



## 5ο Εργαστήριο

### Στόχος

- Κατανόηση των πρωτοκόλλων του επιπέδου μεταφοράς (L4) TCP και UDP και των αντίστοιχων PDUs, που ονομάζονται **segments (τμήματα)**
- Μελέτη των **packets (πακέτα)** του πρωτοκόλλου IP στο επίπεδο δικτύου (L3).
- Μελέτη των **frames (πλαίσια)** του πρωτοκόλλου Ethernet στο επίπεδο ζεύξης (L2) και εξοικείωση με τις **διευθύνσεις MAC**.
- Κατανόηση **ενθυλάκωσης** πληροφοριών του προηγούμενου επιπέδου της στοίβας στο PDU του επομένου

### A1) Συμπληρωματική άσκηση subnetting (προαιρετικά)

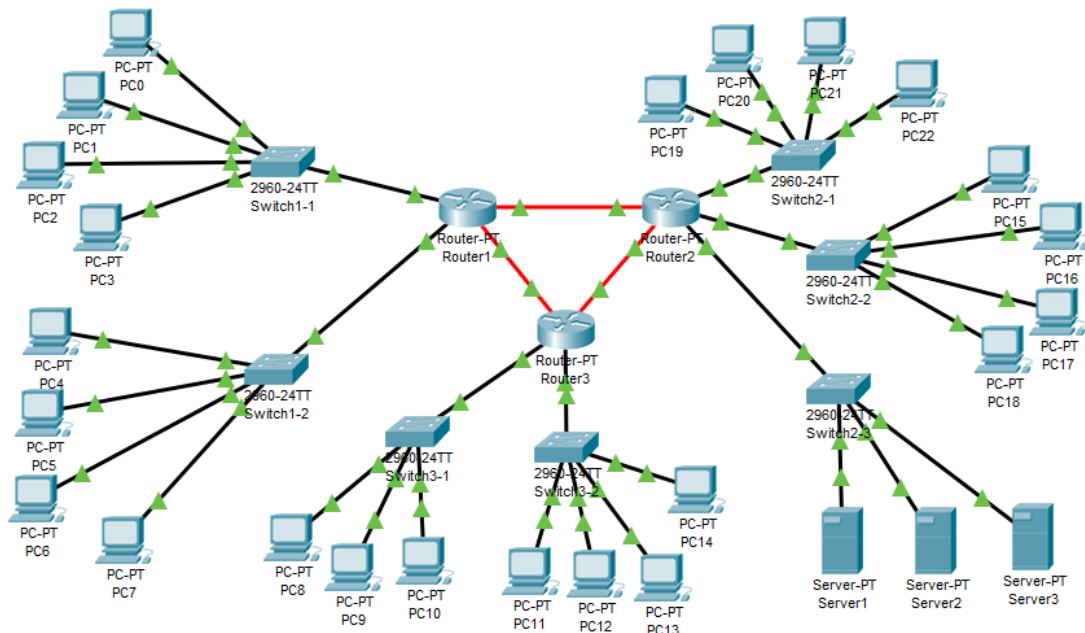
1. Σας δίνεται το δίκτυο 193.92.224.0/22 για την διευθυνσιοδότηση των παρακάτω IP δικτύων. Προχωρήστε στην απόδοση IP διευθύνσεων των δικτυακών συσκευών συμπληρώνοντας τους παρακάτω πίνακες με τις διευθύνσεις που θα χρησιμοποιήσετε.

Όνομα Δικτύου	Μέγεθος	IP διεύθυνση Δικτύου	Prefix
Δ1	43 ifs		
Δ2	15 ifs		
Δ3	27 ifs		
Δ4	125 ifs		
Δ5	14 ifs		
Δ6	40 ifs		
Δ7	79 ifs		
ΔR1-R2	2 ifs		
ΔR2-R3	2 ifs		
ΔR1-R3	2 ifs		

**Βήμα 1.** Βρείτε το μεγαλύτερο δίκτυο και σύμφωνα με αυτό προχωρήστε στην υποδικτύωση. Θα προκύψουν Χ δίκτυα με Υ διευθύνσεις ανά δίκτυο. Εντοπίστε εάν υπάρχουν και άλλα δίκτυα που να μπορούν να εξυπηρετηθούν με τόσα bit όσα αποφασίσατε και όχι λιγότερα και δώστε τους διευθύνσεις.

**Βήμα 2.** Εξαιρέστε από τις ανάγκες διευθυνσιοδότησης τα δίκτυα που έχετε εξυπηρετήσει και επαναλάβετε ξανά το βήμα 1. Θα χρησιμοποιήσετε το επόμενο αχρησιμοποίητο δίκτυο από αυτά που έχουν προκύψει από την προηγούμενη υποδικτύωση. Θα το χρησιμοποιήσετε ώστε να προχωρήσετε εκ νέου σε υποδικτύωση για τα δίκτυα που μένουν.

2. Το δίκτυο του σεναρίου που μπορείτε να φορτώσετε στο Cisco Packet Tracer από το **CNLab4-lab-ver.pkt**, υποθέστε ότι είναι το δίκτυο της εργασίας σας.



Εικόνα 1: Δίκτυο του CNLab4-lab-ver.pkt

Η ανάγκη που προκύπτει είναι η σύνδεση του με το INTERNET. Υποθέστε ότι προστίθεται ακόμη μία κάρτα δικτύου στο δρομολογητή Router2, με όνομα Serial 0. Μέσω αυτής της κάρτας δικτύου ο Router2 επικοινωνεί με τον δρομολογητή του ISP, με όνομα RouterISP. ISP είναι ο οργανισμός ή η εταιρεία που θα σας παρέχει πρόσβαση στο INTERNET. Το IP δίκτυο που θα χρησιμοποιηθεί για την επικοινωνία μεταξύ των δρομολογητών Router2 και RouterISP θα το ονομάζουμε DR2-RISP και θα είναι το 199.200.201.4/30. Η διεύθυνση 199.200.201.5 θα είναι η κάρτα δικτύου του RouterISP και η 199.200.201.6 η διεύθυνση της κάρτας δικτύου του Router2.

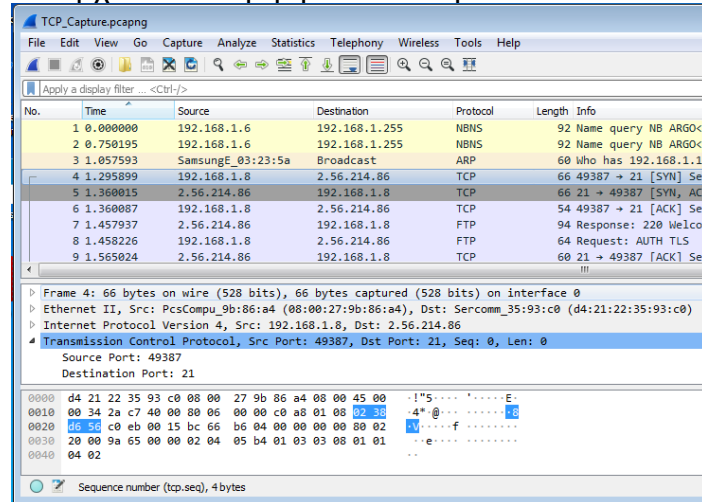
**E5.1** Προχωρήστε στις απαραίτητες ρυθμίσεις για την δρομολόγηση ώστε οι δρομολογητές του δικτύου σας να μπορούν να δρομολογήσουν IP πακέτα με οποιονδήποτε προορισμό.

#### Σημειώσεις:

- Προφανώς όταν συνδέεστε με κάποιο άλλο δίκτυο, στην προκειμένη περίπτωση με το δίκτυο του ISP, το οποίο σας συνδέει με το INTERNET, θα πρέπει να συμμορφώνεστε τουλάχιστον ως προς την μοναδικότητα των IP διευθύνσεων. Υποθέστε ότι αυτό ισχύει
- Υπενθυμίζεται ότι με τα παρακάτω στοιχεία μπορείτε να εισάγετε στατικές διαδρομές στον πίνακα προώθησης ενός δρομολογητή:
  - Network ( το IP δίκτυο για το οποίο ο δρομολογητής θέλετε να δρομολογεί IP πακέτα)
  - Mask (η subnet mask του IP δικτύου)
  - Next Hop (η IP διεύθυνση του δρομολογητή που θα παραλάβει το IP πακέτο και θα το προωθήσει κατάλληλα)

## B1) Πρωτόκολλο TCP

Ανοίξτε στο Wireshark το αρχείο TCP\_Capture.pcapng από τον φάκελο /Protocol Captures/TCP του αποθετηρίου. Περιέχει την καταγραφή της δικτυακής επικοινωνίας μεταξύ ενός FTP server και ενός FTP client (π.χ. Filezilla). Αρχικά θα παρατηρήσουμε την επικοινωνία σε επίπεδο L5 παρουσίασης (presentation) και την διευθυνσιοδότηση IP, ώστε κατόπιν να κατανοήσουμε τα TCP segments στο επίπεδο L4 μεταφοράς (transport). Το ερώτημα DNS έχει ήδη τρέξει και υπάρχει διαθέσιμη η διεύθυνση IP του FTP server.




No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.6	192.168.1.255	NBNS	92	Name query NB ARG0x0
2	0.750195	192.168.1.6	192.168.1.255	NBNS	92	Name query NB ARG0x0
3	1.057593	SamsungE_03:23:5a	Broadcast	ARP	60	Who has 192.168.1.1?
4	1.295899	192.168.1.8	2.56.214.86	TCP	66	49387 → 21 [SYN] Seq
5	1.360015	2.56.214.86	192.168.1.8	TCP	66	21 → 49387 [SYN, ACK
6	1.360087	192.168.1.8	2.56.214.86	TCP	54	49387 → 21 [ACK] Seq
7	1.457937	2.56.214.86	192.168.1.8	FTP	94	Response: 220 Welcom
8	1.458226	192.168.1.8	2.56.214.86	FTP	64	Request: AUTH TLS
9	1.565024	2.56.214.86	192.168.1.8	TCP	60	21 → 49387 [ACK] Seq

Εικόνα 2: Καταγραφή TCP\_Capture.pcapng

**E5.2** Παρατηρήστε τα τέσσερα πρώτα βήματα του πρωτοκόλλου FTP μέχρι να έρθει η απάντηση από τον FTP server. Ποια είναι η IP διεύθυνση του server; Ποιο είναι το μήνυμα καλωσορίσματος που εμφανίζεται, δηλαδή τα data του L5;

**E5.3** Αφού εντοπίσετε το παραπάνω μελετήστε το TCP segment που χρησιμοποιείται για την μεταφορά του μηνύματος καλωσορίσματος στο επίπεδο L4, και εντοπίσετε τα bytes του μηνύματος μέσα segment. Τι υπάρχει πριν από αυτά;

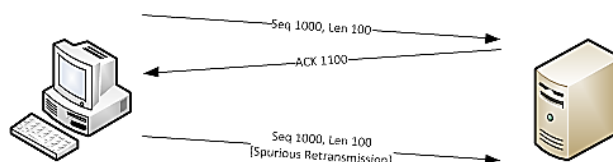
**E5.4** Εφαρμόστε το κατάλληλο φίλτρο ώστε να δείτε μόνο τα segments των ερωτημάτων που στάλθηκαν προς τον FTP server. Ταξινομήστε την προκύπτουσα λίστα κατά χρόνο με κλικ στην στήλη Time. Τι παρατηρείτε σε ένα από τα πεδία του TCP segment, όταν μετακινήστε με 

**E5.5** Εντοπίστε ένα εμφανές πρόβλημα διαδικτυακής ασφάλειας στην καταγραφή και ποια είναι η σειρά του επίμαχου segment μέσα στην επικοινωνία του επιπέδου L4. Πως θα διασφαλιζαμε την επικοινωνία;

**E5.6** Ακυρώστε όλα τα φίλτρα και προσπαθήστε να καταλάβετε πως λειτουργεί σε επίπεδο L4 το ανέβασμα (upload) μιας εικόνας PNG στον FTP server.

**Βοήθημα:** Κοιτάξτε από το “Request: STOR” και κάτω μέχρι το “Response: 226”. Τι παρατηρείτε; Σε ποια port του server γίνεται επικοινωνία του πρωτοκόλλου FTP και σε ποια upload των δεδομένων της εικόνας;

**E5.7 Για προχωρημένους:** Παρατηρούμε ότι κάποιο κομμάτι της εικόνας στάλθηκε δεύτερη προς τον FTP server, καθώς ο client θεώρησε ότι δεν έφτασε ποτέ. Αυτό ονομάζεται **spurious retransmission**. Εντοπίστε την απόκριση (ACK) την οποία δεν πήρε ο client και τον αριθμό του κομματιού των δεδομένων της εικόνας, από τα 10 που εστάλησαν μέσω FTP-DATA.



Εικόνα 3: Παράδειγμα spurious retransmission (κίβδηλης επαναποστολής).

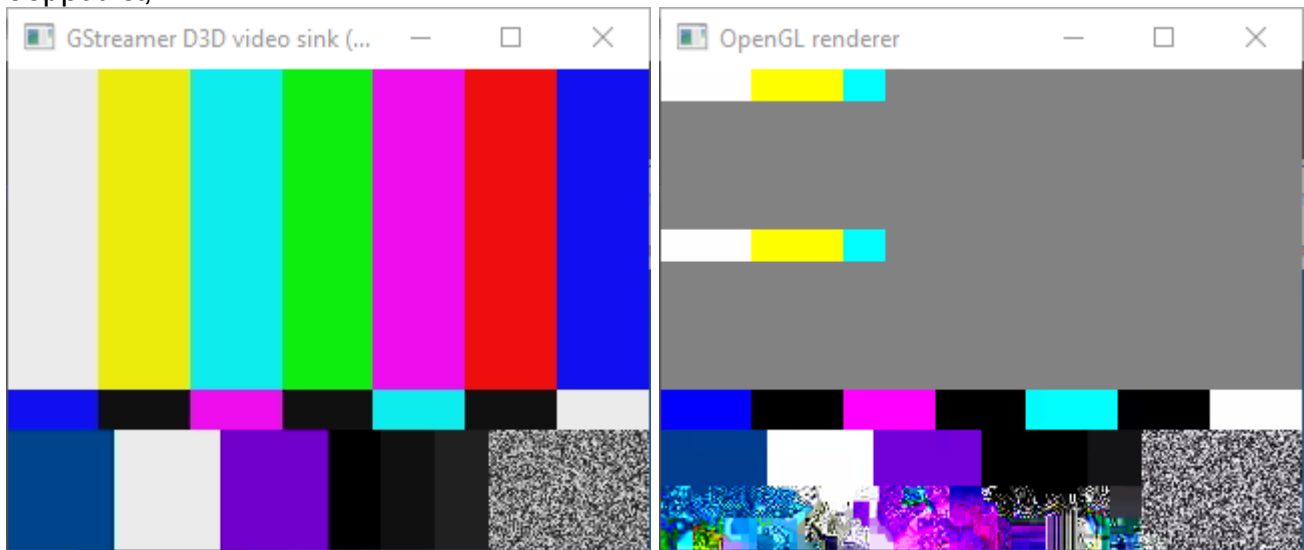
## B2) Πρωτόκολλο UDP

Ανοίξτε στο Wireshark το αρχείο `UDP_Capture.pcapng` από τον φάκελο `/Protocol Captures/TCP` του αποθετηρίου. Περιέχει την καταγραφή μιας ροής video μεταξύ ενός αποστολέα (video transmitter) και ενός παραλήπτη (video receiver), π.χ. ένα μη-επανδρωμένο αερόχημα (UAV) και ένας σταθμός επιτήρησης εδάφους. Τα data στο L5 δεν είναι αναγνώσιμα καθώς είναι κωδικοποίηση συμπίεσης video, αλλά μπορούμε να παρατηρήσουμε στο επίπεδο L4 μεταφοράς (transport) τα UDP segments. Δεν υπάρχει DNS ούτε σύνδεση στο Internet και εδώ χρησιμοποιούνται διευθύνσεις IP σε ένα κλειστό τοπικό δίκτυο.

**E5.8** Ποιος είναι ο video transmitter και ο video receiver, ποιες οι διευθύνσεις τους και σε ποια θύρα λειτουργεί το video streaming;

**E5.9** Ποια είναι η ειδοποιός διαφορά μεταξύ των πρωτοκόλλων μεταφοράς UDP και TCP;

**E5.10** Παρακάτω παρατηρούμε το video που εκπέμπει ο transmitter και το video που παραλαμβάνει ο receiver. Τι συμβαίνει με τα video frames κατά την μεταφορά; Αν έχετε ξαναδεί παρόμοιο πρόβλημα στην καθημερινότητά σας, καταλαβαίνετε πλέον τον λόγο για τον οποίο συμβαίνει;



Εικόνα 4: Αριστερά το video που προσπαθεί να στείλει ο transmitter , δεξιά το video που παραλαμβάνει ο receiver

**E5.11** Πότε θα ήταν προτιμότερο να χρησιμοποιούσαμε TCP segments για video streaming; Μελετήστε τα bytes του πρωτοκόλλου UDP και απαντήστε για ποιον λόγο δεν χρησιμοποιούμε πάντα TCP σε τέτοιες ογκώδεις επικοινωνίες;

## Γ1) Διευθύνσεις Media Access Control (MAC)

Στο επίπεδο ζεύξης (L2) για κάθε **network interface controller (NIC)**, που αποστέλλει και δέχεται πληροφορίες, υπάρχει μια διεύθυνση **Media Access Control (MAC)**, γνωστή και ως **φυσική διεύθυνση**. Είναι ένας 48bit αριθμός που ταυτοποιεί μοναδικά κάθε διαφορετική συσκευή επιπέδου L2, ο οποίος αναπαρίσταται σε δεκαεξαδική μορφή, με έξι bytes που χωρίζονται με παύλα ή άνω και κάτω τελεία. Π.χ. 08-00-27-9B-86-A4 ή 08:00:27:9B:86:A4.

Κάθε συνδεδεμένος υπολογιστής στο διαδίκτυο, που έχει τουλάχιστον ένα NIC, μπορεί να ταυτοποιηθεί μοναδικά από την διεύθυνση MAC. Επίσης στην ίδια διεύθυνση MAC μπορούν χρησιμοποιούνται πολλαπλές διευθύνσεις IP. Για παράδειγμα σε έναν web server, δύναται από την ίδια ενσύρματη ζεύξη δικτύου (L2), δηλαδή το ίδιο καλώδιο (L1), να εξυπηρετούνται πολλαπλά sites (L5-L4), έχοντας το κάθε ένα με την δική του διαφορετική IP (L3).

Στο πρωτόκολλο **DHCP (Dynamic Host Configuration Protocol)** η διεύθυνση MAC χρησιμοποιείται για ταυτοποίηση, ώστε να αποδοθεί δυναμικά μια διεύθυνση IP σε έναν host που

αιτείται προς τον DHCP server. Οι δικτυακές συσκευές router, wireless access point ενσωματώνουν και έναν DHCP server, όπως και το λειτουργικό σύστημα Windows Server.

**E5.12** Βρείτε την MAC address του υπολογιστή σας με χρήση την εντολής `ipconfig /all` σε Windows και `ifconfig -a` σε Linux.

**E5.13** Δείτε τα MAC addresses των συσκευών που είναι συνδεδεμένες στο ίδιο ασύρματο δίκτυο με το κινητό σας. Για λειτουργικό σύστημα android χρησιμοποιήστε την εφαρμογή `fin`.

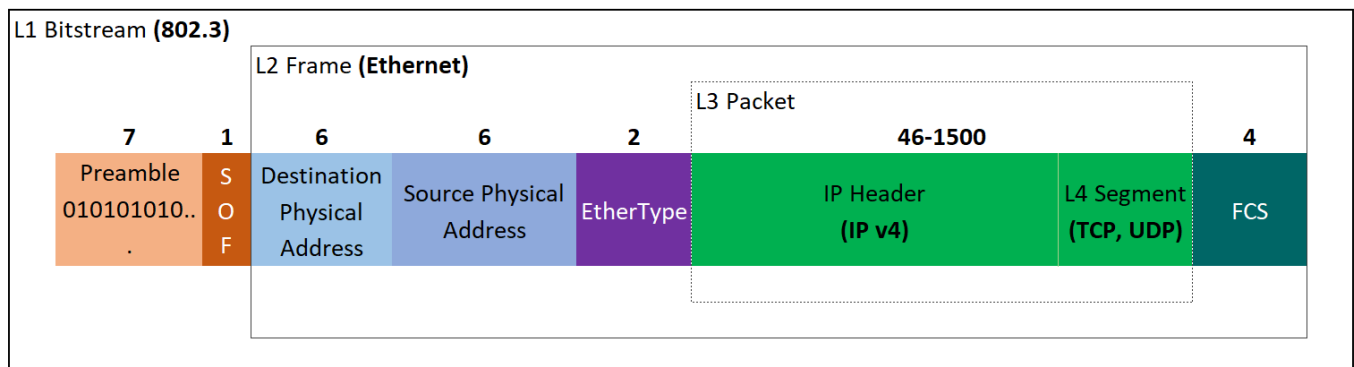
## Γ2) Ανάλυση περιεχομένων πλαισίου

Παρακάτω υπάρχει η δομή ενός πλαισίου (Ethernet frame) που αποτελεί το PDU στο επίπεδο ζεύξης (L2), και που αποτελείται από bytes (ή octets) και συνήθως αναπαρίσταται στο δεκαεξαδικό ως **hex bytes**:

6 octets	<b>Destination Address</b>	Η διεύθυνση στο L2 επίπεδο ζεύξης, της δικτυακής συσκευής που <b>στέλνει</b> το frame.
6 octets	<b>Source Address</b>	Η διεύθυνση στο L2 επίπεδο ζεύξης της δικτυακής συσκευής που <b>πρέπει να λάβει</b> το frame.
2 octets	<b>EtherType</b>	Ο <b>τύπος</b> του πρωτοκόλλου του L3 επιπέδου δικτύου, του οποίου τα δεδομένα έχουν ενθυλακωθεί στο frame.
46–1500 octets	<b>Data</b>	Τα δεδομένα του πρωτοκόλλου του L3 επιπέδου δικτύου. Το μήκος του πεδίου είναι το <b>maximum frame size</b> .
4 octets	<b>Frame Check Sequence (FCS)</b>	Ένας κωδικός που χρησιμοποιείται στον μηχανισμό ανίχνευσης λαθών μετάδοσης των frames. Ο πιο συνηθισμένος είναι ο <b>CRC</b> (Cyclic Redundancy Check).

## Bitstream

Στο φυσικό επίπεδο (L1) το PDU είναι το bit ή **σύμβολο (symbol)** και το frame θα αποσταλεί ως μια **ροή από bits (bitstream)**, που αναφέρεται και ως Ethernet packet ή 802.3 packet. Πριν αρχίσουν τα bits του frame αποστέλλεται το **preamble** που είναι ένα μοτίβο εναλλαγής μεταξύ 0 και 1 και χρησιμεύει στον συγχρονισμό του **bitstream** στα δύο μέρη της επικοινωνίας. Το preamble στο **802.3** που είναι η οικογένεια πρωτοκόλλων φυσικού επιπέδου για ενσύρματη δικτύωση, είναι 7bytes το κάθε ένα με τιμή 0b10101010 = 0xAA. Ακολουθεί ο οριοθέτης **start of frame (SOF)** που είναι ένα byte με τιμή 0xAB και βρίσκεται ακριβώς πριν την έναρξη του frame.



**Figure 1:** Ενθυλάκωση (encapsulation) των τμημάτων L4 σε πακέτα L3, των πακέτων L3 σε πλαίσια L2 και των πλαισίων ως μέρος μια ροής bit του L1.

## Άσκηση

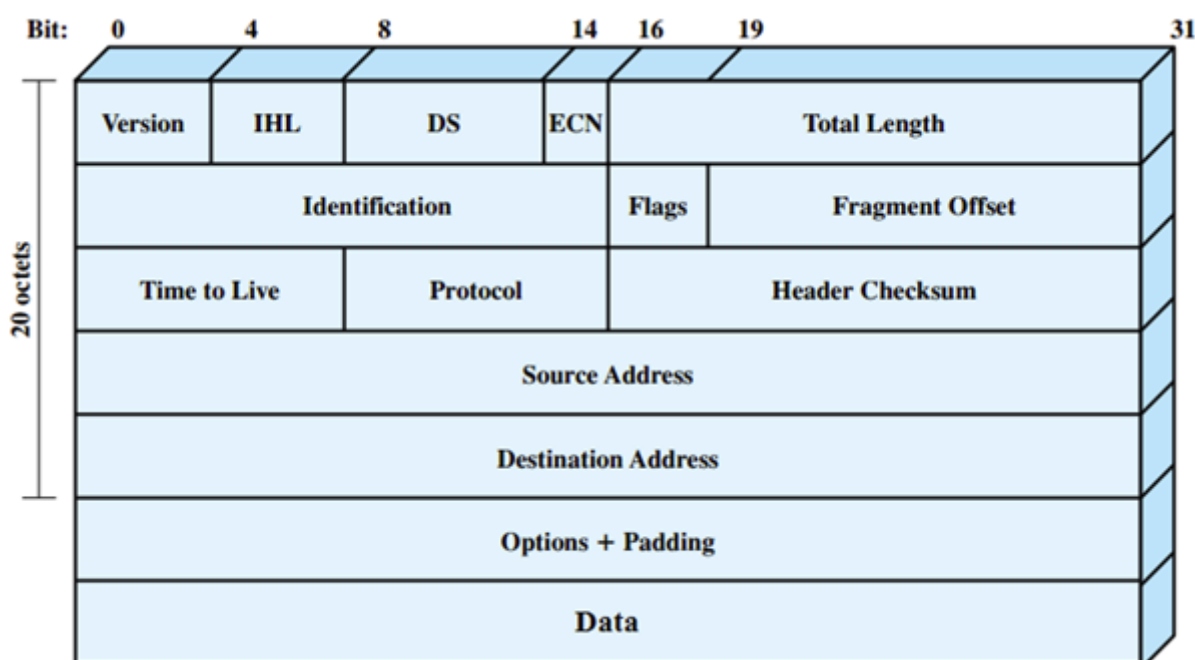
Στον φάκελο /Protocol Captures/TCP του αποθετηρίου του μαθήματος το αρχείο encapdecap-1.bin αναπαριστά ένα Ethernet frame σε δεκαεξαδική μορφή. Από την καταγραφή απουσιάζουν τα 4 bytes του FCS.

Μπορείτε να κατεβάσετε και να εγκαταστήσετε στα Windows έναν hex editor για να βλέπετε και να επεξεργάζεστε δυαδικά αρχεία από το <https://mh-nexus.de/en/hxd/>. Ανοίξτε το αρχείο με την εφαρμογή για να δείτε τα περιεχόμενα του.

**E5.14** Παρατηρήστε το αναγνώσιμο τμήμα του frame. Αυτή η πληροφορία σε ποιο επίπεδο ανήκει;

**E5.15** Σε κάποιο σημείο του frame υπάρχει κωδικοποιημένη στο δεκαεξαδικό η port που χρησιμοποιεί το πρωτόκολλο μεταφοράς, η οποία είναι η 53. Ποιο είναι το πρωτόκολλο εφαρμογής (L5) και ποιο το πρωτόκολλο μεταφοράς (L4) **Βοήθημα:** Επιτρέπεται να αναζητήσετε την δοθείσα port στο Internet σε λίστα με τα γνωστά ports, για να κατανοήσετε καλύτερα το παράδειγμα.

**E5.16** Στον IP header (κεφαλίδα) στο L3 υπάρχει το πεδίο Protocol που δείχνει το πρωτόκολλο μεταφοράς που ενθυλακώνει.



Εικόνα 5: Κεφαλίδα IP v4

Βρείτε την θέση μέσα στα hex bytes του frame για τον κωδικό του πρωτοκόλλου μεταφοράς. Αν έχετε ήδη καταλάβει ποιο είναι αυτό, αναζητήστε το με τον κωδικό του σε δεκαεξαδική μορφή.

**Βοήθημα:** [https://en.wikipedia.org/wiki/List\\_of\\_IP\\_protocol\\_numbers](https://en.wikipedia.org/wiki/List_of_IP_protocol_numbers)

**E5.17** Αναλύστε τα hex bytes του frame με το online εργαλείο <https://hpd.gasmi.net/> ώστε να κατανοήσετε σε βάθος πως λειτουργεί η ενθυλάκωση.

**ΠΡΟΣΟΧΗ:** Ο σκοπός είναι να κατανοήσετε πλήρως το θέμα και να αποκτήσετε την σχετική γνώση. Στις εξετάσεις θα απαιτηθεί αυτή η γνώση και όχι απλά η χρήση ενός εργαλείου.

**E5.18** Σε ποιο offset από την αρχή του frame υπάρχει το πεδίο type. Αναζητήστε την τιμή που περιέχει στην λίστα των EtherTypes: <https://en.wikipedia.org/wiki/EtherType>

**E5.19** Αν σας δινόταν τα bits του πρωτοκόλλου 802.3, που έχουν καταγραφεί να περνούν μέσα από το καλώδιο στο τοπικό σας δίκτυο, μπορείτε να τα μετατρέψετε σε hex bytes και κατόπιν να αναλύσετε το frame (Θυμηθείτε τα *nibbles*); Ποια επιπλέον bytes μπορεί να υπάρχουν σε αυτήν την περίπτωση.