Ονοματεπώνυμο: Χαράλαμπος Καμπουγέρης Ομάδα: 3, Τετάρτη 10:45-12:30, Αιθ.Α2

Όνομα PC/ΛΣ: CHARALAMPOSs-MacBook-Air/ macOS 14.0 Ημερομηνία: 19/11/2023

Εργαστηριακή Άσκηση 6 Πρωτόκολλο ICMP

Άσκηση 1

- 1.1 ether host 0c:e4:41:e1:6c:74
- 1.2 arp or icmp
- **1.3** Μετά την εκτέλεση την εντολής ping προς το default gateway, ανταλλάσονται πακέτα arp με gateway το οποίο γνωρίζοντας την ip του υπολογιστή μας, ζητά να μάθει την MAC address ώστε να συμπληρώσει το arp table.
- **1.4** Πεδίο:Protocol Τιμή: ICMP (01)
- **1.5** Είναι 8 bytes
- 1.6 (1) Type, (2) Code, (3) Checksum, (4) Identifier, (5) Sequence Number
- 1.7 Type: 8 (Echo (ping) request)

Code: 0

1.8 Identifier (BE): 9221 (0x2405) Identifier (LE): 1316 (0x0524)

Sequence Number (BE): 0 (0x0000) Sequence Number (LE): 0 (0x0000)

1.9 Data Length: 48 bytes και το περιεχόμενο είναι

Data:

08090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f202122232425262728292a2b2c2d2e2f3031323334353637

- 1.10 Είναι 8 bytes και έχει ίδια δομή με το Echo Request
- **1.11** Type: 0 (Echo (ping) reply)

Code: 0

1.12 Το πεδίο Type

1.13 Identifier (BE): 9221 (0x2405)

Identifier (LE): 1316 (0x0524)

Sequence Number (BE): 0 (0x0000) Sequence Number (LE): 0 (0x0000)

- 1.14 Εχουν ίδιες τιμές Identifier και Sequence Number
- **1.15** Χρησιμοποιούνται για να γίνεται η αντιστοίχιση ενός request πακέτου με το αντίστοιχο reply.
- 1.16 Data Length: 32 bytes

Data: ίδιο με το περιεχόμενο Data του echo request πακέτου (ερώτημα 1.9)

- **1.17** Όχι
- **1.18** Οι ανταλλαγές πακέτων γίνονται μεταξύ του υπολογιστή και μιας συγκεκριμένης IP. Τα αποτελέσματα της ping αναπαριστούν το χρόνο που έκαναν τα πακέτα για να φτάσουν στην IP και να επιστρέψουν, το περιεχόμενο τους σε bytes και το TTL.
- 1.19 ping -c 2 <destination address>
- **1.20** Στάλθηκαν 2 ARP πακέτα
- **1.21** Στέλνονται κάθε περίπου 1 δευτερόλεπτο
- **1.22** Δε στάλθηκε κανένα μήνυμα ICMP
- 1.23 Δεδομένου ότι δε μπορεί να βρεθεί η διεύθυνση είναι λογικό να μη μπορούν να σταλούν echo requests και να μην υπάρχουν arp replies. Οπότε, είναι αναμενόμενο η ping να επιστρέφει Request timeout for icmp_seq 0

Άσκηση 2

- **2.1** Δεν έχει προστεθεί κάποια διεύθυνση στον πίνακα arp
- 2.2 Destination: 50:78:b3:cd:48:fa Source: 0c:e4:41:e1:6c:74
- 2.3 Source Address: 147.102.203.111 Destination Address: 147.102.1.1
- **2.4** H MAC του Destination (50:78:b3:cd:48:fa) αντιστοιχεί στην IP 147.102.1.1 και η MAC του Source (0c:e4:41:e1:6c:74) στην 147.102.203.111
- 2.5 Όχι, δεν παρατήρησα

- **2.6** Δεν υπήρξαν διότι η ΙΡ προς την οποία έγινε το ping είναι εκτός του τοπικού δικτύου οπότε δεν μπορούμε να βρούμε άμεσα την ΜΑC, χωρίς να διαμεσολαβήσει κάποιος δρομολογητής
- 2.7 Display filter: arp or icmp.type == 0
- 2.8 Προκύπτει από το πεδίο Time to Live της επικεφαλίδας IPv4 του πακέτου reply
- 2.9 Εμφανίζονται μόνο ICMP Echo requests
- **2.10** Στη προηγούμενη περίπτωση δεν είχαμε μηνύματα ICMP requests, αλλά μόνο ARP. Σε αυτή τη περίπτωση, λόγω του διαφορετικού υποδικτύου, δεν στέλνονται στον υπολογιστή μας πακέτα ARP (αλλά στο router). Επομένως, ο υπολογιστής μας κάπως πρέπει να εντοίσει αν υπάρχει ο υπολογιστής με την IP που ψάχνει και αυτό γίνεται στέλνοντας requests τα οποία κάνουν expire.

Άσκηση 3

- **3.2** Στη ping το μήκος είναι μεγαλύτερο κατα 4 bytes. Επίσης το περιεχόμενο στη traceroute είναι μόνο μηδενικά σε αντίθεση με αυτό της ping
- 3.3 Time-to-live exceeded
- **3.4** Type: 11 (Time-to-live exceeded) → 0b HEX Code: 0 (Time to live exceeded in transit) → 00 HEX
- **3.5** Checksum (2 bytes), Unused (1 + 2 bytes), Length (1 byte)
- **3.6** Header Length = 8 bytes, Data = 20 + 8 + 40 = 68 bytes
- **3.7** Το περιεχόμενο του πεδίου δεδομένων είναι ολόκληρα τα πακέτα IPv4 και ICMP του echo request που προκάλεσε το μήνυμα λάθους

Άσκηση 4

- **4.1** Θα πρέπει Data + Headers = MTU. Άρα σε όλες τις τιμές της MTU που αναγράφονται για να ορίσουμε το length του πακέτου αφαιρούμε το IPv4 header (20 bytes) και το ICMP header (8 bytes). Ελέγχουμε, λοιπόν, τις τιμές 1472, 1464, 978, 548
- 4.2 Όχι, δεν παρατηρήσαμε
- **4.3** (Χρησιμοποιήθηκε το αρχείο mtu.pcap)

Type: 3 (Destination unreachable) \rightarrow 03 HEX Code: 4 (Fragmentation needed) \rightarrow 04 HEX

- **4.4** Η τιμη του πεδίου Code (4) μας υποδηλώνει ότι το λάθος οφείλεται στην απαίτηση μη θρυμματισμού (Fragmentation needed). Το MTU of next hop έχει τιμη 1492
- **4.5** Το πλαίσιο ICMP
- **4.6** Για τη τιμή MTU = 1492
- **4.7** Δεν απαντά για τις τιμές 1500, 1492 και 1006
- **4.8** Για τη τιμή MTU = 576
- **4.9** Είναι η MTU κάποιου ενδιάμεσου κόμβου, γιατί για την αμέσως επόμενη μεγαλύτερη τιμή της MTU είχε υπάρξει σφάλμα σε ενδιάμεσο κόμβο.
- 4.10 Όχι, καθώς είναι τελικός κόμβος
- **4.11** Γιατί είναι ο τελικός κόμβος, επομένως δεν χρειάζεται να θρυματίσει το πακέτο.
- **4.12** Έχει μέγεθος 586 bytes και είναι μικρότερο από την τιμή της ερώτησης 4.7

Άσκηση 5

- **5.1** host 147.102.40.15
- **5.2** host edu-dy.cn.ntua.gr 147.102.40.15
- **5.3** no servers could be reached, άρα το μήνυμα δεν φτάνει στον προορισμό του και για αυτό έχουμε communication error: connection refused
- **5.4** Ναι, παρατηρήθηκε 1 μήνυμα DNS
- **5.5** Πρωτόκολλο μεταφοράς είναι το UDP και Destination Port η 53
- **5.6** Ναι, παρατήσαμε 1 ICMP μήνυμα
- **5.7** Type: 3 (Destination unreachable) \rightarrow 03 HEX Code: 3 (Port unreachable) \rightarrow 03 HEX
- **5.8** Το πεδίο Code
- **5.9** Τα μηνήματα DNS έχουν πάντα Destination Port : 53

5.10 Κανονικά απαντάει με echo reply, αλλα εδώ η απάντηση ειναι το destination unreachable

Άσκηση 6

(Χρησιμοποιήθηκε το αρχείο icmpv6.pcap)

6.1 ping6 2001:648:2000:329::101

traceroute6 -I 2001:648:2000:329::101

6.2 Capture filter : ip6

Display filter: icmpv6

6.3 Type: IPv6 (0x86dd)

6.4 IPv6 Header: 40 bytes

6.5

Version: 1 byte
Traffic Class: 4 bytes
Flow Label: 3 bytes
Payload Length: 2 bytes
Next Header: 1 byte
Hop Limit: 1 byte

Source Address: 16 bytes Destination Address: 16 bytes

6.6 Hop Limit

6.7 Το πεδίο Next Header το οποίο έχει τιμή $58 \rightarrow 3\alpha$ HEX

6.8 Ναι, είναι ίδια

6.9 Type: Echo (ping) request (128) \rightarrow 80 HEX

Data Length: 32 bytes

6.10 Ναι, είναι ίδια

6.11 Type: Echo (ping) request (129) \rightarrow 81 HEX

Data Length: 32 bytes

6.12 Έχει διπλάσιο μήκος δεδομένων (64 bytes)

6.13 Όχι, έχει προστεθεί το πεδίο Reserved

6.14 Type: Time Exceeded (3) \rightarrow 03 HEX

Data Length: 64 bytes

6.15 Περιέχει μόνο μηδενικά

6.16 Παρατήρησα μηνήματα ICMPv6 τύπου Neighbor Solicitation και Neighbor Advertisement

6.17 Έχουν Type: Neighbor Solicitation (135) και Type: Neighbor Advertisement (136) αντίστοιχα και μέγεθος πακέτου ίσο με 86 bytes συνολικά.