2η Εργαστηριακή Άσκηση στα Δίκτυα Υπολογιστών

Ονοματεπώνυμο	Γεώργιος Στεφανάκης
Αρ. Μητρώου	el18436
Ομάδα	4
Λειτουργικό Σύστημα	Manjaro Linux x86_64
Διεύθυνση IP	147.102.237.123
Διεύθυνση MAC	b4:69:21:5e:da:03
Ημερομηνία	2022-10-12

1. Στρώμα Ζεύξης Δεδομένων

1.1. Χρησιμοποιήσαμε φίλτρο απεικόνισης “arp or ip” ούτως ώστε να εμφανίσουμε όλα τα πακέτα που έχουν αποσταλεί ή ληφθεί είτε με πρωτόκολλο τύπου IP (IPv4 ή IPv6), είτε με τύπου πρωτόκολλο ARP.

1.2. Τα δύο πεδία της επικεφαλίδας Ethernet είναι το Destination (διεύθυνση MAC του υπολογιστή που λαμβάνει το πακέτο), το Source (διεύθυνση MAC του υπολογιστή που στέλνει το πακέτο) και το Type (τύπος της διεύθυνσης IP του ανωτέρου επιπέδου).

1.3. Όχι δεν υπάρχει πεδίο στην επικεφαλίδα του Ethernet, υπάρχει όμως στην επικεφαλίδα του πακέτου του στρώματος δικτύου. Το μέγεθος του πακέτου του στρώματος δικτύου είναι προφανώς μικρότερο καθώ αυτό ενθυλακώνεται μέσα στο πλαίσιο του στρώματος ζεύξης.

1.4. Το μήκος των διευθύνσεων είναι 6 byte για κάθε μία από τις διευθύνσεις MAC που αναφέρθηκαν, δηλαδή στο σύνολο 12 bytes.

1.5. Ακουμπώντας τον κέρσορα στην επικεφαλίδα Ethernet, εμφανίζεται στο κάτω αριστερά μέρος της εφαρμογής το μέγεθός της, που είναι ίσο με 14 bytes.

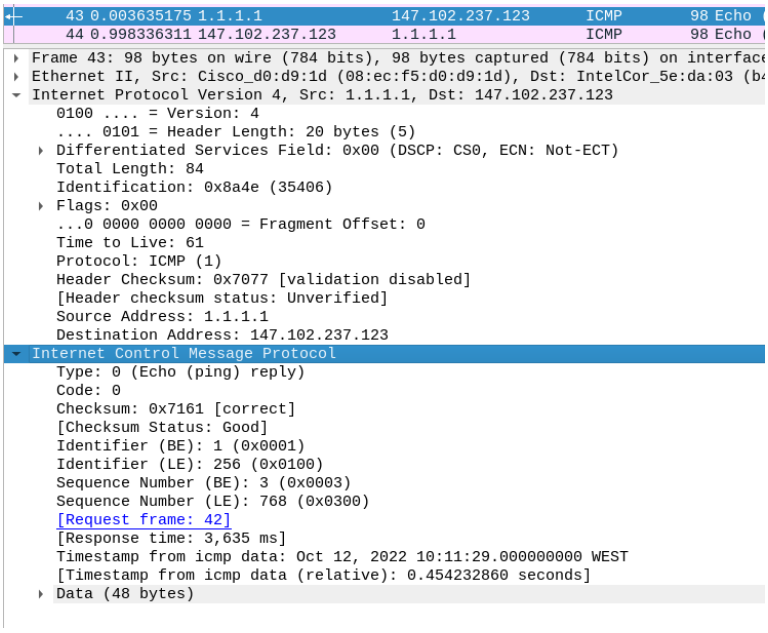
1.6. Το πεδίο Type.

1.7. Το πεδίο Type καταλαμβάνει τα δύο τελευταία bytes της επικεφαλίδας Ethernet.

1.8. Για πακέτα τύπου IPv4, η τιμή του Type είναι 0x0800.

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

2. Στρώμα Δικτύου



2.1. Το φίλτρο απεικόνισης που χρησιμοποιήσαμε δείχνει μόνο τα πακέτα με πρωτόκολλο ICMP (Internet Control Message Protocol) τα οποία προκύπτουν μετά από το “ping 1.1.1.1”.
2.2. Οι διευθύνσεις IPv4 έχουν μήκος 4 byte.
2.3. Τα δύο πρώτα πεδία της επικεφαλίδας IPv4 είναι το Version (IPv4 ή IPv6) και το Length (μέγεθος επικεφαλίδας σε bytes).
2.4. Το πεδίο Version είναι 4 bits με τιμή 0100 και το πεδίο Length είναι 4 bits με τιμή 0101.
2.5. Το μήκος της επικεφαλίδας IPv4 ενός πακέτου είναι 20 bytes.
2.6. Αυτό το μήκος προκύπτει από το πεδίο Length (5), το οποίο σημαίνει ότι έχουμε 5 * 32 bits (4 bytes) = 20 bytes.
2.7. Είναι το μήκος της επικεφαλίδας IPv4 (20 bytes) + το μήκος των δεδομένων (64 bytes) = 84 bytes.
2.8. Υπάρχει το πεδίο Total Length με τιμή 84, όπως αναμέναμε.
2.9. Εάν φέρουμε τον κέρσορα πάνω στην επικεφαλίδα Internet Control Message Protocol, στο κάτω αριστερά μέρος της εφαρμογής φαίνεται ότι τα δεδομένα (payload) ισούνται με 64 bytes.
2.10. Το μήκος του payload μπορεί να προκύψει εάν αφαιρέσουμε από το Total Length (84 bytes), το μήκος της επικεφαλίδας IPv4 (20 bytes), δηλαδή 64 bytes.
2.11. Το πεδίο Protocol είναι εκείνο που καθορίζει το πρωτόκολλο στρώματος μεταφοράς της σουίτας TCP/IP.
2.12. Η θέση του στην επικεφαλίδα είναι το 24^{ο} byte.
2.13. Για το πρωτόκολλο ICMP, η τιμή του είναι 0x01.

3. Στρώμα Μεταφοράς

3.1. Η σημασία του φίλτρου αυτού είναι να κρατά στη λίστα πακέτων μόνο αυτά που έχουν σταλεί ή ληφθεί με πρωτόκολλο TCP ή UDP.
3.2. TCP και UDP.
3.3. Για το TCP, η τιμή πρωτοκόλλου είναι 6 και, για το UDP, η τιμή είναι 17.
3.4. Τα κοινά πεδία των δύο πακέτων είναι τα Source port, Destination port, Checksum.
3.5. Το μήκος της επικεφαλίδας UDP είναι 8 bytes.
3.6. Υπάρχει αυτό το πεδίο στην επικεφαλίδα UDP, και ονομάζεται Length.
3.7. Το πεδίο Length είναι αυτό που καθορίζει το μήκος της επικεφαλίδας TCP, ξεκινάει από 66^{ο} byte της επικεφαλίδας και έχει μέγεθος 32 bytes.
3.8. Όχι δεν υπάρχει τέτοιο πεδίο στην επικεφαλίδα για το συνολικό μήκος των TCP τεμαχίων, υπάρχει μόνο ως παραγόμενο μέγεθος σε αγκύλες από το Wireshark.
3.9. Τα πεδία Destination και Source Port υποδηλώνουν έμμεσα το πρωτόκολλο εφαρμογής. Όπως βλέπουμε από το RFC sourcebook για κάθε πρωτόκολλο μεταφοράς TCP ή UDP, κάθε port αντιστοιχίζεται μοναδικά σε ένα συγκεκριμένο πρωτόκολλο εφαρμογής.
3.10. Παρατηρούμε HTTP, DNS κ.α.

4. Στρώμα Εφαρμογής

4.1. Το DNS χρησιμοποιεί πρωτόκολλο μεταφοράς UDP.
4.2. Το HTTP χρησιμοποιεί πρωτόκολλο μεταφοράς TCP.
4.3. Στην επικεφαλίδα DNS, το πρώτο bit του πεδίου Flags καθορίζει εάν το μήνυμα είναι ερώτημα (query, 0), ή απάντηση (response, 1).
4.4. Η θύρα προορισμού των ερωτήσεων DNS είναι η 53.
4.5. Οι θύρες πηγής των ερωτήσεων DNS που παρατήρησα είναι οι 33138, 33696, 53746.
4.6. Η θύρα πηγής των απαντήσεων DNS είναι η 53, η ίδια θύρα με τη θύρα προορισμού των ερωτήσεων. Συνεπώς συμπεραίνουμε ότι η θύρα αυτή δεσμεύεται για την υλοποίηση του πρωτοκόλλου.
4.7. Οι θύρες προορισμού των απαντήσεων DNS είναι οι ίδιες με τις θύρες πηγής των ερωτήσεων DNS, δηλαδή οι 33138, 33696, 53746.
4.8. Παρατηρούμε ότι υπάρχει ακριβής αντιστοιχία μεταξύ θυρών πηγής ερωτήσεων και θυρών προορισμού απαντήσεων.
4.9. Η θύρα 53.
4.10. Η θύρα προορισμού των μηνυμάτων HTTP είναι η θύρα 80.
4.11. Η θύρα προέλευσης του μηνύματος HTTP είναι η 40914.
4.12. Η θύρα προέλευσης των απαντήσεων HTTP είναι η 80.
4.13. Η θύρα προορισμού της απάντησης HTTP που έλαβα είναι η θύρα 40914.

4.14. Ο εξυπηρετητής HTTP ακούει στη θύρα 80.
4.15. Βλέπουμε ότι η θύρα προορισμού για τα HTTP responses βρίσκεται σε πλήρη αντιστοιχία με τη θύρα πηγής για τα HTTP requests.
4.16. Το πρώτο μήνυμα HTTP από τον υπολογιστή μας στον εξυπηρετητή ιστού έχει όνομα GET /lab2/ HTTP/1.1
4.17. Το HTTP status code που επιστρέφει ο εξυπηρετητής ιστού είναι 200 OK.
4.18. Η εκτέλεση αυτής της εντολής χρειαζόταν γιατί αν είχαμε επισκεφθεί ξανά την ιστοσελίδα, αυτή η μετάφραση των ονομάτων σε διευθύνσεις IP που υλοποιεί το DNS θα είχε γίνει ήδη και θα είχε αποθηκευτεί στην DNS cache οπότε δεν θα παρατηρούσαμε ανταλλαγή πακέτων DNS.