# ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ Ακ. έτος 2023-2024 9ο εξάμηνο, Φοιτητής: Αναστασιάδης Βασίλειος ΑΜ:03119954

## Επικοινωνία στο τοπικό δίκτυο (πλαίσιο Ethernet και πρωτόκολλο ARP)

### Άσκηση 1: Ο Πίνακας ARP

1. arp -n
2. sudo ip neigh flush all
3. ip route | grep default (default via 192.168.188.70 dev enx7e6f5a760fcc proto dhcp metric 100)  cat /etc/resolv.conf (nameserver 127.0.0.53)
4. 
```
vasilis@vasilis-Inspiron-5570:~$ sudo arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.188.70           ether   52:40:7b:58:10:80   C                     enx6a030085e87a
147.102.200.200          ether   08:ec:f5:d0:d9:1d   C                     wlp3s0
147.102.200.110          ether   ec:2e:98:5c:19:1f   C                     wlp3s0
147.102.202.9            ether   b4:b5:b6:74:b1:3d   C                     wlp3s0
147.102.203.254          ether   00:50:56:b5:aa:aa   C                     wlp3s0
```
5. Υπάρχει της προκαθορισμένης πύλης 192.168.188.78-> 62:f5:d0:bf:00:a5
6. ping  147.102.202.9
7. Παρατηρώ ότι ξαναεμφανίστηκε στο arp table η διεύθυνση IPv4 στην οποία έκανα ping μαζί με τη διεύθυνση του default gateway
8. Έχει καταχωρηθεί μόνο η διεύθυνση του gateway γιατί μόνο αυτή χρειάστηκε για την επικοινωνία με το διαφορετικό υποδίκτυο της σελίδας
9. Όχι γιατί βρίσκεται σε διαφορετικό υποδίκτυο, και η επικοινωνία με τα άλλα υποδίκτυα γίνεται μόνο μέσω του δρομολογητή

### Άσκηση 2: Το πλαίσιο Ethernet

1. Destination, Source, Type.
2. Όχι γιατί χρειάζεται μόνο για τον συγχρονισμό
3. Το packet capture library - libpcap του λειτουργικού συστήματος δεν μπορεί να “πιάσει” τα FCS των πλαισίων ethernet
4. 0x0800
5. 0x0806
6. Δεν καταγραφηκαν
7. Source: d2:04:c7:69:95:bf
8. Destination: 4e:34:16:d4:47:d3
9. Όχi

10. Στο δρομολογητή(gateway) γιατί η διεύθυνση της σελίδας βρίσκεται σε διαφορετικό υποδίκτυο οπότε η επικοινωνία πρέπει να γίνει μέσω του δρομολογητή
11. 441 bytes
12. 66 bytes
13. Source: 4e:34:16:d4:47:d3
14. Όχι
15. Στο δρομολογητή(gateway) γιατί η διεύθυνση της σελίδας βρίσκεται σε διαφορετικό υποδίκτυο οπότε η επικοινωνία πρέπει να γίνει μέσω του δρομολογητή, δηλαδη στην ιδια με το ερωτημα 2,10
16. Destination: d2:04:c7:69:95:bf
17. Στον δικό μου
18. 1010 bytes
19. 80 bytes

## Άσκηση 3: Περισσότερα για τα πλαίσια Ethernet

1. Ατομικές και μοναδικές
2. Ομαδικές και μοναδικές
3. Στην πρώτη το πρώτο και στην δέκατη το δεύτερο bit καθώς μεταδίδονται από LSB σε MSB κάθε byte
4. ff:ff:ff:ff:ff:ff
5. IEEE 802.3 Ethernet
6. Το πεδίο Length δηλώνει πόσα byte περιέχονται στο πεδίο δεδομένων
7. Στα πλαίσια IEEE 802.3, το πεδίο "Type/Length" χρησιμοποιείται για το μήκος του πλαισίου σε αντίθεση με το πεδίο "Type" του Ethernet II όπου χρησιμοποιείται για τον τύπο δεδομένων που μεταφέρει το πλαίσιο.
8. 3 bytes και έχει τα πεδία DSAP, SSAP, Control Field
9. Μεταφέρουν Δεδομένατου Spanning Tree Protocol(stp) καιέχουν μέγεθος 36 bytes
10. Έχει μέγεθος 7 bytes και υπάρχει για να εξασφαλίζει το ελάχιστο μέγεθος πλαισίου (των 64 byte)

## Άσκηση 4: Περισσότερα για τα πακέτα ARP

1. Εμφανίζει όλα τα πακέτα που έχουν πλαίσια ethernet με source ή destination την MAC address της κάρτας δικτύου του υπολογιστή μου
2. Εμφανίζει μόνο τα πλαίσια ARP του προηγούμενου φίλτρου
3. Who has 192.168.2.4? Tell 192.168.2.11 , 192.168.2.4 is at 30:24:78:7a:24:39
4. Το πεδίο Type που είναι 0x0800 στα IPv4 και 0x0806 στα πακέτα ARP
5. Hardware type(2 bytes) , Protocol type (2 bytes), Hardware size (1 bytes), Protocol size (1 bytes), Opcode (2 bytes), Sender MAC address(2 bytes), Sender IP address (2 bytes), Target MAC address (2 bytes), Target IP address (2 bytes)
6. Hardware type: Ethernet (1)
7. Protocol type: IPv4 (0x0800)
8. Το Protocol type έχει την τιμή του IPv4(0x0800) ενώ το Ethertype έχει την τιμή των ARP(0x0806 )

9. Γιατί αυτό είναι το μήκος διεύθυνσης του πρωτοκόλλου IPv4 σε bytes
10. Το πεδίο "Hardware size" έχει την τιμή 6 στο ARP προκειμένου να υποδεικνύει ότι πρόκειται για μια διεύθυνση MAC με 6 οκτάδες.
11. Στον υπολογιστή μου
12. Η ff:ff:ff:ff:ff:ff (broadcast)
13. Address Resolution Protocol (reply):28 bytes Ethernet II:14 bytes
14. 20 bytes
15. Opcode: request (1)
16. Sender MAC address
17. Sender IP address
18. Target IP address
19. Target MAC address και έχει τιμή 0 σε όλα τα bits του
20. Η διεύθυνση MAC του αποστολέα ανήκει στην διεύθυνση της συσκευής που κάναμε ping και η διεύθυνση του παραλήπτη ανήκει στον υπολογιστή μου
21. Opcode: reply (2)
22. Sender IP address
23. Sender MAC address
24. Target IP address
25. Target MAC address
26. Address Resolution Protocol (reply):28 bytes Ethernet II:32 bytes
27. Όχι το πλαίσιο ethernet που μεταφέρει το ARP reply έχει μεγαλύτερο μήκος
28. Opcode αν είναι 1 είναι request και αν είναι 2 είναι reply
29. Στο ότι η βιβλιοθήκη ncap του Wireshark συλλαμβάνει τα απερχόμενα πλαίσια πρωτού πάνε στην κάρτα δικτύου, όπου προστίθεται το padding(ή trailer) για να μεταδοθούν
30. Στο ότι το ARP request έχει κενή Target MAC address και στο opcode
31. Θα έμπαινε στα routing tables των άλλων συσκευών του υποδικτύου με αποτέλεσμα να λαμβάνει πακέτα που δεν προορίζονταν αρχικά για αυτόν, να μπορεί να αλλάξει το traffic ή ακόμα και να το μπλοκάρει τελείως, ανοίγοντας έτσι τον δρόμο για άλλες επιθέσεις όπως denial of service, man in the middle ή session hijacking