3η Εργαστηριακή Άσκηση στα Δίκτυα Υπολογιστών

Ονοματεπώνυμο	Γεώργιος Στεφανάκης
Αρ. Μητρώου	el18436
Ομάδα	4
Λειτουργικό Σύστημα	Manjaro Linux x86_64
Διεύθυνση IP	147.102.201.238
Διεύθυνση MAC	b4:69:21:5e:da:03
Ημερομηνία	2022-10-19

1. Ο πίνακας ARP

1.1. arp -v

```
[giorgis@afousis ~]$ arp -v
Address                  HWtype  HWaddress           Flags Mask            Iface
147.102.203.254          ether   00:50:56:b5:aa:aa   C                     wlp2s0
147.102.201.223                  (incomplete)                              wlp2s0
_gateway                 ether   08:ec:f5:d0:d9:1d   C                     wlp2s0
147.102.203.191          ether   ec:be:5f:86:e9:4a   C                     wlp2s0
Entries: 4      Skipped: 0      Found: 4
[giorgis@afousis ~]$
```

1.2. arp -i INTERFACE_NAME -d IP_ADDR

1.3. Εκτελώντας ξανά την εντολή του ερωτήματος 1.1 με την σημαία -n, βλέπουμε την πραγματική IP αντί για το alias “_gateway” του default gateway, το οποίο είναι 147.102.200.200. Για τη διεύθυνση του DNS, πρέπει να κοιτάξουμε στο αρχείο /etc/resolv.conf. Είναι η IP 147.102.224.243.

1.4. Τα περιεχόμενα του πίνακα φαίνονται στην εικόνα του ερωτήματος 1.1.

1.5. Υπάρχει η διεύθυνση του default gateway αλλά οχι οι διευθύνσεις DNS.

1.6. Χρησιμοποίησα τη διεύθυνση 147.102.203.191.

1.7.

```
[giorgis@afousis ~]$ arp -vn
Address                  HWtype  HWaddress           Flags Mask            Iface
147.102.203.254          ether   00:50:56:b5:aa:aa   C                     wlp2s0
147.102.200.200          ether   08:ec:f5:d0:d9:1d   C                     wlp2s0
147.102.203.191          ether   ec:be:5f:86:e9:4a   C                     wlp2s0
Entries: 3      Skipped: 0      Found: 3
[giorgis@afousis ~]$
```

Παρατηρούμε ότι στο ARP table έχουν φορτωθεί ξανά η IP του default gateway, η IP την οποία χτυπήσαμε αλλά και η IP 147.102.203.254. Αυτή η διεύθυνση μάλλον έκανε στο δικό μου υπολογιστή ping, και για να απαντηθεί το αίτημα στον υπολογιστή του αποστολέα, έπρεπε να αποθηκευτεί στο ARP πίνακά μου και η δική του διεύθυνση.

1.8.

```
[giorgis@afousis ~]$ arp -vn
Address                  HWtype  HWaddress           Flags Mask            Iface
147.102.203.254          ether   00:50:56:b5:aa:aa   C                     wlp2s0
147.102.201.223                  (incomplete)                              wlp2s0
147.102.200.200          ether   08:ec:f5:d0:d9:1d   C                     wlp2s0
147.102.203.191          ether   ec:be:5f:86:e9:4a   C                     wlp2s0
Entries: 4      Skipped: 0      Found: 4
[giorgis@afousis ~]$
```

Παρατηρούμε ότι προστέθηκε και η διεύθυνση 147.102.201.223 στο ήδη υπάρχον ARP table. Αυτή η διεύθυνση αντιστοιχεί στη νέα σύνδεση στον εξυπηρετητή, ο οποίος επειδή βρίσκεται στο τοπικό δίκτυο του εργαστηρίου, δρομολογήθηκε από το ARP και προστέθηκε στον πίνακα.

1.9. Όπως αναφέρθηκε παραπάνω, επειδή η διεύθυνση του εξυπηρετητή (147.102.201.223) ανήκει στο τοπικό δίκτυο του εργαστηρίου, για να γίνει η ανταλλαγή πλαισίων έπρεπε να προηγηθεί επικοινωνία με τον DNS server ώστε να μάθει ο υπολογιστής την διεύθυνση που αντιστοιχεί στο domain της ερώτησης, και χρήση του ARP πρωτοκόλλου ώστε να ενημερωθεί ο ARP table και να μεταδωθεί broadcasting μήνυμα από τον προσωπικό μου υπολογιστή προς τους υπόλοιπους υπολογιστές του τοπικού δικτύου. Ο εξυπηρετητής έλαβε το μήνυμα και έστειλε στην διεύθυνση αιτήματος το HTTP response. Η διεύθυνση που προαναφέρθηκε αντιστοιχεί στο domain http://edu-dy.cn.ntua.gr/lab3.

2. Το πλαίσιο Ethernet

Σε αυτή την άσκηση συνδέθηκα με τη διεπαφή Ethernet μου από τον προσωπικό μου χώρο (MAC: 48:2a:e3:25:4d:ab, IPv4: 10.3.40.99).

2.1. Στο πλαίσιο Ethernet περιλαμβάνονται τα πεδία Source, Destination και Type.
2.2. Το προοίμιο δεν έχει καταγραφεί καθώς δεν περιέχει χρήσιμη πληροφορία. Απλά χρησιμεύει για να προλάβουν τα ηλεκτρονικά στοιχεία να ανιχνεύσουν την ύπαρξη σήματος και να αρχίσουν να διαβάζουν πριν αρχίσει η μετάδοση του πλαισίου.
2.3. Το CRC δεν καταγράφεται διότι το Wireshark καταγράφει μόνο αυτά που βρίσκονται στο πακέτο Packet Capture Library (libcap) των Windows. Απαιτείται κατάλληλη ρύθμιση στο λειτουργικό σύστημα.
2.4. Το πεδίο Type για πακέτα IPv4 έχει τιμή 0x0800 = 2048.
2.5. Το πεδίο Type για πακέτα ARP έχει τιμή 0x0806 = 2054.
2.6. Το πεδίο Type για πακέτα IPv6 έχει τιμή 0x86dd = 34525.
2.7. Η διεύθυνση MAC πηγής στο πλαίσιο Ethernet είναι εκείνη της συσκευής μου, δηλαδή 48:2a:e3:25:4d:ab.
2.8. Η διεύθυνση MAC προορισμού είναι η 04:d5:90:da:67:b0.
2.9. Όχι.
2.10. Ο server της σελίδας που ζητάμε βρίσκεται σε άλλο υποδίκτυο και συνεπώς η επικοινωνία μαζί του γίνεται μέσω της default gateway του router στο οποίο είμαι συνδεδεμένος.
2.11. Το μήκος όλου του πλαισίου είναι 480 bytes.
2.12. Προηγούνται 66 bytes (14 από το Ethernet, 20 από το IPv4, 32 από το TCP).
2.13. Η διεύθυνση αποστολέα είναι η ίδια με τη διεύθυνση προορισμού, 04:d5:90:da:67:b0.
2.14. Όχι
2.15. Ανήκει στην default gateway του router στο οποίο είμαι συνδεδεμένος όπως εξηγήσαμε και στο 2.10.
2.16. Η διεύθυνση MAC του παραλήπτη είναι η 48:2a:e3:25:4d:ab.
2.17. Η διεύθυνση αυτή ανήκει στον υπολογιστή μου.
2.18. Το πλαίσιο έχει συνολικό μήκος 599 bytes.
2.19. 14 bytes από το Ethernet + 20 bytes από το IPv4 + 32 bytes από το TCP + 13 bytes από το HTTP μέχρι πριν τον χαρακτήρα “Ο” = 79 bytes.

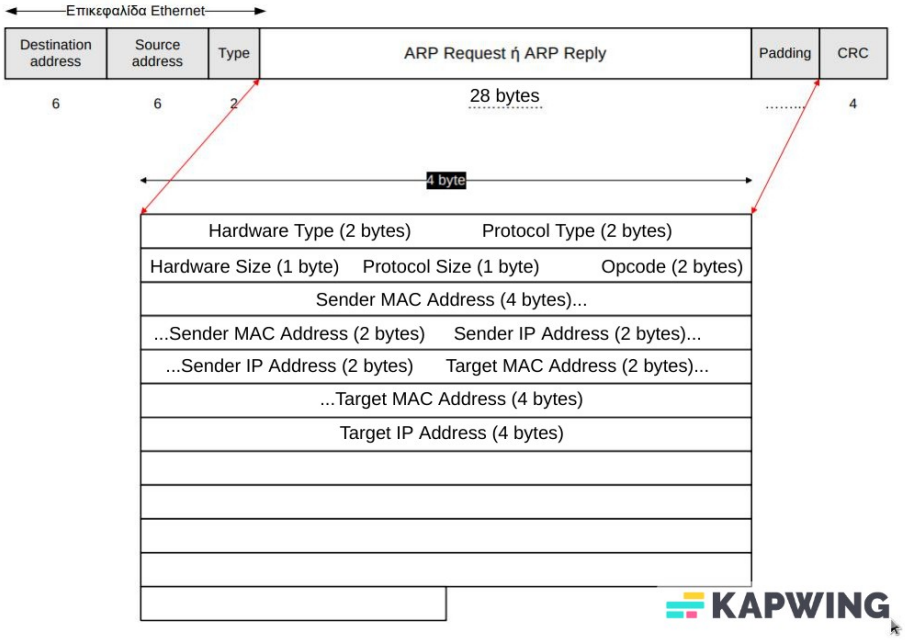
3. Περισσότερα για τα πλαίσια Ethernet

3.1. Οι διευθύνσεις MAC πηγής των πλαισίων Ethernet που καταγράψαμε είναι ατομικές (unicast) και είναι και μοναδικές (global).
3.2. Οι διευθύνσεις MAC προορισμού των πλαισίων Ethernet που καταγράψαμε είναι ομαδικές (multicast/broadcast) και κάποιες είναι μοναδικές (global) και κάποιες άλλες τοπικές (local).
3.3. Το πρώτο bit εμφανίζεται στη διεύθυνση MAC στο πρώτο byte στη θέση 8 και το δεύτερο bit εμφανίζεται αντιστοίχως στο 7ο bit του πρώτου byte της διεύθυνσης MAC.
3.4. Η διεύθυνση MAC για τα πλαίσια εκπομπής (broadcast) είναι ff:ff:ff:ff:ff:ff.
3.5. Με φίλτρο απεικόνισης llc παρατηρούμε ότι παραμένουν μόνο τα πλαίσια με πρωτόκολλο IEEE 802.3 Ethernet.
3.6. Το πεδίο μετά τις διευθύνσεις MAC στα πλαίσια IEEE 802.3 ονομάζεται Length και δηλώνει πόσα byte περιέχονται στο πεδίο δεδομένων.
3.7. Στα πλαίσια IEEE 802.3 αντί για το πεδίο Type υπάρχει το πεδίο Length και επιπλέον μετά το πεδίο Length υπάρχει το πεδίο LLC που προσδιορίζει το πρωτόκολλο του ανώτερου στρώματος το οποίο ενθυλακώνεται.
3.8. Η επικεφαλίδα LLC έχει μέγεθος 3 bytes και περιλαμβάνει τα πεδία DSAP, SSAP και Control Field.
3.9. Μεταφέρουν δεδομένα του Spanning Tree Protocol (STP) και το μέγεθός τους είναι 102 bytes.
3.10. Το padding έχει μέγεθος 7 bytes και υπάρχει γιατί το πρότυπο IEEE 802.3 ορίζει ότι το ελάχιστο μήκος πλαισίου είναι 64 bytes. Συνεπώς αν το πακέτο που ενθυλακώνεται στο πλαίσιο είναι μικρότερο από 46 bytes τότε κάνουμε padding μέχρι να φτάσει το ελάχιστο μήκος των 64 bytes.

4. Περισσότερα για τα πακέτα ARP

Σε αυτή την άσκηση συνδέθηκα με τη διεπαφή Ethernet μου από τον προσωπικό μου χώρο (MAC: 48:2a:e3:25:4d:ab, IPv4: 10.3.40.99).

4.1. Η εφαρμογή αυτού του φίλτρου έχει ως αποτέλεσμα να βλέπουμε τα πλαίσια στα οποία εμπλέκεται η διεύθυνση MAC του υπολογιστή μου είτε ως πηγή είτε ως παραλήπτης.
4.2. Η εφαρμογή του δεύτερου φίλτρου έχει ως αποτέλεσμα να περιορίζει τα πλαίσια του 3.1 σε αυτά που χρησιμοποιούν πρωτόκολλο ARP.
4.3. Ανταλλάχθηκαν 4 πακέτα ARP κατά την εκτέλεση της εντολής ping.
4.4. ο πεδίο του πλαισίου Ethernet που διαφοροποιεί τα πακέτα ARP από τα IPv4 είναι το πεδίο Type που για τα ARP έχει τιμή 0x0806 = 2054 ενώ για τα IPv4 έχει τιμή 0x0800 = 2048.
4.5. (Το padding είναι 18 bytes και αντιστοιχεί στις κενές γραμμές του πακέτου, όπως φαίνεται παρακάτω)



4.6. Hardware type: Ethernet (1).

4.7. Protocol type: IPv4 (0x0800 = 2048).
4.8. Το Protocol type είναι IPv4 (0x0800) ενώ το EtherType ARP (0x0806).
4.9. Η τιμή του Protocol Size έχει την τιμή 4 καθώς οι διευθύνσεις IPv4 έχουν μέγεθος 4 bytes.
4.10. Η τιμή του Hardware Size είναι 6 λόγω του ότι οι διευθύνσεις MAC έχουν μήκος 6 bytes.
4.11. Η διεύθυνση MAC του αποστολέα του πλαισίου Ethernet που μεταφέρει το ARP request είναι η MAC του υπολογιστή μου.
4.12. Η διεύθυνση MAC του παραλήπτη είναι η γενική ff:ff:ff:ff:ff:ff που αφορά μήνυμα broadcast δηλαδή όλους τους υπολογιστές του υποδικτύου.
4.13. Το πακέτο Ethernet έχει μήκος 14 bytes και το πακέτο ARP έχει μήκος 28 bytes.
4.14. Προηγούνται 20 bytes.
4.15. Η τιμή ARP opcode είναι Opcode: request (1).
4.16. Στο πεδίο Sender MAC Address.
4.17. Στο πεδίο Sender IP Address.
4.18. Στο πεδίο Target IP Address.
4.19. Υπάρχει το πεδίο Target MAC Address το οποίο έχει την τιμή 00:00:00:00:00:00, δηλαδή δεν έχει προσδιοριστεί ακόμα.
4.20. Η διεύθυνση MAC του αποστολέα ανήκει στον υπολογιστή που κάναμε ping ενώ η διεύθυνση MAC του παραλήπτη ανήκει στον υπολογιστή μου.
4.21. Η τιμή του opcode στο ARP reply είναι Opcode: reply (2).
4.22. Στο πεδίο Sender IP Address.
4.23. Στο πεδίο Sender MAC Address.
4.24. Στο πεδίο Target IP Address.
4.25. Στο πεδίο Sender MAC Address.
4.26. Το πακέτο Ethernet έχει μήκος 32 bytes και το πακέτο ARP έχει μήκος 28 bytes.
4.27. Εάν το πακέτο έχει Destination = Broadcast, τότε η Ethernet επικεφαλίδα έχει μήκος 14 bytes, όπως αναφέρθηκε στο 4.13. Αλλιώς, για πακέτο ARP με συγκεκριμένη διεύθυνση MAC για προορισμό, η Ethernet επικεφαλίδα έχει και εκείνη 32 bytes.
4.28. Το πεδίο Opcode που έχει τιμή 1 για request και 2 για reply.
4.29. Η διαφορά είναι ότι στα πακέτα ARP reply έχουμε και padding μέχρι να φτάσει το συνολικό μήκος του πακέτου στα 60 bytes (+4 για το CRC = 64 bytes). Το padding δεν υπάρχει στα πακέτα ARP request.
4.30. Τα πακέτα ARP request είναι broadcast καθώς αναφέροναι σε όλους τους υπολογιστές στο υποδίκτυο ενώ τα ARP reply είναι unicast αφού απευθύνονται από τον υπολογιστή με τη συγκεκριμένη IP στην οποία κάναμε ping στον δικό μας υπολογιστή. Επίσης μεταξύ των πακέτων ARP reply και ARP request παρατηρούμε ότι στο ARP reply στο πεδίο Sender MAC Address βρίσκεται η απάντηση της MAC Address που στο request στο πεδίο Target MAC Address είχε τιμή 00:00:00:00:00:00.
4.31. Σε αυτή την περίπτωση ο αιτών της διεύθυνσης MAC θα λάμβανε διπλή απάντηση και θα έκανε διπλή αντιστοίχηση της IP με MAC Address στον πίνακα ARP. Έτσι θα υπήρχε κίνδυνος να στέλνονται πακέτα σε λάθος MAC Address (στον κακόβουλο υπολογιστή) με αποτέλεσμα τα δεδομένα των υπόλοιπων χρηστών να είναι προσβάσιμα από τον κακόβουλο υπολογιστή.