Δίκτυα Υπολογιστών

Εργαστηριακή Άσκηση 3
Επικοινωνία στο τοπικό δίκτυο
(πλαίσιο Ethernet και πρωτόκολλο ARP)

Ονοματεπώνυμο: Νικόλαος Παγώνας, el18175	**Ομάδα:** 4 (Τρίτη εξ' αποστάσεως)
Όνομα PC/ΛΣ: nick-ubuntu/Ubuntu 20.04.3 LTS	**Ημερομηνία:** Τρίτη 26/10/2021
Διεύθυνση IP: `192.168.1.15`	**Διεύθυνση MAC:** `3c:2c:30:e1:1c:55`

Άσκηση 1

1.1

Με την εντολή `ip neigh show` παίρνουμε:

```
~ ❯ ip neigh show
192.168.1.9 dev enp2s0 lladdr 00:51:ed:28:70:bc STALE
169.254.169.254 dev enp2s0  FAILED
192.168.1.1 dev wlp3s0 lladdr e0:0e:e4:59:40:50 STALE
192.168.1.9 dev wlp3s0 lladdr 00:51:ed:28:70:bc STALE
192.168.1.1 dev enp2s0 lladdr e0:0e:e4:59:40:50 DELAY
fe80::1 dev enp2s0 lladdr e0:0e:e4:59:40:50 router REACHABLE
fe80::1 dev wlp3s0 lladdr e0:0e:e4:59:40:50 router STALE
```

1.2

Με την εντολή `ip neigh flush all` μπορούμε να διαγράψουμε τα περιεχόμενα του πίνακα ARP, όπως φαίνεται παρακάτω:

```
~ ❯ sudo ip neigh flush all && ip neigh show
~ ❯
```

Αμέσως μετά το `ip neigh flush all` εκτελέσαμε `ip neigh show` και πήραμε κενή έξοδο, άρα διαγράψαμε τα περιεχόμενα του πίνακα ARP με επιτυχία.

1.3

Με τις εντολές `ip route | grep default` και `resolvectl` βρίσκουμε:
Την διεύθυνση IPv4 της προκαθορισμένης πύλης:

```
~ ❯ ip route | grep default
default via 192.168.1.1 dev enp2s0 proto dhcp metric 100
default via 192.168.1.1 dev wlp3s0 proto dhcp metric 600
```

και την διεύθυνση IPv4 των εξυπηρετητών DNS του υπολογιστή μας:

```
Link 2 (enp2s0)
      Current Scopes: DNS
DefaultRoute setting: yes
       LLMNR setting: yes
MulticastDNS setting: no
  DNSOverTLS setting: no
      DNSSEC setting: no
    DNSSEC supported: no
  Current DNS Server: 192.168.1.1
         DNS Servers: 192.168.1.1
          DNS Domain: ~.
                      home
```

Βλέπουμε ότι είναι ίδιες (`192.168.1.1`)

1.4

```
~ ❯ ip neigh show
192.168.1.6 dev enp2s0 lladdr a4:97:b1:dc:ba:f9 REACHABLE
192.168.1.1 dev enp2s0 lladdr e0:0e:e4:59:40:50 REACHABLE
fe80::1 dev enp2s0 lladdr e0:0e:e4:59:40:50 router REACHABLE
fe80::1 dev wlp3s0 lladdr e0:0e:e4:59:40:50 router STALE
```

1.5

Παρατηρούμε ότι η διεύθυνση της προκαθορισμένης πύλης και των εξυπηρετητών DNS (`192.168.1.1`) βρίσκεται στον πίνακα.

1.6

Αδειάζουμε τον πίνακα ARP με την εντολή `ip neigh flush all` και στην συνέχεια εκτελούμε `ping 192.168.1.6`.

1.7

Αν ξαναεμφανίσουμε τον πίνακα ARP με την εντολή `ip neigh show`, παρατηρούμε ότι η διεύθυνση που κάναμε `ping` ξαναεμφανίστηκε.

1.8

Έχουν καταχωρηθεί τόσο η διεύθυνση του DNS Server, όσο και του default gateway (αφού είναι ίδιες).

1.9

Βλέπουμε ότι η διεύξυνση IPv4 του `edu-dy.cn.ntua.gr` δεν έχει καταχωρηθεί στον πίνακα ARP, αφού βρίσκεται σε διαφορετικό υποδίκτυο.

Άσκηση 2

2.1

Καταγράφει τα πεδία `Destination MAC Address`, `Source MAC Address` και `Type`.

2.2

Το προοίμιο δεν έχει καταγραφεί, αφού δεν ανήκει στο **πλαίσιο** Ethernet.

2.3

Όπως ξέρουμε, το Wireshark χρησιμοποιεί μία βιβλιοθήκη pcap και άρα έχει πρόσβαση στις δυνατότητες της βιβλιοθήκης αυτής. Τα περισσότερα λειτουργικά συστήματα όμως **δεν** υποστηρίζουν την καταγραφή του CRC. Ακόμα κι αν την υποστηρίζουν, χρειάζεται ειδικό configuration. Επομένως, είναι λογικό να μην καταγράφεται το CRC.

2.4

Η τιμή του πεδίου Type της επικεφαλίδας Ethernet για πακέτα IPv4 είναι `0x0800`.

2.5

Για πακέτα ARP, η τιμή του Type είναι `0x0806`.

2.6

Για πακέτα IPv6, η τιμή του Type είναι `0x86dd`.

2.7

Η διεύθυνση MAC της πηγής του πλαισίου είναι `3c:2c:30:e1:1c:55`.

2.8

Η διεύθυνση MAC του προορισμού του πλαισίου είναι `e0:0e:e4:59:40:50`.

2.9

Η παραπάνω διεύθυνση MAC δεν είναι αυτή του `edu-dy.cn.ntua.gr`.

2.10

Με την εντολή `ip neigh show` βλέπουμε ότι η διεύθυνση MAC ανήκει στο Router του τοπικού μας δικτύου (2η γραμμή).

```
~ ❯ ip neigh show
192.168.1.9 dev enp2s0 lladdr 00:51:ed:28:70:bc STALE
192.168.1.1 dev enp2s0 lladdr e0:0e:e4:59:40:50 DELAY
fe80::1 dev enp2s0 lladdr e0:0e:e4:59:40:50 router DELAY
fe80::1 dev wlp3s0 lladdr e0:0e:e4:59:40:50 router STALE
```

Αυτό είναι λογικό, αφού η διεύθυνση του `edu-dy.cn.ntua.gr` είναι εκτός του υποδικτύου στο οποίο βρισκόμαστε, και άρα η επικοινωνία γίνεται μέσω του router.

2.11

Το μήκος του πλαισίου είναι 588 bytes.

2.12

Προηγούνται συνολικά 66 bytes.

2.13

Η διεύθυνση MAC του αποστολέα είναι η `e0:0e:e4:59:40:50`.

2.14

Η παραπάνω διεύθυνση δεν είναι η διεύθυνση MAC του `edu-dy.cn.ntua.gr`.

2.15

Η διεύθυνση αυτή είναι και πάλι η διεύθυνση του router του τοπικού μας δικτύου.

2.16

Η διεύθυνση MAC του παραλήπτη είναι `3c:2c:30:e1:1c:55`.

2.17

Η διεύθυνση αυτή ανήκει στον υπολογιστή μας.

2.18

Το μήκος του πλαισίου είναι 549 bytes.

2.19

Προηγούνται πάλι 66 bytes.

Άσκηση 3

3.1

Παρατηρούμε ότι οι διευθύνσεις MAC πηγής των πλαισίων Ethernet είναι individual και globally unique.

3.2

Παρατηρούμε ότι οι διευθύνσεις MAC προορισμού των πλαισίων Ethernet είναι group, ενώ όσον αφορά το LG έχουμε και locally administered και globally unique

3.3

Το πρώτο bit της διεύθυνσης MAC (IG bit) εμφανίζεται στην 8η θέση του πρώτου byte (δηλαδή στο LSB) (`____ ___x`), ενώ το δεύτερο bit (LG bit) εμφανίζεται στην 7η θέση (`____ __x_`).

3.4

Η διεύθυνση MAC για τα πλαίσια εκπομπής (broadcast) είναι `ff:ff:ff:ff:ff:ff`.

3.5

Παραμένουν πλαίσια IEEE 802.3 (περιέχουν επικεφαλίδα **L**ogical **L**ink **C**ontrol, εξού και το όνομα του φίλτρου).

3.6

Στα πλαίσια IEEE 802.3, το πεδίο μετά τις διευθύνσεις MAC (`Length`) δηλώνει πόσα byte περιέχονται στο πεδίο δεδομένων.

3.7

Τα πλαίσια IEEE 802.3 ξεχωρίζουν από τα Ethernet II ως εξής:

- Στο Wireshark το πλαίσιο αναγράφεται ως IEEE 802.3 αντί για Ethernet II
- Στη θέση του πεδίου `Type` (Ethernet II) βρίσκεται το πεδίο `Length` (IEEE 802.3), το οποίο ξεχωρίζει διότι οι τιμές του πεδίου `Type` είναι μεγαλύτερες από 1536 (0x0600)
- Μετά το *Μήκος*, τα πλαίσια IEEE 802.3 περιέχουν μία επικεφαλίδα LLC, όπως αναφέρεται και στην θεωρία.

3.8

Η επικεφαλίδα LLC έχει μέγεθος 3 byte και περιλαμβάνει τα πεδία `DSAP`, `SSAP` και `Control Field`.

3.9

Του Spanning Tree Protocol, 36 bytes

3.10

Το παραγέμισμα έχει μήκος 7 bytes και υπάρχει σε περιπτώσεις που τα πλαίσια είναι πολύ μικρά, ώστε να ικανοποιείται το πρότυπο IEEE 802.3, το οποίο υπαγορεύει ελάχιστο μήκος πλαισίου 64 bytes.

Άσκηση 4

Σημείωση: Επειδή το μηχάνημα που χρησιμοποιήσαμε στην άσκηση 1 δεν ήταν διαθέσιμο κατά την διάρκεια εκτέλεσης της Άσκησης 4, χρησιμοποιήσαμε μία άλλη συσκευή με IPv4 address 192.168.1.7.

4.1

Η εφαρμογή αυτού του φίλτρου έχει αποτέλεσμα να δείχνει μόνο τα πακέτα που έστειλε/έλαβε η κάρτα δικτύου μας.

4.2

Η εφαρμογή του δεύτερου φίλτρου περιορίζει περαιτέρω το αποτέλεσμα του πρώτου, με τον επιπλέον συνθήκη ότι τα πακέτα πρέπει να ενθυλακώνουν το πρωτόκολλο ARP.

4.3

Ανταλλάχθηκαν 2 πακέτα.

4.4

Το πεδίο που τα διαφοροποιεί είναι το Type (έχει τιμή `0x0806`)

4.5

- Hardware Type: 2 bytes
- Protocol Type: 2 bytes
- Hardware Size: 1 byte
- Protocol Size: 1 byte
- Opcode: 2 bytes
- Sender MAC Address: 6 bytes
- Sender IP Address: 4 bytes
- Target MAC Address: 6 bytes
- Target IP Address: 4 bytes
- Padding: 18 bytes

4.6

Η τιμή του πεδίου `Hardware Type` είναι 1 και υποδεικνύει κάρτα δικτύου Ethernet.

4.7

Η τιμή του πεδίου `Protocol Type` είναι `0x0800` και υποδεικνύει πρωτόκολλο IPv4

4.8

Υπάρχει 1-1 αντιστοιχία, για παράδειγμα αν η τιμή του πεδίου `Protocol Type` είναι `0x0800`, τότε και η αντίστοιχη τιμή του πεδίου `EtherType` θα είναι `0x0800`.

4.9

Η τιμή του πεδίου `Protocol Size` έχει την τιμή 4, διότι έχουμε να κάνουμε με IPv4 πακέτα, και οι IPv4 διευθύνσεις έχουν μήκος 4 bytes.

4.10

Αντίστοιχα, η τιμή του πεδίου `Hardware Size` είναι 6, διότι οι MAC διευθύνσεις έχουν μήκος 6 bytes.

4.11

Η διεύθυνση MAC αποστολέα του πλαισίου Ethernet που μεταφέρει το ARP Request ανήκει στον υπολογιστή μας.

4.12

Η διεύθυνση MAC του παραλήπτη είναι `ff:ff:ff:ff:ff:ff`.

4.13

Το συνολικό μέγεθος του πακέτου ARP Request είναι 28 bytes, ενώ του πλαισίου Ethernet που το μεταφέρει είναι 42 bytes.

4.14

Προηγούνται 20 bytes.

4.15

Η τιμή του πεδίου opcode στο ARP Request είναι 1.

4.16

Περιέχεται στο Sender MAC Address.

4.17

Περιέχεται στο Sender IP Address.

4.18

Περιέχεται στο Target IP Address.

4.19

Υπάρχει το Target MAC Address, με τιμή `00:00:00:00:00:00`.

4.20

Η διεύθυνση MAC του αποστολέα ανήκει στο μηχάνημα που κάναμε ping, ενώ του παραλήπτη ανήκει στο δικό μας μηχάνημα.

4.21

Η τιμή του πεδίου opcode στο ARP Reply είναι 2.

4.22

Περιέχεται στο Sender IP Address.

4.23

Περιέχεται στο Sender MAC Address.

4.24

Περιέχεται στο Target IP Address.

4.25

Περιέχεται στο Sender MAC Address.

4.26

Το συνολικό μέγεθος σε byte του πακέτου ARP Reply είναι 28 bytes, ενώ του πλαισίου Ethernet που το μεταφέρει 60 bytes.

4.27

Παρατηρούμε ότι δεν είναι ίδια.

4.28

Στην περίπτωση που στέλνουμε το ARP Request, το padding γίνεται ακριβώς πριν μεταδοθεί το πακέτο, επομένως το Wireshark δεν μπορεί να το καταγράψει. Αντιθέτως, όταν λαμβάνουμε το ARP Reply, το padding έχει ήδη γίνει από την πλευρά του αποστολέα, οπότε το Wireshark το καταγράφει. Γι' αυτό έχουμε διαφορές στο μέγεθος πακέτου μεταξύ των δύο περιπτώσεων.

4.29

Το πεδίο opcode (1 για request, 2 για reply)

4.30

Στο request έχουμε multicast/broadcast και locally administered address, ενώ στο reply έχουμε globally unique address και unicast (πάντα μιλάμε για το Destination).

4.31

Τότε όλοι οι χρήστες θα έστελναν τα πακέτα τους στον κακόβουλο χρήστη, νομίζοντας ότι τα στέλνουν εκεί που αρχικά ήθελαν, θέτοντας σε κίνδυνο τα δεδομένα τους.