Εργαστηριακή Άσκηση 5
Πρωτόκολλο IP

Ο σκοπός αυτού του εργαστηρίου είναι η σε μεγαλύτερο βάθος εξέταση των ιδιοτήτων του πρωτοκόλλου IP. Θα παρατηρήσετε τα πακέτα IP που παράγονται κατά την εκτέλεση εντολών όπως `ping` και `tracert`. Πιο συγκεκριμένα, θα μελετήσετε τα πεδία του πακέτου IP, καθώς και θα εμβαθύνετε στη λειτουργία του θρυμματισμού (fragmentation) των πακέτων IP. Περισσότερες πληροφορίες για το πρωτόκολλο IP μπορείτε να βρείτε στο Request-For-Comment – RFC 791 στην ιστοθέση http://www.ietf.org/rfc.html. Για τη δομή των επικεφαλίδων των πρωτοκόλλων της σουίτας TCP/IP επίσης συμβουλευθείτε και την ιστοσελίδα http://www.networksorcery.com/enp/default0604.htm επιλέγοντας το "IP protocol suite" από το αριστερό της μέρος και στη συνέχεια το πρωτόκολλο που σας ενδιαφέρει.

Όπως και στο προηγούμενο εργαστήριο, θα εργαστείτε με το πρόγραμμα Wireshark. Εδώ θα χρησιμοποιήσετε τη λειτουργία *Capture* με φίλτρο, ώστε τα πλαίσια που καταγράφονται να περιέχουν κάποια συγκεκριμένα χαρακτηριστικά. Υπενθυμίζεται ότι το φίλτρο απεικόνισης *(Display),* που επιλέγετε από το μενού *Analyze*, μπορεί να (απ)ενεργοποιηθεί οποιαδήποτε στιγμή κατά τη διάρκεια της καταγραφής, καθώς επίσης και μετά την ολοκλήρωση αυτής, προκειμένου να αποκρύπτει(αποκαλύπτει) κάποια από τα συλληφθέντα πλαίσια, ενώ το φίλτρο σύλληψης, που επιλέγετε από το μενού *Capture*, ενεργοποιείται πάντοτε **πριν** ξεκινήσει η διαδικασία καταγραφής, με αποτέλεσμα να καταγράφεται μόνο ένα μέρος των διερχόμενων πλαισίων.

Για να κάνετε μια καταγραφή με φίλτρο, από το μενού *Capture->Interfaces…* πιέστε το κουμπί *Options* δίπλα στο όνομα της κάρτας δικτύου του υπολογιστή σας. Στο παράθυρο που θα εμφανισθεί και στο πεδίο δίπλα από το κουμπί "*Capture Filter*" πληκτρολογήστε μια λογική έκφραση σύμφωνη με την σύνταξη των φίλτρων καταγραφής και πιέστε *Start* για να αρχίσει η καταγραφή. Όπως αναφέρθηκε και σε προηγούμενη εργαστηριακή άσκηση, 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.

1 Ο χρόνος ζωής των πακέτων IP

Στο προηγούμενο εργαστήριο είδατε ότι η διαδρομή που ακολουθεί ένα πακέτο IP μπορεί να ανιχνευθεί με την εντολή `tracert`. Η `tracert` στέλνει μηνύματα ICMP 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. Όταν το TTL μηδενισθεί, ο δρομολογητής οφείλει να στείλει μήνυμα ICMP

τύπου *Time Exceeded* 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.*

Προτού ξεκινήσετε την άσκηση, δημιουργήστε ένα φίλτρο σύλληψης, ώστε να καταγράφονται μόνο τα πλαίσια που περιλαμβάνουν τη διεύθυνση MAC του υπολογιστή σας. Καταγράψτε τα διερχόμενα πλαίσια όταν εκτελείτε την εντολή `tracert -d 195.130.89.210`.

1.1 Ποια είναι η σημασία της παραμέτρου `-d` που χρησιμοποιήσατε κατά την κλήση της `tracert`; *[Υπόδειξη: `tracert /?`]*
1.2 Καταγράψτε τη σύνταξη του φίλτρου σύλληψης που χρησιμοποιήσατε ώστε να συλλαμβάνονται μόνο τα πλαίσια που περιλαμβάνουν τη διεύθυνση MAC του υπολογιστή σας.

Εφαρμόστε τώρα φίλτρο απεικόνισης ώστε να παραμείνουν μόνο πλαίσια σχετιζόμενα με το πρωτόκολλο ICMP.

1.3 Γράψτε τη σύνταξη του φίλτρου απεικόνισης που χρησιμοποιήσατε.

Επιλέξτε ένα μήνυμα ICMP τύπου *Echo Request* και στο αντίστοιχο παράθυρο παρατηρείστε τις λεπτομέρειες της επικεφαλίδας που σχετίζονται με το πρωτόκολλο IP καθώς και τα σχετικά με αυτές περιεχόμενα του πακέτου IP.

1.4 Ποια είναι η διεύθυνση IP του υπολογιστή σας; Σε ποιο πεδίο της επικεφαλίδας IP εμφανίζεται αυτή;
1.5 Καταγράψτε την τιμή του πεδίου Protocol της επικεφαλίδας IP του μηνύματος ICMP *Echo request*.
1.6 Πόσα byte έχει η επικεφαλίδα IP;
1.7 Πόσα byte μεταφέρει το πακέτο IP στο πεδίο δεδομένων;
1.8 Εξηγείστε πώς προσδιορίζεται το παραπάνω μήκος του πεδίου δεδομένων από τα στοιχεία που περιέχει η επικεφαλίδα.

Στη συνέχεια ταξινομείστε κατά φθίνουσα σειρά τα πακέτα IP σύμφωνα με τη διεύθυνση IP της πηγής τους (Source) κάνοντας κλικ στην αντίστοιχη επικεφαλίδα του παράθυρου με τη λίστα καταγεγραμμένων πακέτων. Εάν το μικρό σημάδι 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.

1.9 Ποια πεδία της επικεφαλίδας IP αλλάζουν πάντα από το ένα πακέτο στο επόμενο (της σειράς μηνυμάτων ICMP που έστειλε ο υπολογιστής σας);
1.10 Ποια πεδία της επικεφαλίδας IP παραμένουν αμετάβλητα;
1.11 Ποια πεδία της επικεφαλίδας IP πρέπει να παραμείνουν αμετάβλητα και γιατί;
1.12 Ποια πεδία της επικεφαλίδας IP ***πρέπει*** να αλλάξουν και γιατί;

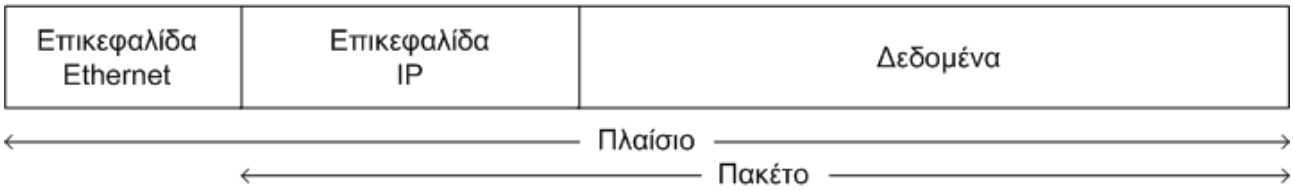
Στη συνέχεια με τα μηνύματα ταξινομημένα όπως πριν, βρείτε τη σειρά μηνυμάτων ICMP τύπου *Time Exceeded* που στέλνονται από τον κοντινότερο προς τον υπολογιστή σας δρομολογητή.

1.13 Ποια είναι η διεύθυνση IP του κοντινότερου προς τον υπολογιστή σας δρομολογητή;

1.14 Ποια είναι η τιμή του πεδίου TTL της επικεφαλίδας IP του πρώτου πακέτου της σειράς;
1.15 Παραμένουν οι τιμές του πεδίου αυτού σταθερές για όλα τα πακέτα της σειράς; Γιατί;

2 Θρυμματισμός (Fragmentation) στο IP

Κάθε δίκτυο επιβάλει ένα μέγιστο μέγεθος στα πακέτα του. Π.χ. σε ένα Ethernet LAN το μέγιστο μέγεθος πλαισίου είναι το πολύ 1.518 byte, ενώ το μέγιστο μέγεθος πακέτου IP είναι 65.535 byte (το ελάχιστο μέγεθος πλαισίου του Ethernet είναι 64 byte). Ένα προφανές πρόβλημα θα εμφανισθεί όταν ένα μεγάλο πακέτο IP θέλει να ταξιδεύσει μέσω ενός δικτύου όπου το μέγιστο μέγεθος πακέτου είναι μικρό. Η λύση του προβλήματος είναι τα πακέτα να κόβονται σε **κομμάτια ή θραύσματα (*fragments*)** και το κάθε θραύσμα να μεταδίδεται ως ξεχωριστό πακέτο IP. Κάθε υποδίκτυο IP έχει μια μέγιστη μονάδα μεταφοράς MTU (Maximum Transmission Unit) που αντιστοιχεί στο μέγεθος του μεγαλύτερου **πακέτου** που μπορεί να μεταδοθεί χωρίς θρυμματισμό. Συνήθη μεγέθη της MTU είναι 1500, 1492, 1006, 576, 552, 544, 512, 508, 296. Στο διαδίκτυο όλοι οι κόμβοι απαιτείται να δέχονται πακέτα IP μέχρι 576 byte, είτε ολόκληρα είτε θρυμματισμένα. Για να στείλουν πακέτα IP μεγαλύτερου μήκους πρέπει να ελέγχουν ότι ο προορισμός μπορεί να τα δεχθεί. Στο τοπικό δίκτυο μπορούν να στείλουν πακέτα IP μέχρι το μέγεθος της MTU. Όταν τα θραύσματα φτάσουν στον τελικό προορισμό τους ο παραλήπτης φροντίζει για την ανασύνθεση τους σε πακέτα, με τη βοήθεια των ειδικών γι' αυτό τον σκοπό πεδίων (*Identification, Fragment offset* και *More fragments flag*) στην επικεφαλίδα κάθε πακέτου IP. Η ανασύνθεση γίνεται μόνο από τον τελικό παραλήπτη, ενώ ο θρυμματισμός μπορεί να γίνει από οποιονδήποτε από τους ενδιάμεσους σε ένα μονοπάτι δρομολόγησης, σύμφωνα με τις ανάγκες.



Στα πακέτα IP όμως, μπορεί να υπάρχει μια σημαία μη θρυμματισμού (*Don't fragment flag*). Αν κάποιος υπολογιστής ή δρομολογητής συναντήσει ένα πακέτο IP μεγαλύτερο της MTU (του δικτύου μέσα από το οποίο πρέπει να το στείλει) με την ένδειξη do not fragment, είναι υποχρεωμένος να απαντήσει με ένα ICMP μήνυμα *"Packet needs to be fragmented but DF set"*. Με τον τρόπο αυτό οι σταθμοί και οι δρομολογητές μπορούν να εντοπίσουν την ελάχιστη MTU στο μονοπάτι δρομολόγησης και να ρυθμίσουν ανάλογα τις αποστολές τους, έτσι ώστε να αποφεύγεται ο υπερβολικός θρυμματισμός.

Ένας τρόπος λοιπόν για να εξακριβώσετε την τιμή της MTU, είναι να στείλετε ένα μήνυμα ICMP *Echo Request* με ενεργοποιημένη την παράμετρο που εμποδίζει τον θρυμματισμό του πακέτου, καθορίζοντας ταυτόχρονα και το μέγεθος του πακέτου (βλ. βοήθεια για το `ping`). Εάν το συνολικό μήκος πακέτου IP που προκύπτει είναι μεγαλύτερο από την MTU, τότε το μήνυμα ICMP δε θα μεταδοθεί και θα εμφανιστεί μήνυμα λάθους, ενώ σε αντίθετη περίπτωση θα πραγματοποιηθεί η αποστολή.

Χρησιμοποιείστε την εντολή: `ping -n 1 -l` *`nnnn`* `-f <διεύθυνση IP>`, για διάφορες τιμές της μεταβλητής *nnnn* (στην περιοχή του 1480), επιλέγοντας για διεύθυνση IP αυτή κάποιου ενεργού υπολογιστή που ανήκει στο ίδιο τοπικό δίκτυο (π.χ. του διπλανού σας).

2.1 Ποια η σημασία της παραμέτρου `-n` με όρισμα `1` (=ο αριθμός ένα) κατά την κλήσης της εντολής `ping`;
2.2 Ποια η σημασία της παραμέτρου `-f` κατά την κλήσης της εντολής `ping`;
2.3 Ποια η σημασία της παραμέτρου `-l` κατά την κλήσης της εντολής `ping`;

Με τη βοήθεια της παραπάνω εντολής, βρείτε τα ακόλουθα μεγέθη:
2.4 Τη μέγιστη τιμή της *nnnn* για την οποία δεν εμφανίζεται θρυμματισμός.
2.5 Τη μικρότερη τιμή της *nnnn* για την οποία απαιτείται θρυμματισμός.

Στη συνέχεια χρησιμοποιείστε το Wireshark με φίλτρο σύλληψης ώστε να καταγράφονται μόνο πλαίσια μονο-εκπομπής (unicast) όταν κάνετε `ping -n 1 -l` *nnnn* `-f <διεύθυνση IP του διπλανού σας>`. Όπου *nnnn*, θα χρησιμοποιήσετε διαδοχικά τις δύο τιμές που προσδιορίσατε προηγουμένως στα ερωτήματα 2.4 και 2.5, αντίστοιχα. Μόλις ολοκληρώσετε την καταγραφή, εφαρμόστε ένα φίλτρο απεικόνισης ώστε να παραμείνουν μόνο πακέτα IP από και προς τη διεύθυνση IP που χρησιμοποιείτε στο `ping`.

2.6 Γράψτε τη σύνταξη του φίλτρου σύλληψης που χρησιμοποιήσατε. *[Υπόδειξη: Συμβουλευτείτε τη σελίδα http://wiki.wireshark.org/CaptureFilters]*
2.7 Γράψτε τη σύνταξη του φίλτρου απεικόνισης που εφαρμόσατε.
2.8 Ποιο είναι το μέγεθος της MTU; Αιτιολογήστε. *[Υπόδειξη: nnnn είναι τα byte δεδομένων του μηνύματος ICMP]*
2.9 Εξηγείστε γιατί δεν παρατηρείτε την αποστολή μηνυμάτων ICMP όταν η παράμετρος *nnnn* λαμβάνει την τιμή του ερωτήματος 2.5;

Στην συνέχεια με τα ίδια φίλτρα σύλληψης και απεικόνισης αρχίστε την καταγραφή πακέτων (με το Wireshark) που παράγονται όταν κάνετε `ping -n 1 -l 6000 <διεύθυνση IP του διπλανού σας>`.

2.10 Βρείτε το πρώτο μήνυμα ICMP τύπου Echo Request που έστειλε ο υπολογιστής σας. Έχει αυτό το μήνυμα μεταφερθεί ως **ένα** πακέτο IP;
2.11 Εάν όχι, πόσα πακέτα IP χρειάσθηκαν και γιατί;
2.12 Για καθένα από αυτά τα πακέτα IP, καταγράψτε τις τιμές των πεδίων της επικεφαλίδας που σχετίζονται με τον θρυμματισμό (*Identification, Fragment Offset, Don't Fragment Bit, More Fragments Bit)*.

Επιλέξτε το πρώτο από τα παραπάνω πακέτα IP (το πρώτο θραύσμα).

2.13 Ποια πληροφορία της επικεφαλίδας IP δηλώνει ότι το πακέτο έχει θρυμματιστεί;
2.14 Ποια πληροφορία της επικεφαλίδας IP δηλώνει ότι αυτό είναι το πρώτο θραύσμα και όχι ένα μεταγενέστερο;
2.15 Ποιο είναι το μήκος του;

Επιλέξτε το δεύτερο από τα παραπάνω πακέτα IP (το δεύτερο θραύσμα).

2.16 Ποια πληροφορία της επικεφαλίδας IP δηλώνει ότι δεν είναι το πρώτο θραύσμα;
2.17 Ακολουθούν άλλα θραύσματα;
2.18 Πώς το αναγνωρίζετε από τις πληροφορίες της επικεφαλίδας μόνο;
2.19 Ποια πεδία της επικεφαλίδας IP αλλάζουν μεταξύ του πρώτου και του δεύτερου θραύσματος;
2.20 Δικαιολογήστε τις τιμές του πεδίου Fragment offset για το προτελευταίο και το τελευταίο θραύσμα που στάλθηκε.
2.21 Ποια πεδία της επικεφαλίδας IP αλλάζουν μεταξύ των θραυσμάτων;

Στην συνέχεια χρησιμοποιείστε την εντολή `ping -n 1 -l` *nnnn* `<διεύθυνση IP του διπλανού σας>`.

2.22 Ποια η μέγιστη τιμή της *nnnn*; *[Σημείωση: η μέγιστη τιμή για μήκος πακέτου IP είναι 65.535 byte]*.

Η δικτυακή διεπαφή του υπολογιστή `edu-dy.cn.ntua.gr` δεν έχει την MTU που βρήκατε πριν. Για να προσδιορίσετε την τιμή της, εκτελέστε την εντολή `ping -n 1 -l` *nnnn* `-f edu-dy.cn.ntua.gr` για τις διάφορες συνήθεις τιμές της MTU (που δίδονται πιο πάνω) αρχίζοντας από την πιο μεγάλη.

2.23 Ποια η μέγιστη τιμή της *nnnn* για την οποία λαμβάνετε απάντηση;
2.24 Ποια η MTU της δικτυακής διεπαφής του `edu-dy.cn.ntua.gr`.

3 IP – Τύπος Υπηρεσίας

Το πεδίο DS/ECN (Differentiated Services/Explicit Congestion Notification) της επικεφαλίδας IP καθορίζει τον τρόπο χειρισμού των πακέτων κατά τη διάβασή τους μέσω του δικτύου. Παλαιότερα αποκαλούνταν TOS (Type of Service). Ο ρόλος του άλλαξε, αλλά υπάρχει συμβατότητα προς τα πίσω. Μπορείτε να βρείτε την σημασία των bit του πεδίου TOS στην ιστοσελίδα *http://www.networksorcery.com/enp/protocol/ip.htm#TOS,%20Type%20of%20Service*.

Να γίνει καταγραφή των διερχόμενων πακέτων κατά τη χρήση των υπηρεσιών Telnet και FTP του υπολογιστή `edu-dy.cn.ntua.gr` με διεύθυνση IP `147.102.40.9`. Για τη χρήση της υπηρεσίας Telnet πληκτρολογήστε `telnet edu-dy.cn.ntua.gr` σε ένα παράθυρο εντολών. Στην προτροπή `login:` πληκτρολογήστε `<Ctrl>+]` και στην προτροπή `Microsoft Telnet>` δίνετε την εντολή `quit` για έξοδο. Στη συνέχεια, για την υπηρεσία FTP του ίδιου υπολογιστή, πληκτρολογήστε `ftp edu-dy.cn.ntua.gr` σε ένα παράθυρο εντολών. Στην προτροπή `User:` πληκτρολογήστε `anonymous` ακολουθούμενο από `<Enter>`, ενώ στην προτροπή `Password:` πληκτρολογήστε το e-mail σας ακολουθούμενο από `<Enter>`. Εκτελέστε την εντολή `ls`, ώστε να δείτε τα αρχεία που βρίσκονται στον εξυπηρετητή (αν εμφανιστεί παράθυρο σχετικό με το τείχος πυρασφάλειας (firewall) των Windows πατήστε OK). Τέλος πληκτρολογήστε `bye` για να τερματίσετε την εφαρμογή `ftp` και σταματήστε την καταγραφή των πακέτων.

Εφαρμόστε στο Wireshark το φίλτρο απεικόνισης `telnet` ώστε να παραμείνουν μόνο μηνύματα σχετιζόμενα με το πρωτόκολλο TELNET και στη συνέχεια ταξινομείστε τα κατά φθίνουσα σειρά σύμφωνα με τη διεύθυνση IP της πηγής τους (Source) κάνοντας κλικ στην αντίστοιχη επικεφαλίδα του παράθυρου με τη λίστα καταγεγραμμένων πακέτων.

3.1 Παρατηρείστε τα μηνύματα Telnet του εξυπηρετητή προς το σταθμό σας και καταγράψετε την τιμή του πεδίου *Differentiated Services Field* της επικεφαλίδας IP.
3.2 Τι αντιπροσωπεύει η τιμή που καταγράψατε και γιατί επιλέχθηκε για την υπηρεσία Telnet; *[Υπόδειξη: Πληροφορίες για τη σημασία της τιμής κάθε bit του πεδίου TOS της επικεφαλίδας IP μπορείτε να βρείτε στην ιστοσελίδα http://www.networksorcery.com/enp/protocol/ip.htm ακολουθώντας το σύνδεσμο TOS που υπάρχει στη σελίδα αυτή]*.
3.3 Παρατηρείστε τα μηνύματα Telnet του σταθμού σας προς τον εξυπηρετητή και καταγράψετε την τιμή του πεδίου *Differentiated Services Field* της επικεφαλίδας IP.
3.4 Η εφαρμογή Telnet στο σταθμό σας υποστηρίζει την ποιότητα υπηρεσίας που χρησιμοποιεί ο εξυπηρετητής;

Αφού διαγράψετε το παλαιό φίλτρο απεικόνισης, εφαρμόστε τώρα το φίλτρο απεικόνισης `ftp` ώστε να παραμείνουν μόνο μηνύματα σχετιζόμενα με τον ***έλεγχο*** στο πρωτόκολλο FTP και στη συνέχεια ταξινομείστε τα κατά φθίνουσα σειρά σύμφωνα με τη διεύθυνση IP της πηγής τους

κάνοντας κλικ στην αντίστοιχη επικεφαλίδα του παράθυρου με τη λίστα καταγεγραμμένων πακέτων.

3.5 Παρατηρείστε τα μηνύματα *ελέγχου* FTP από τον εξυπηρετητή προς το σταθμό σας και καταγράψετε την τιμή του πεδίου *Differentiated Services Field* της επικεφαλίδας IP.
3.6 Τι αντιπροσωπεύει η τιμή που καταγράψατε και γιατί επιλέχθηκε για τα πακέτα που σχετίζονται με τον έλεγχο της υπηρεσίας FTP;

Αφού διαγράψετε το προηγούμενο φίλτρο απεικόνισης, εφαρμόστε τώρα το φίλτρο απεικόνισης `ftp-data` ώστε να παραμείνουν μόνο μηνύματα σχετιζόμενα με τη *μεταφορά δεδομένων* στο πρωτόκολλο FTP.

3.7 Παρατηρείστε τα μηνύματα *μεταφοράς δεδομένων* FTP από τον εξυπηρετητή προς τον σταθμό σας και καταγράψετε την τιμή του πεδίου *Differentiated Services Field* της επικεφαλίδας IP.
3.8 Τι αντιπροσωπεύει η τιμή που καταγράψατε και γιατί επιλέχθηκε για τα πακέτα που σχετίζονται με τη μεταφορά δεδομένων της υπηρεσίας FTP;

Ονοματεπώνυμο:	**Όνομα PC:**
Ομάδα:	**Ημερομηνία:**
Διεύθυνση IP: . . .	**Διεύθυνση MAC: - - - - -**

Εργαστηριακή Άσκηση 5
Πρωτόκολλο IP

Απαντήστε στα ερωτήματα στον χώρο που σας δίνεται παρακάτω και στην πίσω σελίδα εάν δεν επαρκεί. Το φυλλάδιο αυτό θα παραδοθεί στον επιβλέποντα.

1

1.1 .....

1.2 .....

1.3 .....

1.4 .....

1.5 .....

1.6 .....

1.7 .....

1.8 .....

.....

1.9 .....

1.10 .....

1.11 .....

.....

.....

1.12 .....

.....

.....

1.13 .....

1.14 .....

1.15 .....

.....

2

2.1 .....

.....

2.2 .....

.....

2.3 .....

.....