6η Εργαστηριακή Άσκηση στα Δίκτυα Υπολογιστών

Ονοματεπώνυμο	Γεώργιος Στεφανάκης
Αριθμός Μητρώου	el18436
Ομάδα	4
Λειτουργικό Σύστημα	Windows 10 Pro
Διεύθυνση IP	192.168.1.5 (147.102.131.77)
Διεύθυνση MAC	f8:75:a4:a2:7c:b1
Ημερομηνία	2022-11-18

1. Εντολή ping στο τοπικό υποδίκτυο

1.1. Capture filter: "ether host f8:75:a4:a2:7c:b1"

1.2. Display filter: "arp or icmp"

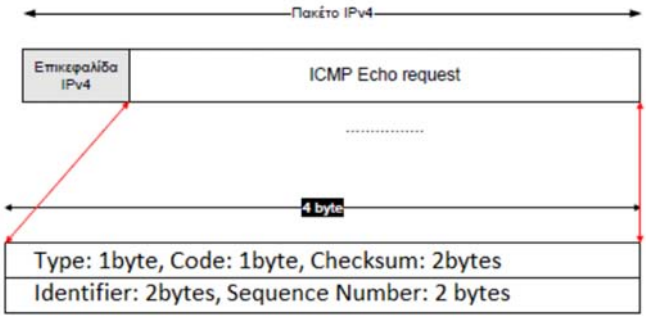
1.3. Καταγράφθηκαν και ο σκοπός τους είναι να γνωστοποιήσουν την διεύθυνση MAC του υπολογιστή στον οποίο κάναμε ping, προσθέτοντας τη διεύθυνσή του στο δικό μου το ARP table.

1.4. Το πεδίο της επικεφαλίδας IPv4 που προσδιορίζει ότι πρόκειται για μήνυμα ICMP είναι το Protocol: ICMP (1).

1.5. Είναι 8 bytes.

1.6. Τα πεδία της επικεφαλίδας είναι τα εξής:

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



1.7. Οι τιμές που καταγράφθηκαν είναι:

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

1.8. Οι τιμές που καταγράφθηκαν είναι:

- Identifier: 1 (0x0001)
- Sequence Number: 1 (0x0001)

1.9. Το μήκος του πεδίου δεδομένων είναι 32 bytes και το περιεχόμενο είναι αύξοντες δεκαδικοί αριθμοί μήκος ενός byte ο καθένας, ξεκινώντας από το 0x0008.

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

1.11. Οι τιμές που καταγράφθηκαν είναι:

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

1.12. Το πεδίο Type είναι το μόνο που αλλάζει.

1.13. Οι τιμές που καταγράφθηκαν είναι:
- Identifier: 1 (0x0001)
- Sequence Number: 11 (0x000b)

1.14. Οι τιμές είναι ίδιες με το ερώτημα 1.13 και ταυτίζονται για τα δύο αυτά πακέτα.

1.15. Χρησιμεύουν στην αντιστοίχιση των πακέτων request και reply. Με την εκτέλεση μίας εντολής ping, όλα τα πακέτα έχουν το ίδιο Identifier ενώ το Sequence number αυξάνεται όσο μεταδίδονται νέα πακέτα. Για να αντιστοιχηθούν τα replies με τα requests που τα προκάλεσαν, κάθε πακέτο reply έχει το ίδιο Sequence number με το πακέτο request που το προκάλεσε.

1.16. Το μήκος των δεδομένων του πακέτου Echo reply είναι 32 bytes.

1.17. Είναι το ίδιο με το μήκος των δεδομένων του πακέτου Echo request.

1.18. Κάθε πληροφορία που τυπώνεται στη γραμμή εντολής από την εντολή ping είναι πληροφορία των πακέτων IPv4 που ανταλλάσσονται μεταξύ των δύο hosts. Οι χρόνοι που τυπώνονται αντιστοιχούν στον χρόνο που έκαναν τα πακέτα να φτάσουν στον απομακρυσμένο host και να επιστρέψουν.

1.19. ping <addr> -n 2

1.20. Στάλθηκαν 6 πακέτα ARP request.

1.21. Κάθε 1 sec.

1.22. Δεν στάλθηκε κανένα ICMP μήνυμα.

1.23. Στη γραμμή εντολών για κάθε αίτημα αναγράφεται "Destination Host Unreachable", πράγμα που επιβεβαιώνουμε και στο Wireshark καθώς δεν υπάρχουν ICMP πακέτα και όλα τα ARP πακέτα δεν έχουν απάντηση.

2. Εντολή ping σε άλλο υποδίκτυο

2.1.

```
Interface: 192.168.1.5 --- 0xb
  Internet Address      Physical Address      Type
  192.168.1.1           14-09-b4-d2-72-ff     dynamic
  192.168.1.2           20-c6-eb-e1-74-e8     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. Διεύθυνση MAC αποστολέα: f8:75:a4:a2:7c:b1, διεύθυνση MAC παραλήπτη: 14:09:b4:d2:72:ff.

2.3. Διεύθυνση IPv4 αποστολέα: 192.168.1.5, διεύθυνση IPv4 παραλήπτη: 147.102.40.1.

2.4. Η διεύθυνση MAC αποστολέα αντιστοιχεί στον προσωπικό μου υπολογιστή, ενώ η διεύθυνση παραλήπτη αντιστοιχεί στο σύστημα στο οποίο κάναμε ping.

2.5. Παρατήρησα 2 πακέτα ARP.

2.6. Το οικιακό router μου, με IPv4 192.168.1.1, ρώτησε τον υπολογιστή μου που έχει την IP 192.168.1.8 ποια είναι η διεύθυνση MAC του ώστε να γίνει η επίλυση από λογικές σε φυσικές διευθύνσεις και να ξέρει το router που μεσολαβεί στην επικοινωνία μεταξύ του υπολογιστή μου και της 147.102.40.1 την αντιστοιχία λογικών-φυσικών διευθύνσεων για να δρομολογήσει την επικοινωνία μεταξύ των 2 μελών.

2.7. Είναι "icmp.type == 0".

2.8. Παρατηρούμε ότι τόσο στην επικεφαλίδα IPv4 όσο και στη γραμμή εντολών η τιμή του TTL = 58. Επίσης γνωρίζουμε ότι η default τιμή του TTL = 64. Συνεπώς καταλαβαίνουμε ότι έγιναν 6 hops μέχρι να φτάσει το

πακέτο σε εμένα. Τρέχοντας και μια εντολή tracert 147.102.40.1 βλέπουμε ότι το router μου με IP 192.168.1.1 απέχει 6 κόμβους μακριά από τον στόχο.

2.9. Εμφανίζονται μόνο πακέτα Echo request, και όχι Echo reply.

2.10. Η διαφορά μεταξύ του ping εντός του υποδικτύου και εκτός αυτού είναι ότι στην πρώτη περίπτωση αποτυγχάνει η απάντηση της ανενεργής συσκευής στο ARP request και επομένως δεν γίνεται ping request. Στην δεύτερη περίπτωση όταν εκτελούμε ping εκτός του υποδικτύου, το ARP request επιτυγχάνει και το request αποστέλλεται στο Default Gateway (router) που είναι ο υπεύθυνος για την δρομολόγηση όμως δε λαμβάνεται reply από το άλλο άκρο αφού είναι ανενεργό.

3. Εντολή tracert/traceroute

3.1. Το μήκος του πεδίου δεδομένων των μηνυμάτων ICMP Echo request που παράγει η tracert είναι 64 bytes και το περιεχόμενο τους είναι 64 μηδενικά bytes.

3.2. Το μήκος είναι διπλάσιο από το αντίστοιχο της εντολής ping και το φορτίο αποτελείται από μηδενικά όχι από διαδοχικούς δεκαεξαδικούς αριθμούς.

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

3.4. Η τιμή των πεδίων Type και Code της επικεφαλίδας ICMP για τα πακέτα που περιέχουν μήνυμα λάθους είναι Type: 11, Code: 0.

3.5. Έχει επιπλέον τα πεδία Checksum (2 bytes) και Unused (4 bytes).

3.6. Το μήκος των δεδομένων είναι το μήκος της επικεφαλίδας IPv4 (20 bytes) + μήκος ICMP (8 bytes) = 28 bytes. Επιπλέον, το μήκος της επικεφαλίδας είναι το μήκος του Type (1 byte) + το μήκος του Code (1 byte) + το μήκος του Checksum (2 bytes) + το μήκος του Unused (4 bytes) = 8 bytes.

3.7. Το περιεχόμενο δεδομένων των πακέτων του προηγούμενου ICMP μηνύματος λάθους είναι η επικεφαλίδα IPv4 και τα 8 πρώτα bytes του ICMP Echo request.

4. Ανακάλυψη MTU διαδρομής (Path MTU Discovery)

4.1. Ξεκινώντας από 1472→1464→978→548 ICMP payload παρατηρούμε ότι μήκος πακέτου 548 Bytes είναι το πρώτο μήκος που επιτυγχάνει.

4.2. Όχι.

4.3. Δεν το παρήγαγε κάποιος κόμβος της διαδρομής.

4.4. Χρησιμοποιήθηκε το αρχείο mtu.pcap. Type: 3 (0x03), Code: 4 (0x04).

4.5. Το πεδίο Code: 4 (Fragmentation needed) δηλώνει ότι είναι απαραίτητος ο θρυμματισμός ενώ η τιμή του πεδίου MTU of next hop είναι 1492.

4.6. Περιέχει το περιεχόμενο του IPv4 του πακέτου που προκάλεσε αυτό το μήνυμα.

4.7. Για την τιμή MTU = 1492.

4.8. Εκτός από την τιμή MTU 1492 δεν λαμβάνουμε μήνυμα λάθους ICMP Destination Unreachable και για την τιμή MTU 1006 αλλά το 147.102.40.15 δεν απαντά.

4.9. Λαμβάνουμε απάντηση για τιμή MTU 576 bytes.

4.10. Η τιμή MTU είναι του προορισμού, όχι ενδιάμεσου κόμβου. Αν υπήρχε μικρότερη τιμή MTU προηγουμένως εφόσον έχουμε ρυθμίσει το flag ώστε να μην γίνεται fragmentation θα είχαμε δει μήνυμα λάθους πιο νωρίς που θα μας ενημέρωνε για την MTU που θα έπρεπε να χρησιμοποιηθεί για να προχωρήσουμε στο επόμενο βήμα. Συνεπώς ο ενδιάμεσος δρομολογητής θα έστελνε μήνυμα λάθους ICMP Destination Unreachable κάτι που δε συμβαίνει όμως.

4.11. Γιατί είναι ο τελικός κόμβος, επομένως δεν χρειάζεται να θρυματίσει το πακέτο.

4.12. Έχει μέγεθος 1464 bytes το οποίο είναι ακέραιο πολλαπλάσιο του 8 bytes.

5. Απρόσιτη θύρα (Port Unreachable)

5.1. Capture filter: "ip host 147.102.40.15"

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

5.3.

```
C:\Windows\system32>nslookup edu-dy.cn.ntua.gr 147.102.40.15
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  147.102.40.15

DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
*** Request to UnKnown timed-out
```

Παρατηρούμε απάντηση "DNS request timed out", δηλαδή το request δεν είχε αρκετά μεγάλο TTL.

5.4. Ναι, παρατηρήθηκαν 5 μηνύματα DNS.

5.5. Πρωτόκολλο μεταφοράς είναι το UDP και Destination Port η 53.

5.6. Ναι, παρατήρησα 5 τέτοια ICMP μηνύματα.

5.7. Οι τιμές των ζητούμενων πεδίων είναι: Type: 3 (Destination unreachable) και Code: 3 (Port unreachable).

5.8. Το πεδίο Code.

5.9. Προκύπτει από το γεγονός ότι στο ICMP μέρος του πακέτου που αποστέλλεται πίσω υπάρχει το UDP header του αρχικού DNS query και αναγράφει και τη θύρα προορισμού (53). Άλλωστε είναι γνωστό πως η θύρα 53 είναι προκαθορισμένη για χρήση DNS queries.

6. IPv6 και ICMPv6

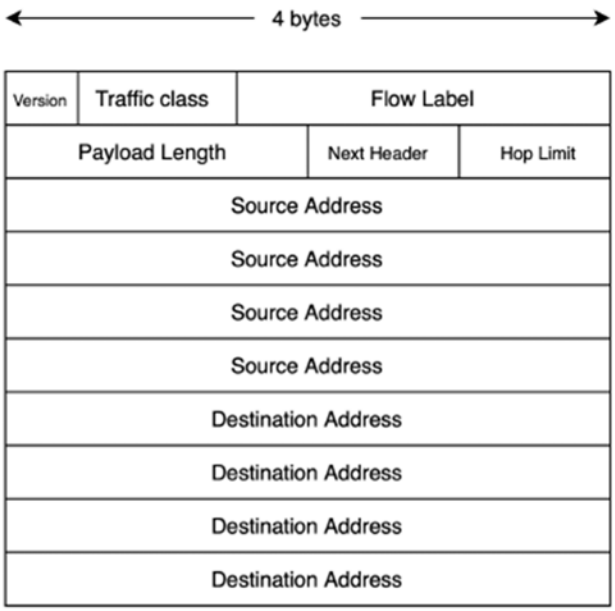
6.1. ping -6 2001:648:2000:329::101, tracert -6 2001:648:2000:329::101

6.2. Capture filter: ip6, Display filter: icmpv6

6.3. Type: IPv6 (0x86dd)

6.4. IPv6 Header : 40 bytes

6.5. Version, Traffic Class, Flow Label, Payload Length, Next Header, Hop Limit, Source Address, Destination Address



6.6. Hop Limit

6.7. Είναι η Next Header και η τιμή για ICMPv6 είναι 58 (0x3a).

6.8. Ναι είναι ίδια.

6.9. Type: Echo (ping) request (128) και μεταφέρει δεδομένα μήκους 32 bytes.
6.10. Ναι, η δομή του είναι ίδια.
6.11. Type: Echo (ping) reply (129) και μεταφέρει δεδομένα μήκους 32 bytes.
6.12. Διαφέρει στο μήκος δεδομένων που είναι ίσο με 64 bytes.
6.13. Δε διαφέρει στη δομή εκτός του πεδίου Unused που εδώ ονομάζεται Reserved στο ICMPv6.
6.14. Type: Time Exceeded (3) και το μήκος δεδομένων που μεταφέρει είναι 40 + 72 = 112 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.