

5.6 Ναι υπάρχουν 3 τέτοια μηνύματα.

5.7 Type:3

Code:3

5.8 Το πεδίο Code.

Code: 3 (Port unreachable)

5.9 Η τιμή 3 στο code το καθορίζει.

5.10 – (Windows)

Μέρος 6

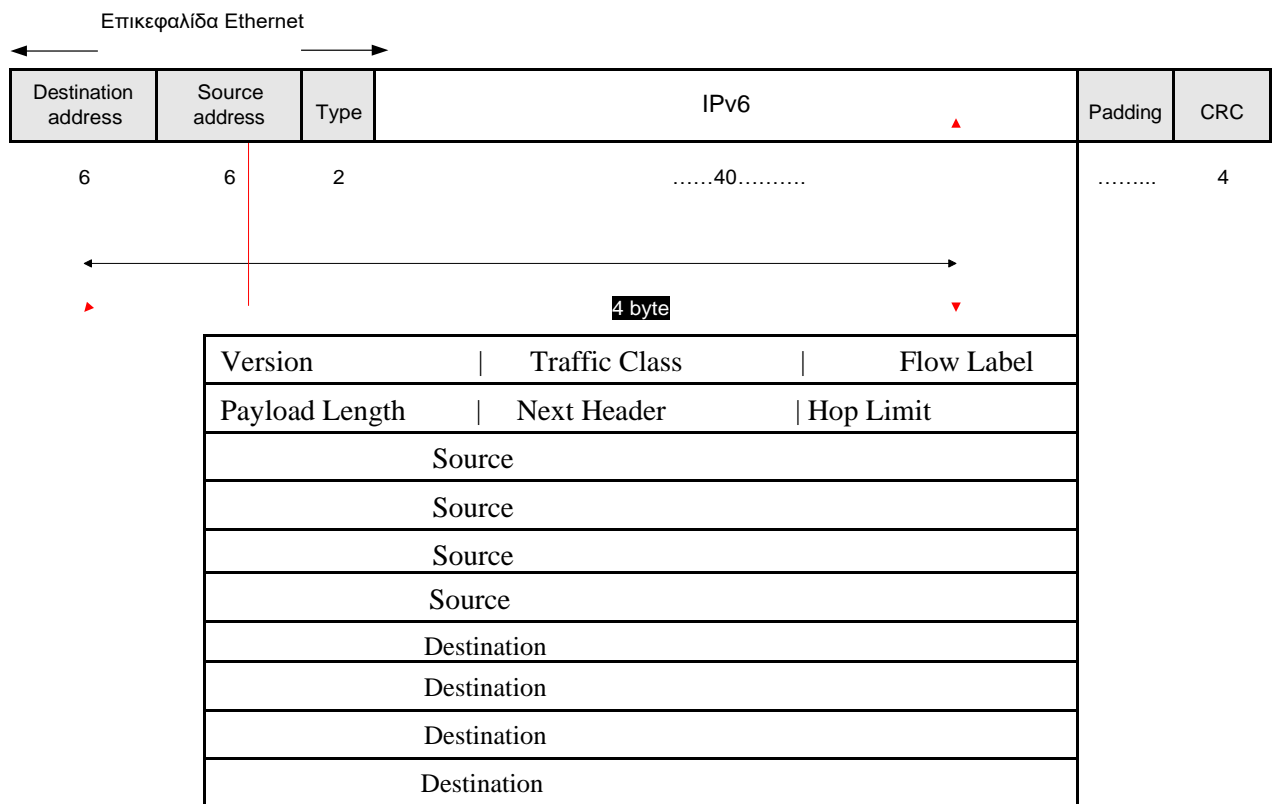
6.1 tracert -6 2001:648:2000:329::101, ping -6 2001:648:2000:329::101

6.2 Φίλτρο σύλληψης: ip6, φίλτρο απεικόνισης: icmpv6

6.3 Type: 0x86dd

6.4 40 bytes

6.5 Version(1 byte), Traffic Class (2 byte), Flow Label(2 byte), Payload Length(2 byte), Next Header(1 byte), Hop Limit(1 byte), Source(16 byte), Destination(16 byte)



6.6 Η επικεφαλίδα Hop Limit.

6.7 Το Next Header (58).

6.8 Η δομή της επικεφαλίδας είναι η ίδια με αυτή του ερωτήματος 1.6.

6.9 Type: 128 και το μήκος των δεδομένων που μεταφέρει δεδομένα μήκους 32 Byte.

6.10 Ναι η δομή είναι η ίδια.

6.11 Type: 129 και το μήκος των δεδομένων που μεταφέρει είναι 32 bytes.

6.12 Το πεδίο δεδομένων στο tracerp έχει μήκος 64 Bytes, σε αντίθεση με του ping που έχει μήκος 32 bytes.

6.13 Εδώ αντί για unused πεδίο, υπάρχει το Reserved(μήκους 4 byte)

6.14 Type = 3 και μήκος δεδομένων = 64Bytes

6.15 Το πεδίο των δεδομένων είναι 0.