

ΓΕΩΡΓΑΚΟΠΟΥΛΟΣ ΓΕΩΡΓΙΟΣ 03120827

ΑΝΑΦΟΡΑ 3ΗΣ ΕΡΓΑΣΤΗΡΙΑΚΗΣ ΑΣΚΗΣΗΣ

Ομάδα: 2

Λογισμικό: Linux Ubuntu 20.04

Όνομα PC: glaptop

Διεύθυνση IP: 147.102.201.188

Διεύθυνση MAC: 70:9c:d1:03:b0:15

ΑΣΚΗΣΗ 1: Ο Πίνακας ARP

1.1 Βλέπουμε τα περιεχόμενα του πίνακα ARP με την εντολή `arp -n`

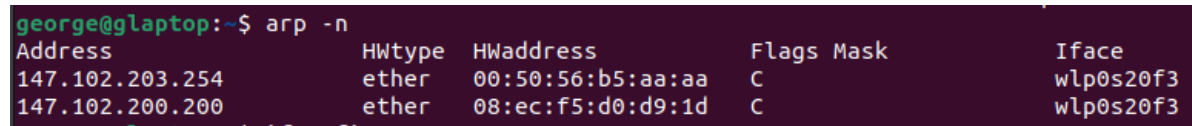
1.2 Διαγράφουμε τα περιεχόμενα του πίνακα ARP με την εντολή `sudo ip -s -s neigh flush all`

1.3 Διευθύνσεις IPv4:

Εντολή: `netstat -rn` και δίνει 147.102.200.200 (Default Gateway)

Εντολή: `resolvectl status` και δίνει 147.102.224.243 (DNS)

1.4



Address	HWtype	HWaddress	Flags	Mask	Iface
147.102.203.254	ether	00:50:56:b5:aa:aa	C		wlp0s20f3
147.102.200.200	ether	08:ec:f5:d0:d9:1d	C		wlp0s20f3

1.5 Ναι, υπάρχει η διεύθυνση της προκαθορισμένη πύλης.

1.6 `ping 147.102.203.254`

1.7 Πλεον στον arp πίνακα περιέχεται ξανά και αυτή η διεύθυνση, μαζί και με τα υπόλοιπα στοιχεία.

1.8 Υπάρχει μόνο η default gateway λόγω της επίσκεψης στην ιστοσελίδα της σχολής. (Σημειώνουμε ότι ο DNS server βρίσκεται σε άλλο τοπικό δίκτυο και αρα δεν θα πρέπει να φαίνεται στον πίνακα μας η διεύθυνση του.)

1.9 Όχι γιατί βρίσκεται σε άλλο υποδίκτυο και στον πίνακα θα καταχωρηθεί μόνο η MAC του default gateway που παρεμβάλλεται ενδιάμεσα.

ΑΣΚΗΣΗ 2: Το πλαίσιο Ethernet

2.1 Το wireshark καταγράφει τα πεδία Destination, Source και Type

2.2 Όχι το προοίμιο δεν έχει καταγραφεί γιατί δεν ανήκει στο πλαίσιο Ethernet

2.3 Το FCS δεν καταγράφεται από το wireshark

2.4 Η τιμή του πεδίου type για IPv4 είναι: 0x0800

2.5 Η τιμή του πεδίου type για ARP είναι: 0x0806

- 2.6 Δεν καταγράφηκαν πακέτα IPv6. Εάν είχαν καταγραφεί η τιμή του type θα ήταν 0x86DD
- 2.7 Η διεύθυνση MAC πηγής του πλαισίου είναι: 70:9c:d1:03:b0:15 (MAC της κάρτας δικτύου μου)
- 2.8 Η διεύθυνση MAC προορισμού του πλαισίου είναι: 08:ec:f5:d0:d9:1d
- 2.9 Όχι, η παραπάνω διεύθυνση MAC δεν είναι αυτή του edu-dy.cn.ntua.gr
- 2.10 Η MAC διεύθυνση αυτή ανήκει στον default gateway, γιατί αυτός θα αναλάβει την επίλυση διευθύνσεων MAC, αφού η διεύθυνση που επιζητούμε ανήκει σε διαφορετικό τοπικό δίκτυο.
- 2.11 Το μήκος του πλαισίου είναι 858 bytes.
- 2.12 Πριν το χαρακτήρα G του GET προηγούνται τoσα bytes όσο το αθροισμα των επικεφαλίδων. Αρα συνολικά 66bytes.
- 2.13 Η διεύθυνση MAC του αποστολέα είναι 08:ec:f5:d0:d9:1d
- 2.14 Όχι, η παραπάνω διεύθυνση MAC δεν είναι αυτή του edu-dy.cn.ntua.gr
- 2.15 Είναι η MAC του default gateway και ναι είναι η ίδια με το ερώτημα 2.10
- 2.16 Η διεύθυνση MAC του παραλήπτη είναι: 70:9c:d1:03:b0:15
- 2.17 Είναι η MAC της κάρτας δικτύου μου
- 2.18 Το μήκος του πλαισίου είναι 596 bytes
- 2.19 Πριν τον χαρακτήρα ASCII "O" της λέξης OK προηγούνται 79 bytes (Επικεφαλίδες + 13 bytes)

ΑΣΚΗΣΗ 3: Περισσότερα για τα πλαίσια Ethernet

**Σε αυτή την άσκηση θα χρησιμοποιήσουμε το αρχείο lab3.pcap που κατεβάσαμε.*

- 3.1 Οι διευθύνσεις MAC πηγής είναι Ατομικές (1ο LSB) και Μοναδικές (2ο LSB)
- 3.2 Οι διευθύνσεις MAC προορισμού είναι Ομαδικές (1ο LSB) και Τοπικές (2ο LSB)
- 3.3 Η μεταδοση γίνεται από αριστερά προς τα δεξιά, αρα στο πρώτο byte το πρώτο bit της διεύθυνσης MAC εμφανίζεται στην 8η θέση, είναι δηλαδή το 1ο LSB και το επόμενο του εμφανίζεται στην 7η θέση
- 3.4 Για τα πλαίσια εκπομπής η διεύθυνση MAC είναι: ff::ff::ff::ff::ff (Δηλαδή όλα άσσοι)
- 3.5 Εφαρμόζοντας φίλτρο απεικόνισης llc παρατηρούμε ότι παραμένουν μόνο τα πλαίσια που ακολουθούν το πρότυπο IEEE 802.3 Ethernet (STP πλαίσια)
- 3.6 Σε αυτό το πρότυπο, το πεδίο μετά τις διευθύνσεις MAC είναι το Length και δηλώνει το μήκος του πακέτου εκτός της επικεφαλίδας Ethernet (και το padding).
- 3.7 Τα πλαίσια IEEE 802.3 από τα Ethernet II ξεχωρίζουν λόγω των διαφορετικών πεδίων του. Το Ethernet II έχει Destination, Source και Type ενώ το IEEE 802.3 έχει Destination, Source, Length και Padding

- 3.8** Το μέγεθος της επικεφαλίδας LLC είναι 3 bytes και περιλαμβάνει τα πεδία DSAP, SSAP και Control Field
- 3.9** Τα πλαίσια IEEE 802.3 μεταφέρουν δεδομένα πρωτοκόλλου STP (Spanning Tree Protocol) και αυτά έχουν μέγεθος 36 bytes ($\text{Length-LLC} = 39 - 3 = 36$)
- 3.10** Το παραγέμισμα (padding) έχει μέγεθος 7 bytes και υπάρχει ώστε να συμπληρωθεί το ελάχιστο μήκος πλαισίου Ethernet (Περίπτωση όπου το πακέτο που ενθυλακώνεται στο πλαίσιο είναι μικρότερο από 46 byte)

ΑΣΚΗΣΗ 4: Περισσότερα για τα πλαίσια ARP

- 4.1** Το φίλτρο αυτό εμφανίζει μόνο τα πακέτα Ethernet που έχει στείλει ή λάβει ο υπολογιστής μου
- 4.2** Μετά το δεύτερο φίλτρο βλέπουμε μόνο τα πακέτα ARP που έχει στείλει ή λάβει ο υπολογιστής μου
- 4.3** Ανταλλάχθηκαν 4 πακέτα ARP
- 4.4** Το πλαίσιο type διαφοροποιεί τα ARP πακέτα από τα IPv4
- 4.5** ARP πακέτο:
- 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)
- 4.6** Η τιμή του πεδίου Hardware Type είναι 0x0001 και υποδικνύει Ethernet κάρτα δικτύου
- 4.7** Η τιμή του πεδίου Protocol Type είναι 0x0800 και υποδικνύει IPv4
- 4.8** Και οι δύο αυτές τιμές έχουν κοινό 2ο byte (08) αλλά διαφορετικό 1ο byte (00 για το IPv4 του Protocol Type του ARP πακέτου και 06 για το ARP του Type της Ethernet επικεφαλίδας)
- 4.9** Η τιμή του πεδίου Protocol size έχει την τιμή 4 γιατί δηλώνει το μήκος της διεύθυνσης IPv4
- 4.10** Η τιμή του πεδίου Hardware size έχει την τιμή 6 γιατί δηλώνει το μήκος της MAC διεύθυνσης
- 4.11** Η διεύθυνση MAC αποστολέα του πλαισίου Ethernet που μεταφέρει το ARP request ανήκει στον δικό μου υπολογιστή.
- 4.12** Η διεύθυνση MAC παραλήπτη που πλαισίου αυτού με βάση το πεδίο Destination του Ethernet είναι ff::ff::ff::ff::ff::ff (εφόσον πρόκειται για broadcast)
- 4.13** Το συνολικό μέγεθος του πακέτου ARP request είναι 28 bytes ενώ του πλαισίου Ethernet που το μεταφέρει είναι 42 bytes (συνολικά)

- 4.14** Από το πεδίο opcode του ARP request προηγούνται συνολικά 20 bytes
- 4.15** Η τιμή του πεδίου opcode του ARP request είναι 0x0001
- 4.16** Η διεύθυνση MAC του αποστολέα περιέχεται στο πεδίο Sender MAC address
- 4.17** Η διεύθυνση IPv4 του αποστολέα περιέχεται στο πεδίο Sender IP address
- 4.18** Η ερώτηση, δηλαδή, η διεύθυνση IPv4 του υπολογιστή του οποίου αναζητείται η διεύθυνση MAC, περιέχεται στο πεδίο Target IP address
- 4.19** Στο πακέτο ARP request υπάρχει πεδίο για τη ζητούμενη διεύθυνση MAC και περιέχει την τιμή 00:00:00:00:00:00
- 4.20** Η διεύθυνση MAC του αποστολέα ανήκει στον υπολογιστή του οποίου την διεύθυνση χρησιμοποιήσαμε στο ping. διεύθυνση MAC του παραλήπτη ανήκει στον δικό μου υπολογιστή (70:9c:d1:03:b0:15)
- 4.21** Η τιμή του πεδίου opcode του ARP reply είναι 0x0002
- 4.22** Η διεύθυνση IPv4 του αποστολέα περιέχεται στο πεδίο Sender IP address
- 4.23** Η διεύθυνση MAC του αποστολέα περιέχεται στο πεδίο Sender MAC address
- 4.24** Η διεύθυνση IPv4 του παραλήπτη περιέχεται στο πεδίο Target IP address
- 4.25** Η απάντηση, δηλαδή η διεύθυνση MAC του υπολογιστή που έχει τη διεύθυνση IPv4 για την οποία έγινε η ερώτηση, περιέχεται στο πεδίο Sender MAC address του ARP reply
- 4.26** Το συνολικό μέγεθος του πακέτου ARP reply είναι 28 bytes ενώ του πλαισίου Ethernet που το μεταφέρει είναι 60 bytes (συνολικά, εφόσον έχουμε και 18 bytes padding)
- 4.27** Για το ARP πακέτο ναι, η απάντηση είναι ίδια με το 4.13 αλλά για το συνολικό μήκος του πλαισίου ethernet όχι καθώς στο reply έχουμε και padding. Αν δεν υπήρχε το padding οι τιμές θα ήταν ίδιες.
- 4.28** Το πεδίο που υποδεικνύει το κατά πόσον πρόκειται για πακέτο ARP request ή ARP reply είναι το opcode (1 για request και 2 για reply)
- 4.29** Το διαφορετικό μέγεθος των ARP request και reply προκύπτει λόγω του padding στο τέλος του πακέτου, ώστε να συμπληρωθεί το ελάχιστο μήκος πακέτου. Η βιβλιοθήκη nrcap του Wireshark δεν πιάνει το padding (που προκύπτει κατά την μετάδοση) στα ARP request πακέτα καθώς συλλαμβάνει τα απερχόμενα πλαίσια πρώτου μεταδοθούν.
- 4.30** Τα πλαίσια για πακέτα ARP request και ARP reply διαφέρουν στο padding στο τέλος, στο opcode και στην MAC διεύθυνση του target, η οποία κατά το request είναι άγνωστη.
- 4.31** Εάν ένας κακόβουλος υπολογιστής στο τοπικό δίκτυο απαντούσε σε όλα τα ARP request δίνοντας τη δική του διεύθυνση MAC, τότε κάθε request θα είχε 2 reply. Έτσι στους πίνακες ARP των υπολογιστών του τοπικού δικτύου, για κάθε διεύθυνση IP θα υπήρχαν 2 MAC διευθύνσεις και έτσι ότι στέλνόταν σε αυτό το δίκτυο θα το λάμβανε και ο κακόβουλος υπολογιστής.