Δίκτυα Υπολογιστών

Εργαστηριακή Άσκηση 6
Πρωτόκολλο ICMP

Ονοματεπώνυμο: Νικόλαος Παγώνας, el18175	**Ομάδα:** 4 (Τρίτη εξ' αποστάσεως)
Όνομα PC/ΛΣ: nick-ubuntu/Ubuntu 20.04.3 LTS	**Ημερομηνία:** Τρίτη 23/11/2021
Διεύθυνση IP: `192.168.1.15`	**Διεύθυνση MAC:** `3c:2c:30:e1:1c:55`

1 - Εντολή ping στο τοπικό υποδίκτυο

Εκτελέσαμε την εντολή `ping 192.168.1.7`.

1.1

Το φίλτρο σύλληψης που χρησιμοποιήσαμε είναι `ether host 3C:2C:30:E1:1C:55`.

1.2

Το φίλτρο απεικόνισης που χρησιμοποιήσαμε είναι `arp || icmp`.

1.3

Ο σκοπός των πακέτων ARP που ανταλλάχθηκαν είναι να βρεθεί σε ποια MAC address αντιστοιχεί η IPv4 διεύθυνση 192.168.1.7.

1.4

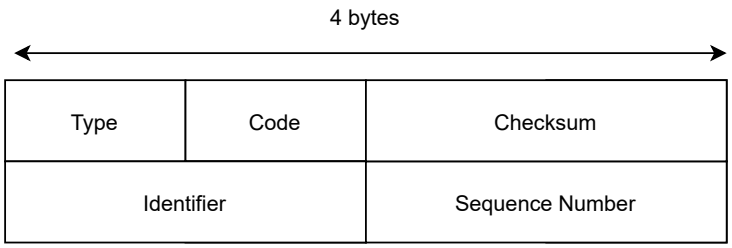
Το πεδίο που προσδιορίζει ότι πρόκειται για μήνυμα ICMP είναι το `Protocol`, και έχει τιμή `0x01`.

1.5

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

1.6

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



1.7

- Type: 0x08
- Code: 0x00

1.8

- Identifier: 0x0001
- Sequence Number: 0x0001

1.9

Το μήκος του πεδίου δεδομένων είναι 48 bytes, ενώ το περιεχόμενο είναι:

2f020400000000001011121314151617181 91a1b1c1d1e1f202122232425262728292a2b2c2d2e2f3031323334353637.

Παρατηρούμε ότι μετά από ένα σημείο έχουμε byte που είναι διαδοχικά μεταξύ τους (10, 11, 12, ...).

1.10

Τόσο το μήκος όσο και η δομή της επικεφαλίδας ενός μηνύματος ICMP Echo reply είναι ίδια με το ICMP Echo request.

1.11

- Type: 0x00
- Code: 0x00

1.12

Το πεδίο Type καθορίζει το είδος του μηνύματος, αφού αυτό είναι που διαφέρει μεταξύ των δύο περιπτώσεων.

1.13

- Identifier: 0x0001
- Sequence Number: 0x0001

1.14

- Identifier: 0x0001
- Sequence Number: 0x0001

Παρατηρούμε ότι τα πεδία έχουν ίδιες τιμές στο Request και στο Reply.

1.15

Τα πεδία αυτά χρησιμοποιούνται προκειμένου να γίνει η αντιστοίχιση μεταξύ request και reply.

1.16

Μήκος 48 bytes, περιεχόμενο πεδίου δεδομένων:

2f020400000000001011121314151617181911a1b1c1d1e1f202122232425262728292a2b2c2d2e2f3031323334353637.

Πάλι έχουμε διαδοχικά byte (10, 11, 12, ...).

1.17

Όχι, είναι το ίδιο.

1.18

Κάθε ανταλλαγή ICMP Request/Reply αντιστοιχεί και σε μία γραμμή που τυπώνει η ping στο παράθυρο εντολών.

1.19

Στέλνουμε στην ίδια συσκευή με διεύθυνση 192.168.1.7, αλλά τώρα της έχουμε απενεργοποιήσει το ίντερνετ.
Χρησιμοποιήσαμε την εντολή `ping -c 2 192.168.1.7`.

1.20

Στάλθηκαν:

- 1 πακέτο ARP ”Who has 192.168.1.15? Tell 192.168.1.1”
- 1 πακέτο ARP ”192.168.1.15 is at 3c:2c:30:e1:1c:55”
- 4 πακέτα ARP ”Who has 192.168.1.7? Tell 192.168.1.15”.

1.21

Τα τελευταία 4 πακέτα στέλνονται ανά 1 sec περίπου.

1.22

Δεν στάλθηκε κανένα πακέτο ICMP.

1.23

Παρατηρούμε από το παράθυρο εντολών ότι έγινε προσπάθεια να σταλούν 2 πακέτα, αλλά ”χάθηκαν” και τα 2, δηλαδή δεν είχαμε επιτυχή αποστολή.

2 - Εντολή ping σε άλλο υποδίκτυο

2.1

Κάνουμε `ip neigh flush all` για να φανούν ξεκάθαρα οι διευθύνσεις IPv4 που θα προκύψουν μετά το ping. Στην συνέχεια κάνουμε `ping 147.102.1.1`. Με την εντολή `ip neigh` καταγράφουμε τις διευθύνσεις 192.168.1.1 και 192.168.1.9.

2.2

- Source: `3c:2c:30:e1:1c:55`
- Destination: `e0:0e:e4:59:40:50`

2.3

- Source: `192.168.1.15`
- Destination: `147.102.1.1`

2.4

Η διεύθυνση `3c:2c:30:e1:1c:55` αντιστοιχεί στην `192.168.1.15`, δηλαδή στο μηχάνημά μας, ενώ η `e0:0e:e4:59:40:50` αντιστοιχεί στην `192.168.1.1`, δηλαδή στην διεύθυνση του router μας.

2.5

Ναι, παρατηρήσαμε.

2.6

Επειδή είχαμε κάνει flush τον πίνακα arp, έπρεπε να γίνει η αντιστοίχιση των IPv4 διευθύνσεων σε διευθύνσεις MAC. Επομένως είναι λογικό να εμφανιστούν πακέτα ARP κατά την καταγραφή.

2.7

Επειδή τα ICMP Echo replies έχουν Type = 0, το φίλτρο θα είναι `icmp.type == 0`.

2.8

Επειδή η default τιμή του TTL ακριβώς μόλις φεύγουν τα πακέτα είναι 64, και η τιμή που βλέπουμε με το Wireshark είναι 58, αυτό σημαίνει ότι η διεύθυνση Η διεύθυνση 147.102.1.1 είναι 7 hops μακριά (μπορούμε να το επιβεβαιώσουμε και με την traceroute).

2.9

Εμφανίζονται `ICMP echo ping request` και `ICMP destination unreachable (port unreachable)`.

2.10

Στην περίπτωση που κάναμε ping στο μηχάνημα του υποδικτύου μας, τα πακέτα ICMP δεν έφυγαν ποτέ, αφού χρειαζόταν η MAC address του μηχανήματος. Αντίθετα, όταν κάνουμε ping σε ανενεργό υπολογιστή εκτός του υποδικτύου μας, τα πακέτα ICMP πηγαίνουν στο router, άσχετα αν στη συνέχεια δεν θα βρουν τον προορισμό, οπότε παρατηρείται η κίνησή τους.

3 - Εντολή tracert/traceroute

3.1

Το μήκος είναι 32 bytes και το περιεχόμενο είναι:

48494a4b4c4d4e4f505152535455565758595a5b5c5d5e5f6061626364656667

(αυξανόμενοι δεκαεξαδικοί αριθμοί από το 48 μέχρι και το 67).

3.2

Στο 1.9 είχαμε 48 bytes, ενώ τώρα έχουμε 32.

3.3

Time-to-live exceeded (Time to live exceeded in transit)

3.4

Type: 0x0b (Time-to-live exceeded), Code: 0x00 (Time to live exceeded in transit)

3.5

- Checksum: 2 bytes
- Unused: 1 byte
- Length: 1 byte
- Unused: 2 bytes

3.6

Μήκος επικεφαλίδας 8 bytes, Μήκος δεδομένων 68 bytes.

3.7

Το περιεχόμενο είναι το IP Header του πακέτου που προκάλεσε το σφάλμα, καθώς και ένα μέρος (τα leading octets) των δεδομένων του.

4 - Ανακάλυψη MTU διαδρομής (Path MTU Discovery)

4.1

Οι τιμές πεδίου δεδομένων που θα χρησιμοποιήσουμε είναι 1472, 1464, 978, 548, 524, 516, 484, 480, 268, κατά 28 byte μικρότερες από το μέγεθος πακέτων IPv4 που αναγράφονται στην εκφώνηση (επειδή το IP header είναι 20 bytes και το ICMP Header 8 bytes).

4.2

Ναι, παρατηρήσαμε.

4.3

Το παρήγαγε ο κόμβος με IPv4 διεύθυνση 192.168.1.1, δηλαδή το router μας.

4.4

- Type: 0x03 (Destination Unreachable)
- Code: 0x04 (Fragmentation Needed)

4.5

Το πεδίο `Fragmentation needed` δείχνει ότι χρειαζόταν θρυμματισμός, ενώ το πεδίο `MTU of next hop` είναι 1492.

4.6

Περιέχει την επικεφαλίδα IPv4, την επικεφαλίδα ICMP και 520 bytes ICMP Data από το πακέτο που έλαβε ο κόμβος που στέλνει το μήνυμα Destination Unreachable.

4.7

Είναι 1492 bytes.

4.8

Συνολικά δεν απαντά για τις τιμές 1500 (προφανώς αφού ξεπερνά το MTU) αλλά και για τις τιμές 1492 και 1006.

4.9

Η τιμή MTU για την οποία λαμβάνουμε απάντηση είναι 576 bytes.

4.10

Αν κάνουμε ping με καταγραφή διαδρομής μέχρι τον 147.102.40.15 και μετά κάνουμε ping σε όλους τους ενδιάμεσους κόμβους, με απαίτηση μη θρυμματισμού και με μέγεθος πακέτου IPv4 1006 (το αμέσως μεγαλύτερο από το 576), τότε βρίσκουμε ότι ο πρώτος κόμβος που δεν απαντά είναι ο 147.102.40.15, άρα η MTU είναι του 147.102.40.15.

4.12

Δεν παρατηρήσαμε θρυμματισμό.

5 - Απρόσιτη Θύρα (Port Unreachable)

5.1

Χρησιμοποιήσαμε φίλτρο σύλληψης `ip && host 147.102.40.15`.

5.2

Η σύνταξη της εντολής που χρησιμοποιήσαμε είναι: `dig -4 @147.102.40.15 edu-dy.cn.ntua.gr`

5.3

Λάβαμε την εξής απάντηση: connection timed out; no servers could be reached

```
~ ❯ dig -4 @147.102.40.15 edu-dy.cn.ntua.gr

; <<>> DiG 9.16.1-Ubuntu <<>> -4 @147.102.40.15 edu-dy.cn.ntua.gr
; (1 server found)
;; global options: +cmd
;; connection timed out; no servers could be reached
```

Αυτό σημαίνει ότι το request δεν έφτασε στον εξυπηρετητή DNS του 147.102.40.15.

5.4

Ναι, παρατηρήσαμε.

5.5

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

5.6

Ναι παρατηρήσαμε.

5.7

- Type: 0x03
- Code: 0x03

5.8

Το πεδίο Code.

5.9

Επειδή η θύρα 53 είναι προκαθορισμένη για αιτήματα DNS.

5.10

Έχουμε δει από την Εργαστηριακή Άσκηση 5 ότι ο προορισμός απαντά με Destination Unreachable (Port Unreachable).

6 - IPv6 και ICMPv6

6.1

Η σύνταξη των εντολών είναι:

```
ping -6 -c 1 2001:648:2000:329::101
traceroute -6 -I 2001:648:2000:329::101
```

6.2

Το φίλτρο σύλληψης είναι `ip6` και το φίλτρο απεικόνισης είναι `icmpv6`.

6.3

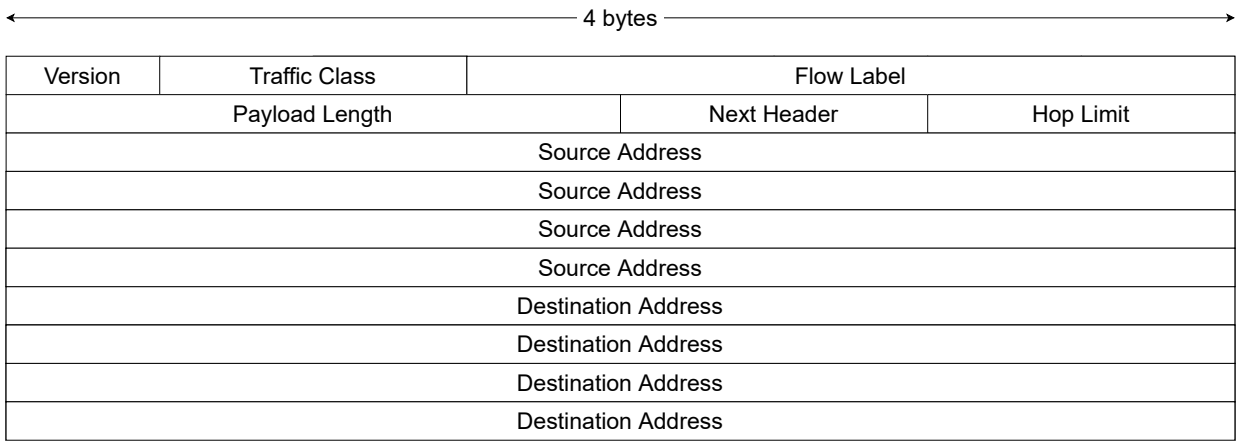
Το πεδίο Type έχει τιμή `0x86dd`.

6.4

Το μήκος της επικεφαλίδας IPv6 είναι 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 Address: 16 bytes
- Destination Address: 16 bytes



6.6

Η αντίστοιχη της TTL είναι η επικεφαλίδα Hop Limit.

6.7

Η επικεφαλίδα Next Header, για το ICMPv6 η τιμή της είναι 58.

6.8

Ναι, είναι ίδια.

6.9

Type: Echo (ping) request (128), μήκος δεδομένων: 56 bytes

6.10

Ναι, είναι ίδια.

6.11

type: Echo (ping) reply (129), μήκος δεδομένων: 56 bytes

6.12

Διαφέρει στα πεδία Payload Length (άρα και στο μέγεθος των ICMP Data), και στο πεδίο Hop Limit (αφού αρχικά η traceroute στέλνει πακέτα με μικρό Hop Limit και στη συνέχεια στέλνει πακέτα με σταδιακά μεγαλύτερο Hop Limit).

6.13

Η δομή είναι ίδια, εκτός από το ότι έχουμε το πεδίο Reserved αντί για το πεδίο Unused.

6.14

Η τιμή του πεδίου Type είναι 3 και το μήκος δεδομένων είναι 80 bytes.

6.15

Περιέχει τα IPv6 και ICMPv6 headers, καθώς και τα δεδομένα του μηνύματος που ελήφθη.

6.16

Παρατήρησα μηνύματα ICMPv6 Neighbor Advertisement/Solicitation.

6.17

Τα μηνύματα Neighbor Advertisement έχουν μήκος 24 ή 32 bytes και Type = 136, ενώ τα Neighbor Solicitation έχουν μέγεθος 32 bytes και Type = 135.