

6^ο Εργαστήριο στα Δίκτυα Υπολογιστών

Πρωτόκολλο ICMP

Όνοματεπώνυμο: **Αλέξανδρος Κυριακάκης (03112163)**

Ομάδα: **2**

Όνομα PC/ΛΣ: **MacBook Pro - Alexandros, macOS Catalina**

Ημερομηνία: **9/11/2020**

Διεύθυνση IP: **192.168.1.5**

Διεύθυνση MAC: **a4:83:e7:97:af:31**

1 Εντολή ping στο τοπικό υποδίκτυο

1.1 Το φίλτρο σύλληψης είναι "ether host a4:83:e7:97:af:31".

1.2 Το φίλτρο απεικόνισης είναι "icmp or arp"

1.3 Καταγράφηκαν και ο σκοπός τους είναι να γνωστοποιήσουν την MAC Address της default gateway (στην οποία έκανα την μετάδοση) στον υπολογιστή μου.

1.4 Το όνομα είναι Protocol και η τιμή του είναι ICMP (0x01).

1.5 Είναι 8bytes.

1.6 Είναι τα εξής,

- Type: 1byte
- Code: 1byte
- Checksum: 2bytes
- Identifier: 2bytes
- Sequence Number: 2bytes

← 4 bytes →

Type	Code	Checksum
Identifier		Sequence Number
Timestamp from icmp data		
Timestamp from icmp data		

1.7 Είναι,

- Type: 8 (0x08)
- Code: 0 (0x00)

1.8 Είναι,

- Identifier: 29958 (0x7506)
- Sequence Number: 0 (0x0000)

1.9 Το μήκος είναι 48 bytes και το περιεχόμενο είναι αύξοντες δεκαεξαδικοί αριθμοί μήκους 1 byte ο καθένας, ξεκινώντας από το 0x08.

1.10 Το μήκος επικεφαλίδας ICMP Echo reply είναι πάλι 8 *bytes* και έχει την ίδια δομή με το Echo request.

1.11 Είναι,

- Type: 0 (0x00)
- Code: 0 (0x00)

1.12 Το πεδίο Type. (Μαλλον έχει γίνει τυπογραφικό λάθος στην άσκηση και εννοούσε **1.7** και 1.11)

1.13 Είναι,

- Identifier: 29958 (0x7506)
- Sequence Number: 0 (0x0000)

(Στο 1.8 είχαμε διαλέξει το πρώτο request και τώρα διαλέξαμε το πρώτο reply)

1.14 Είναι ίδιες.

- Identifier: 29958 (0x7506)
- Sequence Number: 0 (0x0000)

1.15 Βοηθούν στο ταίριασμα των request και replies ένα προς ένα. Όπως βλέπω και στα πακέτα που έστειλα με μία εντολή ping, όλα έχουν το ίδιο Identifier και το Sequence number αυξάνετε όσο μεταδίδονται νέα. Για να αντιστοιχηθούν ένα προς ένα τα replies σε αυτά που έστειλα, έχουν όλα το ίδιο Identifier με τα Request και τα αντιστοιχα αύξοντα Sequence Numbers (0,1,2,...).

1.16 Το μήκος είναι 48 bytes και το περιεχόμενο είναι το ίδιο με το Echo Request (αύξοντες δεκαεξαδικοί 1.9).

1.17 Όχι δεν διαφέρει.

1.18 Είναι άρρηκτα συνδεδεμένα αφού κάθε πληροφορία που τυπώνει η εντολή ping είναι πληροφορία των πακέτων IPv4 που στέλνει, ή παράγωγο αυτής.

1.19 Στάλθηκαν 5 πακέτα ARP μέχρι που η εντολή ping τύπωσε "Host is down".

1.20 Κάθε 1 sec.

1.21 Κανένα. (Σε δεύτερη προσπάθεια που έκανα έλαβα ένα Destination Not Reachable)

1.22 Κάθε ένα ICMP πακέτο προκειμένου να φύγει από τον υπολογιστή μου για τον "κενό" προορισμό πρέπει να ξέρει την MAC Address του. Έτσι για τα 5 πρώτα ICMP κάνει αυτόματα 5 broadcast σε όλους τους κόμβους για να μάθει την MAC Address. Αφού δεν λαμβάνει απάντηση υποθέτει ότι ο "Host is down" και παύει να προσπαθεί.

2 Εντολή ping σε άλλο υποδίκτυο

2.1 Κάνοντας την εντολή,

```
~ arp -a
? (192.168.1.1) at 94:a7:b7:47:13:ae on en0 ifscope [ethernet]
? (192.168.1.4) at a4:e9:75:2b:91:33 on en0 ifscope [ethernet]
? (192.168.1.5) at a4:83:e7:97:af:31 on en0 ifscope permanent [ethernet]
? (192.168.1.9) at 16:c2:73:ff:55:4e on en0 ifscope [ethernet]
? (192.168.1.13) at f4:db:e3:4b:35:2c on en0 ifscope [ethernet]
? (192.168.1.255) at ff:ff:ff:ff:ff:ff on en0 ifscope [ethernet]
? (224.0.0.251) at 1:0:5e:0:0:fb on en0 ifscope permanent [ethernet]
? (239.255.255.250) at 1:0:5e:7f:ff:fa on en0 ifscope permanent [ethernet]
```

Άρα οι IPv4 που περιέχει είναι

- 192.168.1.1
- 192.168.1.4
- 192.168.1.5
- 192.168.1.9
- 192.168.1.13
- 192.168.1.255
- 224.0.0.251
- 239.255.255.250

2.2 Του αποστολέα είναι: a4:83:e7:97:af:31 και του παραλήπτη: 94:a7:b7:47:13:ae.

2.3 Του αποστολέα είναι: 192.168.1.5 και του παραλήπτη 147.102.7.1.

2.4 Οι διευθύνσεις του 2.2, όπως βλέπουμε από τον πίνακα ARP 2.1 αντιστοιχούν ως εξής,

- 192.168.1.1 → 94 : a7 : b7 : 47 : 13 : ae
- 192.168.1.5 → a4 : 83 : e7 : 97 : af : 31

2.5 Όχι δεν παρατήρησα.

2.6 Η εντολή ping που έτρεξα έστειλε πακέτα σε εξωτερικό δίκτυο που σημαίνει ότι δρομολογήθηκαν μέσω της default gateway της οποίας έχω ήδη αποθηκευμένη την MAC Address στον ARP πίνακα αυτού υπολογιστή.

2.7 Είναι "icmp.type == 0".

2.8 Βλέπω ότι η τιμή σε όλα τα πακέτα είναι $TTL = 57$. Επίσης γνωρίζω ότι η default τιμή $TTL = 64$. Οπότε αν υποθέσουμε ότι έχει αυτή την τιμή τότε το 57 που βλέπουμε υποδεικνύει ότι έγιναν 8 hops μέχρι να φτάσει το πακέτο σε μένα. Τρέχοντας την εντολή "tracert 147.102.7.1" βλέπουμε ότι όντως είναι 8 κόμβους μακριά το συγκεκριμένο υποδίκτυο.

2.9 Εμφανίζονται δύο τύποι μηνυμάτων ICMP,

1. Type: 8 (0x08) (Echo (ping) Request)
2. Type: 3 (0x03) (Destination unreachable)

2.10 Θεμελιώδης διαφορά είναι ότι στην περίπτωση του τοπικού μου δικτύου τα πακέτα ICMP δεν έφυγαν ποτέ, αφού δεν είχαν την MAC Address της συσκευής για να συμπληρωθεί η επικεφαλίδα Ethernet. Αντιθέτως δεδομένου ότι τα πακέτα σε εξωτερικά υποδίκτυα δρομολογούνται μέσω της default gateway, έχουμε την MAC Address της, και επίσης αφού δεν μπορούμε να γνωρίζουμε αν οι IPv4 Addresses αντιστοιχούν σε ενεργό κόμβο, τα πακέτα φεύγουν κανονικά. Τέλος δεδομένου ότι διέρχονται από τον DNS μας, στην περίπτωση του εξωτερικού δικτύου, παίρνουμε απάντηση από αυτόν το πακέτο τύπου 3 Destination Unreachable, κάτι που στο τοπικό μας δίκτυο δεν συμβαίνει.

Στο εξής η IPv4 μου είναι 192.168.1.4

3 Εντολή tracert/traceroute

3.1 Το μήκος των δεδομένων είναι 44 bytes και το περιεχόμενό τους μηδενικά (0x00).

3.2 Διαφέρουν και τα δύο καθώς,

- Το μήκος στην εντολή ping ήταν 48 bytes ενώ τώρα είναι 44.
- Το περιεχόμενο στην εντολή ping ήταν αύξοντες αριθμοί ενώ τώρα είναι μηδενικά.

3.3 Παρατηρώ το μήνυμα "Time-to-live exceeded (Time to live exceeded in transit)".

3.4 Είναι

- Type: 11 (0x0b)
- Code: 0 (0x00)

3.5 Υπάρχουν τα,

- Checksum: 2 bytes
- Unused: 4 bytes

3.6 Είναι 68 bytes.

3.7 Το περιεχόμενο του μηνύματος λάθους είναι το IPv4 header του ληφθέντος ICMP request μηνύματος στον κόμβο καθώς και τα πρώτα 64 bit (8 bytes) του ICMP request μηνύματος που έλαβε. (Κάποιοι από τους κόμβους επιστρέφουν και 40 bytes από το περιεχόμενο του ICMP request)

4 Ανακάλυψη MTU διαδρομής(Path MTU Discovery)

4.1 Χρησιμοποίησα τις εξής τιμές, 1472, 1464, 978, 548, 524, 516, 484, 480, 268.

4.2 Ναι παρατήρησα.

4.3 Το παράγγαγε το router μου. Φαίνεται από την source διεύθυνση IPv4, 192.168.1.1.

4.4

- Type: 3 (0x03)
- Code: 4 (0x04)

4.5 Το Code: 4 δηλώνει ότι χρειαζόταν θρυμματισμός, ενώ η τιμή του πεδίου "MTU of next hop" είναι 1492.

4.6 Περιέχει την Επικεφαλίδα IPv4 και ICMP καθώς και 520 bytes από το δεδομένα ICMP request που έλαβε ο κόμβος αυτός.

4.7 Είναι 1492 bytes.

4.8 Συνολικά δεν απαντά για τις εξής τιμές της MTU: 1500, 1492, 1006.

4.9 Είναι 576 bytes.

4.10 Είναι κάποιου ενδιάμεσου κόμβου. Το εξακριβώσα με τον εξής τρόπο,

1. Έκανα μελέτη του μονοπατιού μέχρι την διεύθυνση 147.102.40.15 με την εντολή "ping -c 1 -R" όπως είδαμε σε προηγούμενο πρόβλημα.
2. Έστειλα Echo requests σε έναν έναν τους ενδιάμεσους κόμβους "ping -c 1 -D -s \$((1006-28)) 80.106.125.100"...
3. Παρατήρησα ότι σταματούσε η μετάδοση πριν φτάσω στον κόμβο προορισμού. Συγκεκριμένα στον κόμβο ote-2.gr-ix.gr (176.126.38.34).

4.11 Διότι ο κόμβος που παρήγαγε το μήνυμα ενδεχομένως έβαλε στα δεδομένα όλη την πληροφορία που έλαβε και έτσι ξεπέρασε το MTU σε κάποιο από τους κόμβους επιστροφής, καθώς γνωρίζουμε ότι δεν είναι αναγκαία οι ίδιοι κόμβοι με αυτούς που περνάει για να φτάσει ως εκεί.

4.12 Δεν παρατηρώ Θρυμματισμό.

5 Απόρσιτη θύρα (Port Unreachable)

5.1 Χρησιμοποίησα το "ip host 147.102.40.15".

5.2 Είναι "dig -4 @147.102.40.15 edu-dy.cn.ntua.gr".

5.3 Έλαβα την απάντηση Destination Unreachable (Port unreachable). Που σημαίνει ότι η διεύθυνση του DNS δεν ακούει στην συγκεκριμένη port (53).

5.4 Ναι παρατήρησα.

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

5.6 Ναι παρατήρησα.

5.7 Είναι,

- Type: 3 (0x03)
- Code: 3 (0x03)

5.8 Το δηλώνει το πεδίο Code.

5.9 Η port 53 είναι προκαθορισμένη για χρήση DNS Queries.

5.10 Αφού έκανα την εντολή "traceroute edu-dy.cn.ntua.gr" και χρησιμοποιώντας το ίδιο φίλτρο σύλληψης για το wireshark, παρατήρησα ότι απαντά με το ίδιο ακριβώς μήνυμα, Destination Unreachable (Port unreachable).

6 IPv6 και ICMPv6

6.1 Είναι η "ping6 -c 1 2001:648:2000:329::101 ; traceroute6 -I 2001:648:2000:329::101".

6.2 Το φίλτρο σύλληψης είναι το "ip6" και το φίλτρο απεικόνισης είναι "icmpv6"

6.3 Type: IPv6 (0x86dd).

6.4 Έχει μήκος 40 bytes.

6.5 Είναι τα εξής,

- Version: 4 bit
- Traffic Class: 8 bit
- Flow Label: 4 bit + 2 byte
- Payload Length: 2 byte
- Next Header: 1 byte
- Hop Limit: 1 byte
- Source Address: 16 byte
- Destination Address: 16 byte

←————— 4 bytes —————→

Version	Traffic class	Flow Label	
Payload Length		Next Header	Hop Limit
Source Address			
Source Address			
Source Address			
Source Address			
Destination Address			
Destination Address			
Destination Address			
Destination Address			

- 6.6** Είναι το Hop Limit.
- 6.7** Είναι το Next Header και η τιμή της για ICMPv6 είναι 58 (0x3a).
- 6.8** Ναι είναι ίδια.
- 6.9** Η τιμή του πεδίου Type είναι 128 (0x80) και το μήκος των δεδομένων του είναι 8 bytes.
- 6.10** Ναι είναι ίδια.
- 6.11** Η τιμή του πεδίου Type είναι 129 (0x81) και το μήκος των δεδομένων του είναι 8 bytes.
- 6.12** Διαφέρουν σε όλα τα πεδία εκτός από το Type και το Code.
- 6.13** Είναι ίδια εκτός από το τελευταίο πεδίου οπού στην 3.4, 3.5 υπάρχει το πεδίο Unused που εδώ αντικαθίσταται από το πεδίο Reversed.
- 6.14** Η τιμή του πεδίου Type είναι 3 (0x03) και το μήκος των δεδομένων του είναι 56 bytes.
- 6.15** Περιέχει τις επικεφαλίδες των IPv6 και ICMPv6 του μηνύματος που ελήφθη καθώς και τα δεδομένα αυτού.