Ονοματεπώνυμο: Χρήστος Τσούφης			**Ομάδα:** 2
Όνομα PC/ΛΣ: DESKTOP-EUMLCMA/Windows 10		**Ημερομηνία:**	10/11/2020
Διεύθυνση IP:	192.168.1.3	**Διεύθυνση MAC:**	34-F6-4B-07-39-B5

Εργαστηριακή Άσκηση 6
Πρωτόκολλο ICMP

1

1.1 Η σύνταξη του φίλτρου σύλληψης: `ether host 34-F6-4B-07-39-B5`.

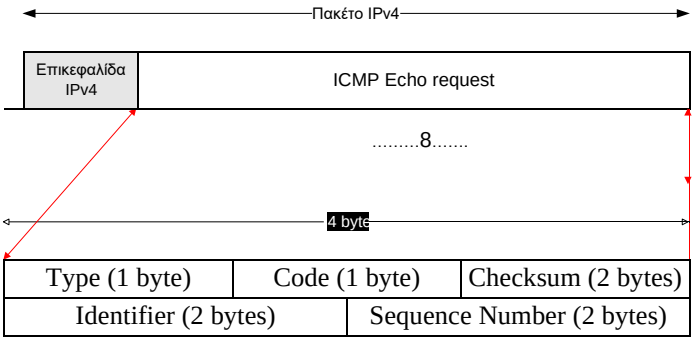
1.2 Η σύνταξη του φίλτρου απεικόνισης: `arp or icmp`.

1.3 Δεν παρατηρήθηκε κάποια καταγραφή για τα πακέτα ARP που ανταλλάχθηκαν διότι είχε γίνει αντιστοίχιση των IP του υποδικτύου με την MAC του και περιλάμβανε την Default Gateway και επομένως, υπήρχαν ήδη στον πίνακα ARP.

1.4 Για το πρώτο μήνυμα Echo Request, το όνομα και η τιμή του πεδίου της επικεφαλίδας IPv4 είναι: Protocol: ICMP (1) (δηλ. με τιμή 0x01).

1.5 Το μήκος της επικεφαλίδας των μηνυμάτων ICMP Echo Request είναι: 8 bytes.

1.6 Τα ονόματα και το μήκος σε byte των πεδίων της επικεφαλίδας του μηνύματος ICMP Echo Request είναι:



1.7 Για την επικεφαλίδα των ICMP Echo Request παρατηρείται: Type: 8 (Echo (ping) Request), Code: 0.

1.8 Για την επικεφαλίδα των ICMP Echo Request παρατηρείται:

Identifier: (BE) (0x0001), (LE) (0x0100)

Sequence number: (BE) (0x013e), (LE) (0x3e01)

1.9 Το ICMP Echo Request που παράγει η εντολή ping είναι έχει μήκος δεδομένων 32 bytes, και είναι, μεταξύ άλλων, μια ακολουθία των γραμμάτων του αγγλικού αλφαβήτου.

1.10 Το ICMP Echo Reply έχει μήκος επικεφαλίδας 8 bytes και η δομή δεν διαφέρει από το ICMP Echo Request.

1.11 Για την επικεφαλίδα των ICMP Echo Reply παρατηρείται: Type: 0 (Echo (ping) Reply), Code: 0.

1.12 Το πεδίο Type καθορίζει το είδος του μηνύματος ICMP.

1.13 Για την επικεφαλίδα των ICMP Echo Request παρατηρείται:

Identifier: (BE) (0x0001), (LE) (0x0100)

Sequence number: (BE) (0x013e), (LE) (0x3e01).

1.14 Για το μήνυμα αυτό ισχύει ότι τα πεδία αυτά έχουν ίδια τιμή για το πεδίο ταυτότητας & αύξοντα αριθμού.

1.15 Χρησιμοποιείται για αντιστοίχιση των Echo Requests με τα Reply τους γι' αυτό πρέπει να στέλνονται οι ίδιες τιμές.

1.16 Το ICMP Echo Reply έχει μήκος 32 bytes και για το περιεχόμενο, προκύπτει η ίδια ακολουθία με την 1.9 .

1.17 Όχι, δεν διαφέρει.

1.18 Η ανταλλαγή των μηνυμάτων ICMP σχετίζονται με τα αποτελέσματα της εντολής ping διότι, είτε από το Wireshark είτε από το παράθυρο εντολών, παρατηρούνται 4 ICMP Requests και 4 ICMP Reply τα οποία αντιστοιχούν σε 4 Request to Default Gateway και 4 Reply from Default Gateway.

1.19 Στάλθηκαν 12 πακέτα ARP Request.

1.20 Κάθε περίπου 1 – 1,5 sec.

1.21 Κανένα μήνυμα ICMP.

1.22 Μεταξύ των προηγούμενων και των αποτελεσμάτων της εντολής ping στο παράθυρο εντολών, ισχύει ότι για κάθε 1 Request που γίνεται και δεν αντιστοιχεί σε κάποια υπαρκτή διεύθυνση, αντιστοιχούν 3 ARP Request. Επίσης, το ping μπορεί να επιστρέψει Time Out και έτσι, να μην υπάρξουν μηνύματα ICMP.

2

2.1 Ο πίνακας ARP περιέχει τα εξής:

Interface: 192.168.1.3 --- 0x13

Internet Address	Physical Address	Type
192.168.1.1	78-96-82-50-a1-2a	dynamic
192.168.1.4	ac-07-5f-b6-95-fc	dynamic
192.168.1.255	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 Destination: 78-96-82-50-a1-2a, Source: 34-F6-4B-07-39-B5 .

2.3 Destination: 147.102.1.1, Source: 192.168.1.3 .

2.4 Η MAC Address του Source, είναι η IPv4 Address του υπολογιστή. Η MAC Address του Destination είναι η IPv4 Address 147.102.1.1 .

2.5 Όχι, δεν παρατηρήθηκαν πακέτα ARP.

2.6 Δεν παρατηρήθηκαν, διότι το Destination είναι εκτός του υποδικτύου οπότε η πρόσβαση σε αυτόν, γίνεται με τον δρομολογητή, ο οποίος έχει ήδη καταγραφεί στον πίνακα ARP.

2.7 Η σύνταξη: `icmp.type == 0`.

2.8 Επεξήγηση: οι τιμές του TTL στις επικεφαλίδες των πακέτων IPv4, είναι ίδιες με τις τιμές TTL στο παράθυρο εντολών. Μάλιστα, ενώ αρχικά η τιμή ήταν 64, σε κάθε hop μειώνεται κατά ένα οπότε, για την τιμή 58 θα ισχύει ότι τα μηνύματα πέρασαν από 64 – 58 + 1 = 7 ενδιάμεσους κόμβους.

2.9 Εμφανίζονται μόνο Type: (8) ICMP Echo Request.

2.10 Επειδή στέλνονται Echo Request εκτός δικτύου, η πρόσβαση γίνεται με χρήση δρομολογητή, ο οποίος υπάρχει στον πίνακα ARP, οπότε δεν στέλνονται μηνύματα ARP.

3

3.1 Το μήκος είναι 64 bytes και το περιεχόμενο των ICMP Echo Request είναι 00000000…

3.2 Συγκριτικά, είναι διπλάσιο και περιέχει μόνο μηδενικά.

3.3 Το μήνυμα είναι: Time-to-live Exceeded.

3.4 Για το προηγούμενο μήνυμα ισχύει: Type: 11 (Time-to-live Exceeded), Code: 0 (Time-to-live Exceeded in transit).

3.5 Υπάρχουν τα εξής: Type (1 Byte), Code (1 Byte), Checksum (2 Bytes), Unused (1 Byte), Length (1 Byte), Unused (4 Byte) και οι επικεφαλίδες IPv4 και ICMP του αντίστοιχου ICMP Request.

3.6 Το μήκος είναι 64 bytes.

3.7 Το περιεχόμενο του πεδίου δεδομένων είναι ίδιο (περιέχει μηδενικά) με αυτό του IPv4.

4

4.1 Οι τιμές μήκους δεδομένων ICMP για τις MTU είναι: 548(576-28), 978(1006-28), 1464(1492-28), 1472(1500-28).

4.2 Ναι, παρατηρήθηκε μήνυμα λάθους.

4.3 Παράχθηκε από: Source: 46.103.38.51 .

4.4 Για το ICMP Destination Unreachable: Type: 3 (Destination Unreachable), Code: 4 (Fragmentation needed).

4.5 Το πεδίο Code δηλώνει ότι το λάθος οφείλεται στην απαίτηση μη θρυμματισμού, διότι έχει τιμή 4 (Fragmentation needed). Η επικεφαλίδα Next-Hop MTU έχει τιμή: 1492.

4.6 Το πεδίο δεδομένων περιέχει τις επικεφαλίδες ICMP & IPv4 αλλά και τα πρώτα 520 bytes των δεδομένων του πακέτου που έστειλε ο υπολογιστής.

4.7 Για πρώτη φορά δεν λαμβάνεται μήνυμα λάθους για MTU: 1492 bytes.

4.8 Η Address δεν απαντά και για τις τιμές, 1006, 1500 και 1464 bytes.

4.9 Λαμβάνεται απάντηση για την τιμή: 576 bytes.

4.10 Η τιμή αυτή, είναι η τιμή MTU της διεπαφής του 147.102.40.15 .

4.11 Αυτό συμβαίνει διότι το 147.102.40.15 δεν λαμβάνει πακέτα μεγαλύτερα από την MTU της διεπαφής του, αφού αυτό είναι αρμοδιότητα του προηγούμενου δρομολογητή που ελέγχει το Next-Hop MTU.

4.12 Το μέγεθος του πρώτου θραύσματος που λαμβάνει ο υπολογιστής είναι: 586 bytes με Data 552 bytes. Ισχύει ότι, το μέγιστο μέγεθος κάθε θραύσματος προκύπτει ως το μέγεθος της MTU (576) αφαιρώντας το μέγεθος της επικεφαλίδας IPv4 (20 bytes) (δηλ. όσο τα Data + 4 για να είναι πολλαπλάσιο του 8). Επιπλέον, η επικεφαλίδα Ethernet έχει 14 bytes κι έτσι προκύπτουν τα

586 bytes.

5

5.1 Το φίλτρο σύλληψης: `host 147.102.40.15`.

5.2 Η ακριβής σύνταξη της εντολής: `nslookup 147.102.40.15 edu-dy.cn.ntua.gr`.

5.3 Η απάντηση που ελήφθη είναι: DNS Request timed out (δηλ. το αίτημα δεν μπόρεσε να φτάσει στο destination).

5.4 Ναι, παρατηρήθηκαν πακέτα DNS.

5.5 Το πρωτόκολλο μεταφοράς και η θύρα προορισμού είναι: Protocol: UDP (17) & Destination Port: 53.

5.6 Ναι, παρατηρήθηκαν.

5.7 Οι τιμές είναι: Type: 3 (Destination Unreachable) & Code: 3 (Port Unreachable).

5.8 Το πεδίο: Code: 3 (Port Unreachable).

5.9 Η Destination Port: 53 είναι η γνωστή ως θύρα προορισμού DNS.

5.10 Απάντηση: Η άσκηση πραγματοποιήθηκε με το λειτουργικό σύστημα Windows 10.

6

6.1 Η σύνταξη είναι: `ping -6 2001:648:2000:329::101` &

`tracert -6 2001:648:2000:329::101`.

6.2 Το φίλτρο σύλληψης: `ip6`, `φίλτρο απεικόνισης: icmpv6`.

6.3 Το πεδίο θα έχει την τιμή: Type: IPv6 (0x86dd).

6.4 Το μήκος είναι: 40 bytes.

6.5 Τα πεδία είναι:

Traffic Class (8 bits), Version (4 bits), Flow Label (20 bits), Payload Length (2 bytes), Next Header (1 byte), Hop Limit (1 byte), Source (16 bytes), Destination (16 bytes).

6.6 Η επικεφαλίδα Hop Limit είναι η αντίστοιχη.

6.7 Η επικεφαλίδα Next Header: ICMPv6 (58).

6.8 Ναι, είναι η ίδια δομή.

6.9 Η τιμή του πεδίου είναι: Type: Echo (ping) Request (128) με μήκος: Data (32 bytes).

6.10 Ναι, είναι η ίδια δομή.

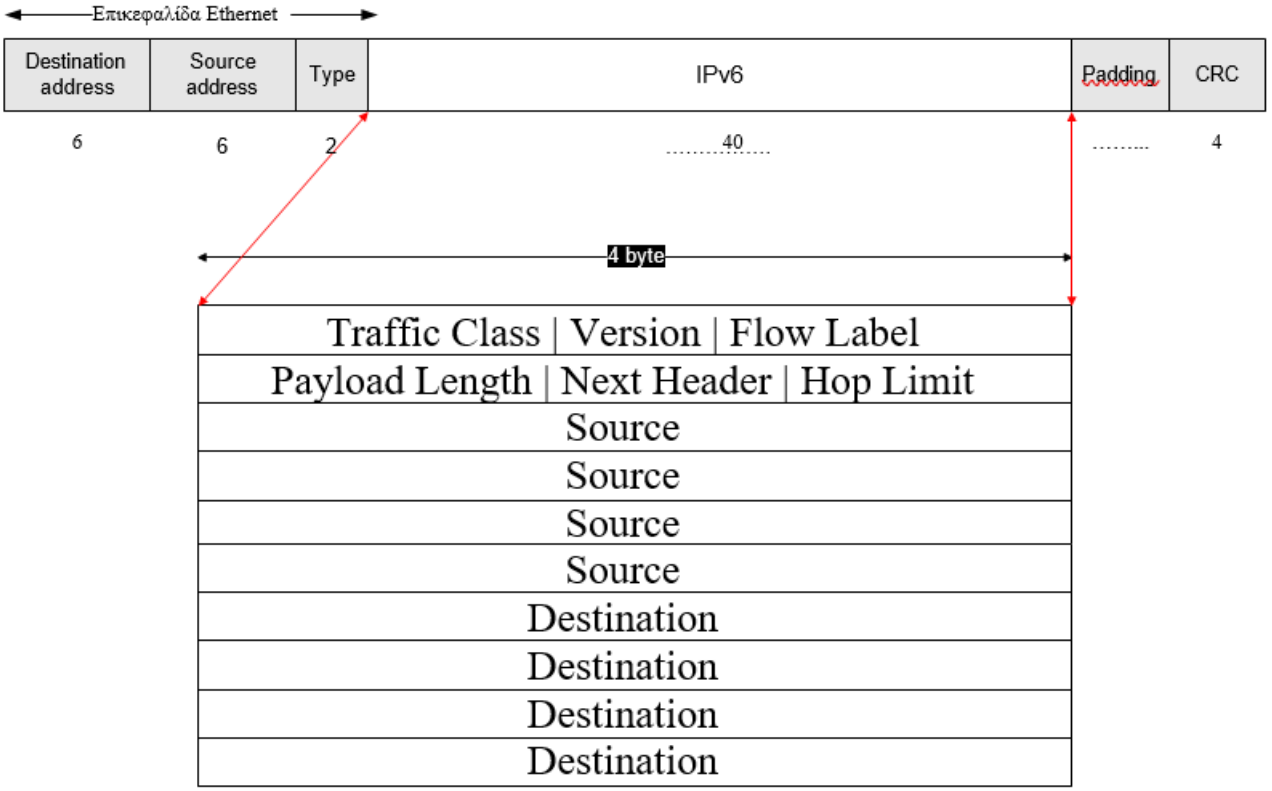
6.11 Η τιμή του πεδίου είναι: Type: Echo (ping) Request (12) με μήκος: Data (32 bytes).

6.12 Παρατηρείται ότι από την επικεφαλίδα IPv4 διαφέρουν τα πεδία Payload Length και Hop Limit ενώ από την επικεφαλίδα ICMPv6 το πεδίο Sequence. Επιπλέον, το πεδίο δεδομένων του μηνύματος με tracert έχει μήκος 64 bytes ενώ αυτό του ping έχει 32 bytes.

6.13 Η δομή διαφέρει διότι, αντί του πεδίου Unused, υπάρχει το πεδίο Reserved.

6.14 Η τιμή είναι: Type: Time Exceeded (3) και το μήκος: 64 bytes.

6.15 Το πεδίο δεδομένων περιέχει μηδενικά (δηλ. 000000…) που είναι τα ίδια με το αντίστοιχο Request.


Επικεφαλίδα Ethernet
Destination address
Source address
Type
IPv6
Padding
CRC
6
6
2
40
4
4 byte
Traffic Class | Version | Flow Label
Payload Length | Next Header | Hop Limit
Source
Source
Source
Source
Destination
Destination
Destination
Destination