Ονοματεπώνυμο: ΙΟΡΔΑΝΙΔΗΣ ΚΡΙΤΩΝ
Ομαδα: 1
Όνομα PC/OS: Kriton’s Air / MacOS 12.6
Ημερομηνία: 19/10/2022
Διεύθυνση IP: 147.102.237.144
Διεύθυνση MAC: –

ΕΡΓΑΣΤΗΡΙΑΚΗ ΑΣΚΗΣΗ 3: ΕΠΙΚΟΙΝΩΝΙΑ ΣΤΟ ΤΟΠΙΚΟ ΔΙΚΤΥΟ (ΠΛΑΙΣΙΟ ETHERNET ΚΑΙ ΠΡΩΤΟΚΟΛΛΟ ARP)

Άσκηση 1

1.1 arp –a
1.2 sudo arp –d –a
1.3 netstat –rn 147.102.236.200
    scutil –dns 147.102.224.243
1.4
1.5 Βγαζει και την default gateway και το DNS
1.6 147.102.239.40
1.7 Παρατηρω οτι έχει προστεθεί στη λίστα η διεύθυνση που εκανα ping
1.8 Τώρα έχει καταχωρηθεί μόνο το default gateway 147.102.236.200 καθώς αποστάλθηκαν DNS αρχεία
1.9 Όχι, γιατί η διεύθυνση του site ανήκει σε άλλο υποδίκτυο και η επικοινωνία γίνεται μέσω του default gateway

Άσκηση 2

2.1 Τα πλαίσια source, destination και type
2.2 Όχι διότι η χρησιμότητα του είναι ο συγχρονισμός δέκτη–αποστολέα
2.3 Το CRC δεν μπορεί να καταγραφεί διότι δεν το καταγράφει ο μηχανισμός καταγραφής πακέτων του λειτουργικού συστήματος
2.4 0x0800
2.5 0x0806
2.6 0x86dd
2.7 –
2.8 –
2.9 Όχι διότι δεν είναι στο ίδιο υποδίκτυο
2.10 Ανήκει στο default gateway διότι αυτό το gateway θα αναλάβει να επιλύσει τη διεύθυνση MAC του site
2.11 510 bytes
2.12 66 bytes
2.13 –
2.14 Όχι
2.15 Στο default gateway
2.16 –
2.17 στον δικό μου
2.18 6590 bytes
2.19 79 bytes

Άσκηση 3

3.1 Είναι μοναδικές (globally unique) και ατομικες (individual)

3.2 Είναι ομαδικές (group) και καποιες είναι μοναδικές ενω άλλες είναι τοπικες (locally administered)
3.3 Λαμβάνεται πρώτα το bit στη θέση 7 και μετά στη θέση 6 (ξεκινώντας αρίθμηση από τη θέση 0 στην οποία βρίσκεται το MSB του byte)
3.4 ff:ff:ff:ff:ff:ff
3.5 Παραμένουν τα πλαίσια με πρωτόκολλο STP
3.6 Είναι το length και δηλωνει το μέγεθος των δεδομένων του πακέτου αν αφαιρέσουμε την επικεφαλίδα
3.7 Το ethernet 2 έχει πεδία source, destination και type ενω το IEEE 802.3 έχει destination, source length και padding
3.8 Η επικεφαλίδα LLC έχει μέγεθος 3 bytes και περιλαμβάνει τα πεδία DSAP, SSAP και Control Field
3.9 Μεταφέρει δεδομένα STP και έχουν μέγεθος 36 bytes
3.10 Έχει μέγεθος 7 bytes

Άσκηση 4

4.1 Μας εμφανίζει μόνο τα πακέτα ethernet τα οποία στέλνει ή δέχεται ο υπολογιστής μου
4.2 Απομονώνει τα πακέτα με πρωτόκολλο ARP
4.3 Ανταλλάχθηκαν 16 πακέτα. Εγινε ping 8 φορες και για καθε μία φορα στάλθηκε ενα request και ένα reply
4.4 Το type
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
4.6 Έχει τιμή 1 και υποδεικνύει κάρτα Ethernet
4.7 0x0800 και υποδεικνύει IPv4
4.8 Οι τιμές των δύο πεδίων αντιστοιχούν στα ίδια πρωτόκολλα (π.χ. η τιμή 0x0800 αντιστοιχεί στο IPv4 σε αμφότερα τα πεδία)
4.9 Το protocol size μας δίνει το μήκος διεύθυνσης IPv4 και για αυτό το λόγο η τιμή του είναι 4 (bytes)
4.10 Το hardware size μας δινει το μήκος της διεύθυνσης MAC του υπολογιστή και για αυτό η τιμη του είναι 6 (bytes)
4.11 Ανήκει στον υπολογιστή μου
4.12 ff:ff:ff:ff:ff:ff
4.13 Το ARP request έχει μέγεθος 28 bytes, ενώ το πλαίσιο Ethernet 42 bytes
4.14 20 bytes
4.15 1
4.16 Στο Sender MAC address
4.17 Στο Sender IP address
4.18 Στο Target IP address
4.19 Ναι, υπάρχει το Target MAC address και περιέχει τη τιμή 00:00:00:00:00:00
4.20 Η διεύθυνση MAC του αποστολέα ανήκει στον υπολογιστή προς τον οποίο έγινε το ping ενώ η MAC του παραλήπτη ανήκει στον δικό μου υπολογιστή
4.21 2
4.22 Στο Sender IP address

4.23 Στο Sender MAC address
4.24 Στο Target IP address
4.25 Στο Target MAC address
4.26 Το πλαίσιο ethernet έχει μέγεθος 42 bytes, ενώ το ARP reply 28 bytes
4.27 Φυσικά και είναι
4.28 Το opcode του οποίου η τιμη 1 αντιστοιχεί σε request, ενω η τιμη 2 αντιστοιχεί σε reply
4.29 Η βιβλιοθήκη libpcap έπιασε το ARP reply πριν ενθυλακωθει μεσα απο τη καρτα δικτυου οποτε δεν έχει trailer, ενώ το request το έπιασε μέσα απο τη καρτα δικτύου και άρα έχει trailer
4.30 Διαφέρουν στο ότι ένα ARP request πρέπει να έχει την target MAC address μηδενικη καθως δεν μπορεί να τη ξέρει, ενω κατα την επιστροφη (reply) αυτή η διευθυνση εχει προσδιοριστεί στο πεδίο Sender MAC address. Επίσης, διαφέρει το opcode όπως αναφέρθηκε στην ερωτηση 4.28
4.31 θα υπήρχαν δύο ARP replies για κάθε request και στο ARP table θα είχαμε δύο MAC διευθύνσεις για κάθε IP στο υποδίκτυο. Οπότε, ό,τι στέλναμε θα το λάμβανε και ο κακόβουλος υπολογιστής