Εργαστήριο Δικτύων - Τμήμα Μηχανικών Η/Υ & Πληροφορικής
Πανεπιστήμιο Πατρών

Εργασία: Ανάλυση πρωτοκόλλων με χρήση του λογισμικού Wireshark.

Εισαγωγή

Για τις παρακάτω ασκήσεις θα χρησιμοποιηθεί το λογισμικό Wireshark (https://www.wireshark.org/) και μπορείτε να το κατεβάσετε από εδώ: https://www.wireshark.org/index.html#download. Για την λειτουργία του Wireshark και την καταγραφή πακέτων, θα χρησιμοποιήσετε τη λειτουργία Capture με φίλτρο, ώστε τα πλαίσια που καταγράφονται να περιέχουν κάποια συγκεκριμένα χαρακτηριστικά. Για να κάνετε μια καταγραφή με φίλτρο, από το μενού Capture->Interfaces... πιέστε το κουμπί Options. Στο παράθυρο που θα εμφανισθεί επιλέξτε την κάρτα δικτύου του υπολογιστή σας στην οποία θέλετε να κάνετε την καταγραφή. Με διπλό κλικ στο όνομα της κάρτας θα εμφανισθεί το μενού για το φίλτρο σύλληψης.

Στο πεδίο δίπλα από το κουμπί “Capture Filter” πληκτρολογήστε μια λογική έκφραση σύμφωνη με τη σύνταξη των φίλτρων καταγραφής. Πιέζοντας το Start θα αρχίσει η καταγραφή. Υπάρχουν έτοιμοι κανόνες χρωματισμού από την εγκατάσταση του Wireshark, τους οποίους μπορείτε να κρατήσετε ή να αλλάξετε από τη θέση View→Coloring rules.... Τα πλαίσια που καταγράφονται θα εμφανιστούν έγχρωμα στο παράθυρο με τη λίστα καταγεγραμμένων πακέτων του Wireshark. Κάθε γραμμή αντιστοιχεί σε ένα πλαίσιο που συλλαμβάνεται. Μπορείτε να επιλέξτε ένα οποιοδήποτε από τα πλαίσια που καταγράφηκαν κάνοντας κλικ στην αντίστοιχη γραμμή του παραθύρου.
Τα βασικά πεδία της επικεφαλίδας κάθε πρωτοκόλλου, που περιέχεται στο πλαίσιο που επιλέξατε, εμφανίζονται με γραφικό τρόπο στο παράθυρο με τις λεπτομέρειες επικεφαλίδας στο μεσαίο τμήμα της οθόνης. Στο παράθυρο με τα περιεχόμενα (κάτω τμήμα της οθόνης) εμφανίζονται τα δεδομένα του επιλεγμένου πλαισίου σε δεκαεξαδική και ASCII μορφή. Μπορείτε να δείτε όλο το περιεχόμενο μιας επικεφαλίδας με διπλό κλικ ή κάνοντας κλικ επάνω της και πιέζοντας το πλήκτρο ‘+’ ή με κλικ στο σύμβολο στα αριστερά της. Όταν κάνετε κλικ πάνω σε κάποια επικεφαλίδα ή σε κάποιο πεδίο μιας επικεφαλίδας (στο παράθυρο με τις λεπτομέρειες επικεφαλίδας), τότε εμφανίζεται με αντιστροφή χρώματος (highlighted) το αντίστοιχο κομμάτι του πλαισίου στο παράθυρο με τα περιεχόμενα του πλαισίου. Τέλος, το μέγεθος και των τριών παραθύρων (καταγεγραμμένα πλαίσια, λεπτομέρειες επικεφαλίδας, περιεχόμενα πλαισίου) μπορεί να μεταβληθεί επιλέγοντας και σύροντας τις οριζόντιες μπάρες που τα διαχωρίζουν.

Ανάλυση DNS πρωτοκόλλου

Στην παρούσα άσκηση θα μελετηθεί το DNS σύστημα χρησιμοποιώντας τις εντολές nslookup και ifconfig/ipconfig (Linux/Windows) αντίστοιχα. Για να εξοικειωθείτε με τις εντολές εκτελέστε τις παρακάτω και αναφέρατε τα αποτελέσματα:

1. nslookup www.ceid.upatras.gr
2. ifconfig ή ip a (Linux)
3. ipconfig \all (windows)
4. ipconfig /displaydns (windows)
5. ipconfig /flushdns
6. dig www.ceid.upatras.gr (Linux)

Εκκινήστε το Wireshark. Καταγράψτε και δείξτε τα πακέτα DNS που στέλνονται από τον υπολογιστή σας εκτελώντας πριν την καταγραφή πρώτα τα παρακάτω :

- ipconfig για να σβήσετε το DNS cache.
- Εκκαθάριση του cache του browser
- δήλωση “ip.addr == your_IP_address” στο φίλτρο του Wireshark

Εκκινήστε την καταγραφή στο Wireshark και πραγματοποιείστε τα παρακάτω:

- επισκεφτείτε την σελίδα http://www.ietf.org
- σταματήστε την καταγραφή στο Wireshark.

Απαντήστε στα παρακάτω ερωτήματα και δώστε screenshots από τα πακέτα.

1. Βρείτε και αναφέρατε τα DNS μηνύματα που ανταλλάχθηκαν. Αναλύστε τα πακέτα που αφορούν το DNS (query and response) και εξηγείστε κάθε πεδίο του μηνύματος καθώς και το είδος του πρωτοκόλλου (TCP/UDP) που χρησιμοποιήθηκε.
2. Ποια είναι η θύρα προορισμού για το μήνυμα ερώτησης DNS και ποια είναι η θύρα προέλευσης του μηνύματος απόκρισης DNS;
3. Σε ποια διεύθυνση IP εμφανίζεται το μήνυμα ερώτησης DNS; Χρησιμοποιήστε το ipconfig για να καθορίσετε την Διεύθυνση IP του τοπικού σας διακομιστή DNS. Αυτές οι δύο διευθύνσεις IP είναι ίδιες;
4. Εξετάστε το μήνυμα ερώτησης DNS (query message). Τι "τύπος" ερωτήματος DNS είναι; Περιέχει το ερώτημα οποιεσδήποτε "απαντήσεις"?
5. Εξετάστε το μήνυμα απόκρισης DNS (response message). Πόσες "απαντήσεις" παρέχονται; Τι περιέχει η κάθε απάντηση?
6. Εξετάστε το επόμενο πακέτο TCP SYN που στέλνει ο υπολογιστής σας. Η διεύθυνση IP του πακέτου SYN αντιστοιχεί σε οποιαδήποτε από τις διευθύνσεις IP που παρέχονται στο το μήνυμα απάντησης DNS;

Απαντήστε στα παρακάτω γενικά ερωτήματα για τον τρόπο λειτουργίας του DNS

7. Ποια τα πεδία του header ενός DNS πακέτου? Εξηγείστε το καθένα.
8. Αναλύστε κάθε πεδίο του παρακάτω DNS πακέτου. Τι είδους DNS πακέτο είναι? Για ποιο domain ζητάει την IP? Χρησιμοποιήστε την ιστοσελίδα http://packetor.com/ για άμεση ανάλυση.

```
48 F8 B3 26 DF 49 BA BA BA BA BA BA 08 00 45 00 00 38 66 BD 00
00 80 11 02 0C C0 A8 01 34 08 08 08 08 D5 39 00 35 00 24 44 8F 00 03
01 00 00 01 00 00 00 00 00 00 06 67 6F 6F 67 6C 65 03 63 6F 6D 00 00
01 00 01
```

9. Ομοίως αναλύστε κάθε πεδίο του παρακάτω DNS πακέτου: Τι είδους DNS πακέτο είναι?

```
BA BA BA BA BA BA 48 F8 B3 26 DF 49 08 00 45 08 00 E8 B2 EF 00
00 37 11 FE 21 08 08 08 08 C0 A8 01 34 00 35 D5 39 00 D4 28 A2 00 03
81 80 00 01 00 0B 00 00 00 00 06 67 6F 6F 67 6C 65 03 63 6F 6D 00 00
01 00 01 C0 0C 00 01 00 01 00 00 00 04 00 04 4A 7D EC 23 C0 0C 00
01 00 01 00 00 00 04 00 04 4A 7D EC 25 C0 0C 00 01 00 01 00 00 00 04
00 04 4A 7D EC 27 C0 0C 00 01 00 01 00 00 00 04 00 04 4A 7D EC 20
C0 0C 00 01 00 01 00 00 00 04 00 04 4A 7D EC 28 C0 0C 00 01 00 01
00 00 00 04 00 04 4A 7D EC 21 C0 0C 00 01 00 01 00 00 00 04 00 04 4A
7D EC 29 C0 0C 00 01 00 01 00 00 00 04 00 04 4A 7D EC 22 C0 0C 00
01 00 01 00 00 00 04 00 04 4A 7D EC 24 C0 0C 00 01 00 01 00 00 00 04
00 04 4A 7D EC 2E C0 0C 00 01 00 01 00 00 00 04 00 04 4A 7D EC 26
```

Ανάλυση DHCP πρωτοκόλλου

Στην παρούσα άσκηση θα μελετηθεί το DHCP πρωτόκολλο με χρήση Wireshark, Εκτελέστε τα παρακάτω βήματα:

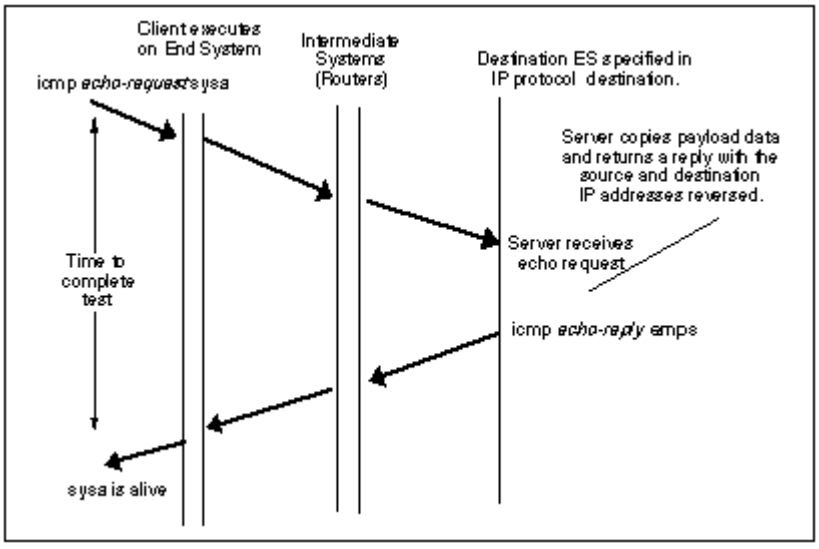
- Σε περιβάλλον windows ανοίξτε το Command Prompt και πληκτρολογείστε πληκτρολογήστε "ipconfig /release" (το εκτελέσιμο είναι στο C:\windows\system32.). Τι κάνει αυτή η εντολή ?
- Εκκινήστε τον Wireshark, και ξεκινήστε την καταγραφή πακέτων Wireshark.
- Στο Command Prompt των Windows πληκτρολογήστε "ipconfig /renew". Τι κάνει αυτή η εντολή? Ποια IP διεύθυνση αποκτάει ο υπολογιστής σας?
- Μετά πληκτρολογήστε ξανά την ίδια εντολή "ipconfig /renew". Όταν το δεύτερο "ipconfig /renew" τερματίσει, πληκτρολογήστε την εντολή "ipconfig/release" για να αποδεσμεύσετε την προηγούμενη IP διεύθυνση που είχε διατεθεί στον υπολογιστή σας.
- Τέλος, πληκτρολογήστε ξανά την εντολή "ipconfig /renew" για να έχετε εκ νέου μια IP διεύθυνση για τον υπολογιστή σας.
- Σταματήστε τη καταγραφή πακέτων Wireshark. ***Δείξτε όλα τα μηνύματα DHCP που κατέγραψε σε hex μορφή και σημειώστε ποιο πρωτόκολλο μεταφοράς και ποια θύρα χρησιμοποιήθηκε***.

Απαντήστε στις παρακάτω ερωτήσεις:

- Σχεδιάστε ένα datagram χρονισμού που να απεικονίζει την ακολουθία των πρώτων τεσσάρων πακέτων: Discover/Offer/Request/ACK DHCP μηνυμάτων μεταξύ του υπολογιστή σας και του DHCP server. Για κάθε πακέτο, δείξτε τα port numbers της πηγής και του προορισμού.
- Ποια θύρα και ποιο εκ των TCP/UDP πρωτοκόλλων χρησιμοποιείται?
- Ποια είναι η διεύθυνση του επιπέδου δεδομένων (π.χ., Ethernet) του υπολογιστή σας?
- Ποια πεδία διαφοροποιούνται μεταξύ των μηνυμάτων DHCP discover και DHCP request?
- Εάν η IP διεύθυνση δεν έχει ανατεθεί μέχρι το τέλος των 4 μηνυμάτων που ανταλλάσσονται, τότε τι τιμές χρησιμοποιούνται στα IP πακέτα των τεσσάρων αυτών μηνυμάτων? Για κάθε ένα μήνυμα δείξτε την IP διεύθυνση της πηγής και του προορισμού.
- Ποια η IP διεύθυνση του DHCP server? Ποια IP διεύθυνση προσφέρεται από τον DHCP server στον υπολογιστή σας? Δείξτε ποια μηνύματα που ανταλλάσσονται περιέχουν την προσφερόμενη IP.
- Εξηγείστε την χρήση του χρόνου lease time. Ποιος είναι αυτός στη περίπτωση σας?
- Ποια η χρήση του μηνύματος DHCP release? Στέλνει ο DHCP server επιβεβαίωση λήψης του μηνύματος DHCP request του υπολογιστή σας? Τι θα γίνει στην περίπτωση που που το μήνυμα το υπολογιστή DHCP release χαθεί ?
- Ανταλλάχθηκαν ARP packets κατά την διάρκεια των ανταλλαγών των DHCP μηνυμάτων? Εξηγείστε την χρήση τους.

Ανάλυση ICMP πρωτοκόλλου - Ping

Στην παρούσα άσκηση θα αναλυθεί το πρωτόκολλο ICMP με την καταγραφή των πακέτων που παράγονται από το Ping πρόγραμμα. Το πρόγραμμα Ping είναι ένα απλό εργαλείο που επιτρέπει στον καθένα (για παράδειγμα, έναν διαχειριστή δικτύου) να επαληθεύσει εάν ένας host είναι ενεργός ή όχι. Το πρόγραμμα Ping στον source host, στέλνει ένα πακέτο στη διεύθυνση IP του στόχου. Αν ο στόχος αποκρίνεται, ο στόχος απαντάει στέλνοντας πίσω ένα πακέτο.



Υλοποιείστε τα παρακάτω βήματα:

- Ξεκινήστε το Wireshark και αρχίστε την καταγραφή πακέτων.
- Εκτελέστε την ping σε περιβάλλον windows παρακάτω “ping –n 10 8.8.8.8”. Η παράμετρος “-n 10” υποδεικνύει ότι 10 ping μηνύματα πρέπει να σταλούν.
- Όταν τερματίσει το πρόγραμμα Ping, σταματήστε την καταγραφή πακέτων στο Wireshark.

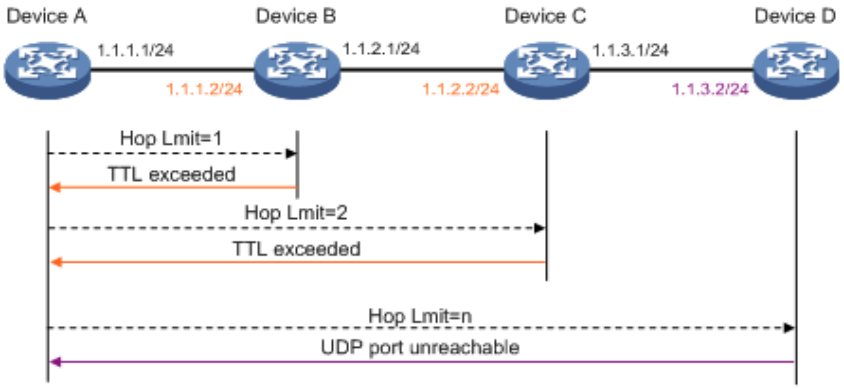
Απαντήστε στις παρακάτω ερωτήσεις:

1. Δώστε screenshot από τα αποτελέσματα του ping και υπολογίστε την μέση τιμή του RTT.

2. Δώστε screenshot από τα αποτελέσματα στο Wireshark που αφορούν τα ICMP μηνύματα και αναλύστε τα πακέτα, εξηγείται κάθε πεδίο του μηνύματος και τι μήνυμα αφορά. Ποιος ο τύπος, το άθροισμα ελέγχου, το αναγνωριστικό, ο αύξοντας αριθμός και το code του ICMP μηνύματος?
3. Γιατί ένα πακέτο ICMP δεν έχει τους αριθμούς θυρών πηγής και προορισμού;
4. Εξετάστε το αντίστοιχο ping πακέτο απάντησης. Ποιοι είναι οι τύποι και code αριθμοί ICMP; Τι άλλα πεδία έχει αυτό το ICMP πακέτο; Πόσα byte είναι τα πεδία άθροισμα ελέγχου, αύξοντα αριθμού και το αναγνωριστικό;

Ανάλυση ICMP πρωτοκόλλου - Traceroute

Στην συνέχεια θα μελετήσουμε την καταγραφή πακέτων που παράγονται από το πρόγραμμα tracert σε Windows περιβάλλον (ή traceroute σε Linux). Το πρόγραμμα tracert/traceroute στέλνει μηνύματα ICMP ((ή UDP)) τύπου Echo Request με μεταβαλλόμενες τιμές του πεδίου Time-To-Live (TTL), του πακέτου IP, προς τον προορισμό. Κάθε δρομολογητής κατά μήκος της διαδρομής προς τον προορισμό μειώνει το TTL κατά 1, προτού προωθήσει το πακέτο.
Για παράδειγμα το πρόγραμμα στέλνει το πρώτο πακέτο με TTL=1, το δεύτερο πακέτο με TTL=2 και ούτω καθεξής. Όταν ένα πακέτο φτάνει σε ένα router με TTL=1, το router στέλνει ένα ICMP πακέτο σφάλματος (ICMP τύπου Time Exceeded) πίσω στην πηγή.
Η διαδρομή βρίσκεται εξετάζοντας τα μηνύματα Time Exceeded που προκαλούνται από διαδοχικά μηνύματα ηχούς με συνεχώς αυξανόμενες τιμές του TTL και καταγράφοντας την εκάστοτε διεύθυνση IP της πηγής που παράγει το μήνυμα ICMP τύπου Time Exceeded.



- Ξεκινήστε το Wireshark και αρχίστε την καταγραφή πακέτων.
- Πληκτρολογήστε “tracert 8.8.8.8” στη γραμμή εντολών των windows. Όταν το Traceroute πρόγραμμα τερματίσει, σταματήστε την καταγραφή πακέτων από το Wireshark.
- Δείξτε με screenshot τα αποτελέσματα του tracert και δείξτε το χρόνο RTT για τον προορισμό. Μέσα στις μετρήσεις του tracert, υποδείξτε το πιο αργό link που υπάρχει. Με βάση τα ονόματα των router, μπορείτε να ελέγξετε την τοποθεσία και την απόσταση αυτού του router?
- Στη συνέχεια στο Wireshark ταξινομείστε κατά φθίνουσα σειρά τα ICMP πακέτα, σύμφωνα με τη διεύθυνση IP της πηγής τους (Source) κάνοντας κλικ στην αντίστοιχη επικεφαλίδα του παράθυρου με τη λίστα καταγεγραμμένων πακέτων. Εάν το μικρό βέλος δείχνει προς τα πάνω (αύξουσα σειρά), κάντε πάλι κλικ στην επικεφαλίδα ώστε να δείχνει προς το κάτω (φθίνουσα σειρά). Στη λίστα καταγεγραμμένων πακέτων θα πρέπει να εμφανίζονται τώρα με τη σειρά όλα τα μηνύματα ICMP που έστειλε ο υπολογιστής σας. Επιλέξτε το πρώτο μήνυμα ICMP τύπου Echo Request που έστειλε ο υπολογιστής σας. Με κλικ στο σύμβολο στα αριστερά της επικεφαλίδας Internet Protocol (στο παράθυρο με τις λεπτομέρειες επικεφαλίδας του επιλεγμένου πακέτου) αναπτύξετε τα περιεχόμενά της. Χρησιμοποιώντας το πλήκτρο ↓ (κάτω βέλος) μετακινηθείτε από το πρώτο στο τελευταίο μήνυμα της σειράς μηνυμάτων ICMP που έστειλε ο υπολογιστής σας.
- Δείξτε με screenshot από τα αποτελέσματα στο Wireshark και αναλύστε ένα ολόκληρο “πακέτο σφαλμάτων” και ένα πακέτο “Echo Request”. Εξηγείστε κάθε πεδίο του μηνύματος.
- Για το πρώτο μήνυμα Echo request και πακέτο σφαλμάτων επιβεβαιώστε από την ανάλυση το TTL και ότι η IP είναι η ίδια από την εκτέλεση της εντολής στο τερματικό.

Απαντήστε στις παρακάτω ερωτήσεις:

5. Αν το ICMP στείλει UDP πακέτα (όπως στα Unix/Linux), ο αριθμός IP πρωτοκόλλου θα ήταν και πάλι 01 για τα πακέτα ανίχνευσης; Αν όχι, ποιος θα ήταν;

6. Εξετάστε το ICMP echo πακέτο στο screenshot σας. Είναι διαφορετικό από τα πακέτα ερωτημάτων ICMP ping? Αν ναι, γιατί?
7. Εξετάστε το ICMP πακέτο σφαλμάτων στο screenshot σας. Έχει περισσότερα πεδία από το ICMP echo πακέτο. Τι περιέχετε στα πεδία αυτά;
8. Εξετάστε τα τελευταία τρία ICMP πακέτα που παρέλαβε ο host της πηγής. Τι διαφορετικό έχουν αυτά τα πακέτα από τα ICMP error πακέτα; Γιατί είναι διαφορετικά;

9. Αναλύστε κάθε πεδίο του παρακάτω ICMP πακέτου. Τι είδους ICMP πακέτο είναι?

   0f 00 08 00 4f 00 00 64 00 00 00 00 ff 01 2e 61 0e 00 00 02 64 00 00 01
   07 27 08 0e 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 00 e9 57 00 00
   00 00 00 00 00 00 00 3c 00 c8 ab cd ab cd ab cd ab cd ab cd ab cd ab
   cd ab cd ab cd ab cd ab cd ab cd

10. Αναλύστε κάθε πεδίο του παρακάτω ICMP πακέτου. Τι είδους ICMP πακέτο είναι?

    0f 00 08 00 4f 00 00 64 00 00 00 00 fc 01 05 ab 64 00 00 01 0e 00 00
    02 07 27 28 0e 00 00 02 0d 00 00 01 0b 00 00 02 0a 00 00 02 64 00
    00 01 0a 00 00 01 0b 00 00 01 0d 00 00 02 0e 00 00 01 00 00 00 f1 57
    00 00 00 00 00 00 00 00 00 3c 00 c8 ab cd ab cd ab cd ab cd ab cd ab
    cd ab cd ab cd ab cd ab cd ab cd ab cd

11. Αναλύστε κάθε πεδίο του παρακάτω ICMP πακέτου. Τι είδους ICMP πακέτο είναι?

    00 1d 60 b3 01 84 00 12 7f eb 6b 40 08 00 45 c0 00 38 00 9c 00 00 fe
    01 39 14 c0 a8 01 02 c0 a8 00 02 03 03 fc 5d 00 00 00 00 45 00 05 78
    00 00 40 00 01 11 f2 20 c0 a8 00 02 c0 a8 01 02 82 09 ad 9f 05 64 cb
    91

Ανάλυση IP πρωτοκόλλου

Δίνεται το παρακάτω frame δεδομένων.

00 A0 92 48 72 45 00 00 0C 05 C3 58 08 00 4 5 00 00 29 DB FB 40 00 FE 06 7D CB 81 6E 1E 1A 81
6E 02 11 02 03 00 50 6A 86 7B 57 B6 B6 B0 20 50 10 24 00 17 c4 00 00 02 54 41 4D 49 4C D7 87 6C
A4

Κάντε πλήρη ανάλυση όλων των hex πεδίων και επιπλέον απαντήστε στα παρακάτω ερωτήματα:

1. Ποια η IP διεύθυνση προορισμού και αποστολής?
2. Ποιο το μήκος του IP header και πιο όλου του πακέτου?
3. Είναι το frame μέρους ενός μεγαλύτερου πακέτου?
4. Τι πρωτόκολλο του στρώματος μεταφοράς χρησιμοποιεί και ποια η θύρα αποστολέα και δέκτη?
5. Ποια η τιμή του header checksum? Υπολογίστε εάν η τιμή στο frame είναι η σωστή.