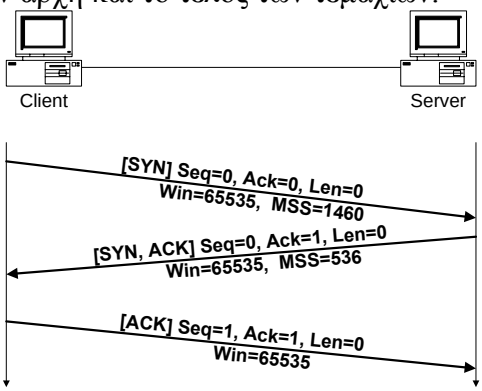
Εργαστηριακή Άσκηση 7
Πρωτόκολλα TCP και UDP

Ο σκοπός αυτής της εργαστηριακής άσκησης είναι η εξέταση των ιδιοτήτων των πρωτοκόλλων μεταφοράς TCP και UDP του Internet. Πληροφορίες για τα πρωτόκολλα αυτά μπορείτε να βρείτε στις σελίδες http://www.networksorcery.com/enp/protocol/tcp.htm και http://www.networksorcery.com/enp/protocol/udp.htm, αντίστοιχα. Για την πραγματοποίηση κάποιων από τις επιμέρους ασκήσεις, θα πρέπει να χρησιμοποιήσετε τον υπολογιστή σας σε συνεργασία με τον υπολογιστή του διπλανού σας. 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. Πληροφορίες για τη σύνταξη του φίλτρου σύλληψης μπορείτε να βρείτε στην ιστοθέση http://wiki.wireshark.org/CaptureFilters. Για να κάνετε μια καταγραφή με φίλτρο, από το μενού *Capture->Options…* στο παράθυρο που θα εμφανισθεί και στο πεδίο δίπλα από το κουμπί "*Capture Filter*" πληκτρολογήστε μια λογική έκφραση σύμφωνη με τη σύνταξη των φίλτρων καταγραφής και πιέστε *Start* για να αρχίσει η καταγραφή.

Το TCP είναι πρωτόκολλο με συνδέσεις (connection-oriented). Παρέχει αξιόπιστη μετάδοση συρμού byte απ' άκρη σ' άκρη πάνω από μη αξιόπιστο δίκτυο. Το TCP παραδίδει τα δεδομένα προς το IP σε τεμάχια[1]. Όμως, προς τα ανώτερα στρώματα, το TCP παραδίδει τα δεδομένα ως ακολουθία από byte χωρίς να καθορίζει όρια μεταξύ των byte. Έτσι τα ανώτερα στρώματα δεν γνωρίζουν την αρχή και το τέλος των τεμαχίων.



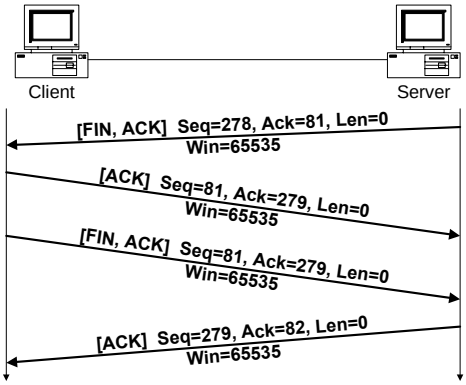
Πριν από οποιανδήποτε μεταφορά δεδομένων, το TCP εγκαθιστά μια σύνδεση. Η εγκατάσταση της σύνδεσης αρχίζει όταν ο πελάτης TCP στέλνει μια αίτηση σύνδεσης στον εξυπηρετητή TCP[2]. Για την εγκατάσταση μιας σύνδεσης TCP ανταλλάσσονται τρία τεμάχια, όπως στο προηγούμενο σχήμα, σύμφωνα με μια διαδικασία που είναι γνωστή ως *τριμερής χειραψία* (*3-way handshake*). Κατά τη διάρκεια της τριμερούς χειραψίας δεν μεταφέρονται δεδομένα, αλλά γίνεται διαπραγμάτευση για βασικές παραμέτρους της σύνδεσης TCP, όπως οι αρχικοί αύξοντες αριθμοί, το μέγιστο μέγεθος τεμαχίου και το μέγεθος του παραθύρου για

[1] Στο πρωτόκολλο TCP η μονάδα ανταλλασσόμενης πληροφορίας αποκαλείται *τεμάχιο (segment)*. Αντιπαραβάλετε, *πακέτο* για το πρωτόκολλο IP και *πλαίσιο* για το Ethernet.
[2] Ο εξυπηρετητής TCP πρέπει να τρέχει όταν ζητείται η σύνδεση.

τον έλεγχο ροής. Μετά μπορεί να ακολουθήσει αμφίδρομη ροή δεδομένων με τα τεμάχια που ανταλλάσσονται.

Το TCP χρησιμοποιεί μια παραλλαγή του πρωτοκόλλου ολισθαίνοντος παραθύρου για τον έλεγχο ροής μεταξύ πομπού και δέκτη, ώστε να εξασφαλίζει την αξιόπιστη και με τη σειρά παράδοση των byte. Ο αύξων αριθμός (sequence number) στην επικεφαλίδα TCP δηλώνει τον αριθμό του πρώτου byte στα δεδομένα του τεμαχίου. Ο αριθμός επαλήθευσης (acknowledgement number) είναι ο αύξων αριθμός του επόμενου byte που αναμένεται από την άλλη πλευρά. Οι επαληθεύσεις είναι συσωρευτικές, δηλαδή, επαληθεύουν τη λήψη μέχρι και του προηγούμενου από το δηλούμενο byte.

Η απόλυση της σύνδεσης γίνεται με τρία ή τέσσερα τεμάχια, όπως στο επόμενο σχήμα. Κατά την απόλυση της σύνδεσης, η κάθε πλευρά διακόπτει τη ροή δεδομένων *ανεξάρτητα* από την άλλη (half close).



Το TCP δε διαθέτει ειδικά τεμάχια για την εγκατάσταση και απόλυση των συνδέσεων, αντίθετα χρησιμοποιεί σημαίες μήκους 1 bit (bit flags) στην επικεφαλίδα TCP για να μεταφέρει την πληροφορία ελέγχου. Για την εγκατάσταση και απόλυση των συνδέσεων χρησιμοποιούνται οι σημαίες SYN, ACK και FIN.

1 Απόρριψη σύνδεσης TCP

Δημιουργήστε ένα φίλτρο σύλληψης στο Wireshark ώστε να καταγράφονται μόνο πακέτα IP που περιλαμβάνουν τη διεύθυνση IP του υπολογιστή σας, ανοίξτε ένα παράθυρο εντολών και καταγράψτε την κίνηση που παράγεται όταν κάνετε telnet στον υπολογιστή `1.1.1.1` (που *δεν* υπάρχει) *[Περίπτωση Α]*. Μετά επιχειρήστε telnet στον υπολογιστή `2.2.2.2` που επίσης *δεν* υπάρχει *[Περίπτωση Β]*. Στη συνέχεια, επαναλάβετε με telnet σε έναν υπολογιστή που υπάρχει, αλλά δεν είναι εξυπηρετητής, π.χ. στον υπολογιστή του διπλανού σας *[Περίπτωση Γ]*. Τέλος, επιχειρείστε telnet στον υπολογιστή `147.102.40.1` όπου όμως δε γίνονται δεκτές τέτοιες συνδέσεις *[Περίπτωση Δ]*. Όταν τελειώσει η διαδικασία, σταματήστε την καταγραφή των πακέτων. Με βάση τα αποτελέσματα απαντήστε στα παρακάτω ερωτήματα.

1.1 Καταγράψτε τη σύνταξη του φίλτρου σύλληψης που χρησιμοποιήσατε ώστε να συλλαμβάνονται μόνο τα πακέτα που περιλαμβάνουν τη διεύθυνση IP του υπολογιστή σας.

1.2 Σε ποια θύρα (του άλλου υπολογιστή) προσπαθεί να συνδεθεί ο δικός σας υπολογιστής; *[Υπόδειξη: Μπορείτε να βρείτε τις πιο συχνά χρησιμοποιούμενες πασίγνωστες θύρες στην ιστοσελίδα http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers]*.

1.3 Εφαρμόστε ένα φίλτρο απεικόνισης ώστε να παραμείνουν μόνο τα τεμάχια που σχετίζονται με τη θύρα αυτή. Ποια είναι η σύνταξή του; *[Υπόδειξη: Αναζητήστε την κατάλληλη έκφραση φίλτρου μεταξύ των σχετικών επιλογών για το πρωτόκολλο TCP που θα βρείτε πατώντας το πλήκτρο Expression δίπλα στο πεδίο για την εισαγωγή φίλτρου απεικόνισης]*.

1.4 Ποια σημαία μήκους 1 bit ενεργοποιείται για την εκκίνηση της εγκατάστασης της σύνδεσης TCP;
1.5 Πόσες προσπάθειες κάνει ο υπολογιστής σας προκείμενου να εγκαταστήσει σύνδεση TCP στις Περιπτώσεις Α-Γ;
1.6 Καταγράψτε τη χρονική απόσταση μεταξύ των διαδοχικών προσπαθειών εγκατάστασης σύνδεσης. *[Υπόδειξη: Από το μενού View μπορείτε να επιλέξετε Time Display Format → Seconds Since Previous Displayed Packet]*.
1.7 Τι παρατηρείτε συγκρίνοντας τα αποτελέσματα των τριών περιπτώσεων;
1.8 Ποια βήματα της τριμερούς χειραψίας παρατηρήσατε;
1.9 Ο υπολογιστής σας απολύει τη σύνδεση ή απλώς εγκαταλείπει την προσπάθεια;

Στη συνέχεια, εφαρμόστε νέο φίλτρο απεικόνισης ώστε να παραμείνουν μόνο τα τεμάχια που σχετίζονται με τον υπολογιστή της Περίπτωσης Δ.

1.10 Ποια είναι η σύνταξή του;
1.11 Πόσες προσπάθειες κάνει ο υπολογιστής σας προκείμενου να εγκαταστήσει σύνδεση TCP;
1.12 Ποια σημαία μήκους 1 bit ενεργοποιείται για την άρνηση της εγκατάστασης σύνδεσης TCP;
1.13 Συγκρίνοντας με την απάντηση σας στο ερώτημα 1.7, τι συμπεραίνετε για το πότε επαναλαμβάνονται οι προσπάθειες εγκατάστασης της σύνδεσης;

Επιλέξτε ένα από τα τεμάχια TCP που στέλνει ο υπολογιστής σας προκειμένου να εγκαταστήσει σύνδεση με τον υπολογιστή `147.102.40.1`.

1.14 Ποιο είναι το μέγεθος της επικεφαλίδας και ποιο το μέγεθος του πεδίου δεδομένων αυτού του τεμαχίου TCP;
1.15 Να καταγραφεί το όνομα και το μήκος του πεδίου της επικεφαλίδας TCP που προσδιορίζει το μέγεθος της επικεφαλίδας TCP σύμφωνα με την ιστοσελίδα http://www.networksorcery.com/enp/protocol/tcp.htm. Ποιο όνομα χρησιμοποιεί το Wireshark για το πεδίο αυτό της επικεφαλίδας TCP στο παράθυρο με τις λεπτομέρειες του επιλεγμένου πακέτου;
1.16 Πώς προκύπτει η τιμή του σε σχέση με τη δεκαεξαδική τιμή που παρατηρείτε στα περιεχόμενα πακέτου σε δεκαεξαδική τιμή;
1.17 Υπάρχει πεδίο της επικεφαλίδας TCP που να δηλώνει το μήκος του τεμαχίου;
1.18 Πώς προκύπτει το μήκος αυτό με βάση τα στοιχεία των επικεφαλίδων IP και TCP;
1.19 Ποιο είναι το μέγεθος της επικεφαλίδας των τεμαχίων TCP που λαμβάνει ο υπολογιστής σας από τον υπολογιστή `147.102.40.1`;
1.20 Υπάρχει διαφορά στο μέγεθος της επικεφαλίδας TCP των δύο παραπάνω περιπτώσεων; Εάν ναι, που οφείλεται;

2 Εγκατάσταση σύνδεσης, μεταφορά δεδομένων και απόλυση σύνδεσης TCP

Χρησιμοποιώντας το προηγούμενο φίλτρο σύλληψης στο Wireshark, ώστε να καταγράφονται μόνο πακέτα IP που περιλαμβάνουν τη διεύθυνση IP του υπολογιστή σας, ανοίξτε ένα παράθυρο εντολών και καταγράψτε τα διερχόμενα πακέτα (με το Wireshark) όταν χρησιμοποιείτε την υπηρεσία FTP του υπολογιστή `edu-dy.cn.ntua.gr` με διεύθυνση IP `147.102.40.9`. Στην προτροπή `User:` πληκτρολογήστε `anonymous` ακολουθούμενο από `<Enter>`, ενώ στην προτροπή `Password:` πληκτρολογήστε το e-mail σας ακολουθούμενο από `<Enter>`. Στη συνέχεια, πληκτρολογήστε την εντολή `bin`, ώστε η μεταφορά αρχείων να γίνει σε δυαδική μορφή. Επιλέξτε την επιφάνεια εργασίας ως τον

προορισμό όπου επιθυμείτε να αποθηκεύσετε το πρόγραμμα με την εντολή `lcd desktop`. Κατεβάστε το `PCATTCP.exe` με την εντολή `get PCATTCP.exe` *[Προσοχή στα μικρά και κεφαλαία γράμματα]*. Τέλος, πληκτρολογήσετε `bye` για να τερματίσετε την εφαρμογή `ftp` και σταματήσετε την καταγραφή των πακέτων.

Εγκατάσταση σύνδεσης

Παρατηρείστε τα τεμάχια TCP που ανταλλάχθηκαν και εντοπίστε τα σχετικά με την τριπλή χειραψία πακέτα IP. Θα βρείτε δύο τριπλές χειραψίες: μία για την εγκατάσταση της σύνδεσης ελέγχου FTP και μία για τη μεταφορά δεδομένων FTP. *[Σημείωση: τα αρχικά τεμάχια εγκατάστασης και απόλυσης σύνδεσης έχουν διαφορετικό χρώμα]*.

2.1 Σε ποια θύρα του `edu-dy.cn.ntua.gr` προσπαθεί να συνδεθεί ο υπολογιστής σας για να αρχίσει η επικοινωνία με τον εξυπηρετητή FTP; *[Υπόδειξη: Συμβουλευθείτε την ιστοσελίδα http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers για τη θύρα FTP]*.

2.2 Με ποια θύρα (δεδομένων FTP) του υπολογιστή `edu-dy.cn.ntua.gr` γίνεται η σύνδεση για τη μεταφορά των δεδομένων (του αρχείου `PCATTCP.exe`);

Εφαρμόστε ένα *φίλτρο απεικόνισης* της μορφής `tcp.port` ώστε να παραμείνουν μόνο τα τεμάχια TCP *που σχετίζονται με τη θύρα ελέγχου FTP*.

2.3 Ποια είναι η σύνταξή του φίλτρου;
2.4 Πόσα τεμάχια ανταλλάσσονται για την εγκατάσταση της σύνδεσης ελέγχου FTP;
2.5 Ποιες σημαίες χρησιμοποιούνται για την εγκατάσταση της σύνδεσης TCP;
2.6 Ποιο είναι το μέγεθος των επικεφαλίδων TCP των τεμαχίων αυτών;
2.7 Ποιο είναι το μέγεθος δεδομένων των τεμαχίων αυτών;
2.8 Πόσο διαρκεί η διαδικασία εγκατάστασης της σύνδεσης; *[Υπόδειξη: Από το μενού View μπορείτε να επιλέξετε Time Display Format → Seconds Since Previous Displayed Packet]*.

Κατά την εγκατάσταση της σύνδεσης, ο πελάτης TCP και ο εξυπηρετητής TCP αναγγέλλουν ο ένας στον άλλο τους αύξοντες αριθμούς που θα χρησιμοποιήσουν κατά τη μετάδοση δεδομένων. Το πεδίο Sequence Number στην επικεφαλίδα TCP δείχνει τον αύξοντα αριθμό του πρώτου byte στο πεδίο δεδομένων που αποστέλλονται και το πεδίο Acknowledgement number δείχνει τον αύξοντα αριθμό του επόμενου byte δεδομένων που αναμένονται.

2.9 Ποιοι είναι οι απόλυτοι αρχικοί αύξοντες αριθμοί (Sequence Number) που ανακοινώνει η κάθε πλευρά; *[Υπόδειξη: Το Wireshark για ευκολία εμφανίζει τους σχετικούς αύξοντες αριθμούς. Για να δείτε τις απόλυτες τιμές επιλέξτε κάποια γραμμή για το πρωτόκολλο TCP στο παράθυρο με τις λεπτομέρειες επικεφαλίδας και κάντε δεξί κλικ. Στο παράθυρο που θα εμφανισθεί επιλέξτε το Protocol Preferences…, στη λίστα πρωτοκόλλων το TCP και φροντίστε να μην είναι επιλεγμένο το πεδίο Relative sequence numbers and window scaling. Πιέστε το Apply για να εμφανισθούν οι απόλυτες τιμές και μετά το Cancel για να επανέλθετε σε σχετική αρίθμηση.]*
2.10 Πώς προκύπτει ο αριθμός της επιβεβαίωσης (Acknowledgement Number) του τεμαχίου με το οποίο ο εξυπηρετητής FTP δηλώνει ότι αποδέχεται τη σύνδεση;
2.11 Πώς προκύπτουν ο αύξων αριθμός και ο αριθμός επιβεβαίωσης (Sequence Number και Acknowledgement Number) της επιβεβαίωσης του υπολογιστή σας προς τον εξυπηρετητή FTP για την εγκατάσταση της σύνδεσης;
2.12 Ποια είναι η μέγιστη τιμή που μπορεί να λάβουν οι αύξοντες αριθμοί και οι αριθμοί επιβεβαίωσης;

Το TCP χρησιμοποιεί έλεγχο ροής με ολισθαίνον παράθυρο. Σε κάθε τεμάχιο TCP η κάθε πλευρά ανακοινώνει στην άλλη το μέγεθος του παραθύρου (window), δηλαδή, το μέγιστο πλήθος byte που μπορεί να δεχθεί ή, ισοδύναμα, να στείλει η άλλη πλευρά. Ο έλεγχος ροής επιτυγχάνεται ως εξής: ο αποδέκτης διαφημίζει στην επικεφαλίδα της επαλήθευσης ένα παράθυρο (Win) σχετιζόμενο με το χώρο προσωρινής μνήμης που διαθέτει. Ο αποστολέας μπορεί να στείλει δεδομένα μέχρι το διαφημιζόμενο παράθυρο, δηλαδή, τα byte με αύξοντες αριθμούς SeqNo=AckNo, AckNo+1, …, AckNo + win -1.

2.13 Προσδιορίστε το μέγεθος των παράθυρων που ανακοινώνει ο υπολογιστής σας και ο εξυπηρετητής κατά τη διάρκεια της τριπλής χειραψίας.
2.14 Σε ποιο πεδίο της επικεφαλίδας μεταφέρεται η σχετική πληροφορία;
2.15 Ποιο είναι το μικρότερο και ποιο το μεγαλύτερο μέγεθος παραθύρου;.

Το TCP προσπαθεί να αποφύγει τον θρυμματισμό (fragmentation) των πακέτων IP. Όταν εγκαθίσταται η σύνδεση TCP, γίνεται διαπραγμάτευση του μέγιστου μεγέθους τεμαχίου (MSS - Maximum Segment Size)[3]. Τόσο ο πελάτης όσο και ο εξυπηρετητής TCP αποστέλλουν το MSS σε μία επιλογή (option) της επικεφαλίδας TCP του πρώτου τεμαχίου TCP που μεταδίδεται. Κάθε πλευρά θέτει τέτοια τιμή για το MSS, ώστε να μην γίνει θρυμματισμός στη διεπαφή δικτύου κατά την αποστολή του πακέτου IP. Η **ελάχιστη** MSS γίνεται αποδεκτή ως MSS για τη σύνδεση. Η ανταλλαγή των MSS αναφέρεται μόνο στους περιορισμούς στα δύο άκρα, αλλά όχι στους ενδιάμεσους δρομολογητές. Για να διαπιστωθεί η μικρότερη MTU (Maximum Transmission Unit) στη διαδρομή από τον αποστολέα ως τον παραλήπτη, το TCP χρησιμοποιεί μία μέθοδο γνωστή ως **Path MTU Discovery**, που λειτουργεί ως εξής: Ο αποστολέας πάντα ενεργοποιεί το "don't fragment" (DF) bit σε όλα τα πακέτα IP. Αν υπάρξει ανάγκη θρυμματισμού κάποιου πακέτου με ενεργοποιημένο το DF σε κάποιο δρομολογητή, τότε αυτός απορρίπτει το πακέτο και αποστέλλει ένα ICMP πακέτο τύπου "*Destination unreachable; Fragmentation needed*". Με τη λήψη ενός τέτοιου πακέτου, ο αποστολέας TCP ελαττώνει το MSS. Η διαδικασία συνεχίζεται μέχρι το MSS να λάβει τιμή που δεν παράγει τέτοια μηνύματα. Με βάση την προηγούμενη καταγραφή της κίνησης FTP, απαντήστε στα παρακάτω ερωτήματα.

2.16 Να καταγραφεί η τιμή του MSS που προτείνει ο υπολογιστής σας κατά την εγκατάσταση της σύνδεσης ελέγχου. *[Υπόδειξη: Αναζητήστε μεταξύ των παραμέτρων που εμφανίζονται στο παράθυρο με τη λίστα καταγεγραμμένων πακέτων]*.
2.17 Πώς προκύπτει η παραπάνω τιμή από την ισχύουσα MTU (1500 byte) για τον υπολογιστή σας;
2.18 Σε ποιο πεδίο της επικεφαλίδας TCP μεταφέρεται η τιμή του MSS;
2.19 Να καταγραφεί η τιμή του MSS που αντιπροτείνει ο `edu-dy.cn.ntua.gr`.
2.20 Πώς προκύπτει η παραπάνω τιμή από την ισχύουσα MTU (576 byte) για τον `edu-dy.cn.ntua.gr`;
2.21 Ποια είναι η τιμή του MSS που συμφωνείται κατά την τριμερή χειραψία TCP στη θύρα ελέγχου του FTP;

Απόλυση σύνδεσης

Στη συνέχεια, εντοπίστε τα τεμάχια TCP που σχετίζονται με την απόλυση της σύνδεσης ελέγχου FTP.

2.22 Ποια σημαία μήκους 1 bit ενεργοποιείται για την εκκίνηση της απόλυσης της σύνδεσης TCP;

[3] Το MSS είναι ο μέγιστος αριθμός δεδομένων του στρώματος εφαρμογής που περιέχονται στο τεμάχιο.

2.23 Ποια πλευρά εκκινεί τη διαδικασία απόλυσης;
2.24 Πόσα τεμάχια TCP ανταλλάσσονται συνολικά;
2.25 Ποιο είναι το μέγεθος των επικεφαλίδων TCP των τεμαχίων αυτών;
2.26 Ποιο είναι το μέγεθος δεδομένων των τεμαχίων αυτών;
2.27 Πόσα byte μεταδόθηκαν συνολικά στη σύνδεση ελέγχου FTP από κάθε πλευρά;
2.28 Με ποιο τρόπο προσδιορίσατε το πλήθος τους;

Μεταφορά δεδομένων

Ακυρώστε το τρέχον *φίλτρο απεικόνισης* και εφαρμόστε ένα νέο της μορφής `tcp.port` ώστε να παραμείνουν μόνο τα τεμάχια TCP *που σχετίζονται με τη θύρα δεδομένων FTP*.

2.29 Ποια είναι η σύνταξή του φίλτρου αυτού;
2.30 Ποια είναι η τιμή του MSS που συμφωνείται κατά την τριμερή χειραψία TCP στη θύρα δεδομένων FTP;
2.31 Ποια είναι η μέγιστη τιμή που θα μπορούσε να λάβει το MSS;

Εφαρμόστε τώρα το φίλτρο απεικόνισης `ftp-data` ώστε να εμφανίζονται μόνο τα τεμάχια TCP που αφορούν τη μεταφορά δεδομένων του FTP.

2.32 Παρατηρώντας την κίνηση που απομένει λόγω του παραπάνω φίλτρου, να καταγραφεί το μέγεθος πλαισίου (frame) σε byte και το μήκος των επικεφαλίδων Ethernet, IP και TCP του πρώτου μηνύματος FTP.
2.33 Ποια είναι η σχέση της παραπάνω τιμής με την τιμή του MSS που συμφωνείται κατά τη διάρκεια της τριμερούς χειραψίας TCP στη θύρα μεταφοράς δεδομένων του FTP;
2.34 Πόσα byte μεταδόθηκαν συνολικά στη σύνδεση δεδομένων από κάθε πλευρά;
2.35 Καταγράψτε τον συνολικό αριθμό byte που μεταδόθηκαν και στις δύο κατευθύνσεις, συμπεριλαμβάνοντας επικεφαλίδες Ethernet και IP. *[Υπόδειξη: Συμβουλευτείτε το μενού Statistics → Conversations tabs]*.

3 Μετάδοση δεδομένων με UDP

Το πρωτόκολλο μεταφοράς UDP παρέχει μια υπηρεσία "καλύτερης προσπάθειας" χωρίς σύνδεση (connectionless). Είναι μια μινιμαλιστική επέκταση της υπηρεσίας "best-effort" του IP. Τα δεδομενογράμματα UDP μπορεί να χαθούν (μη αξιόπιστη μετάδοση) ή να παραδοθούν εκτός σειράς στο ανώτερο στρώμα. Κάθε δεδομενόγραμμα UDP αντιμετωπίζεται ανεξάρτητα από τα άλλα. Το UDP είναι ένα λιτό πρωτόκολλο μεταφοράς για να στέλνει κανείς όσο γρήγορα μπορεί.

Με τη βοήθεια του Wireshark να καταγράψτε την κίνηση ενώ κάνετε χρήση της υπηρεσίας DNS. Εφαρμόστε φίλτρο σύλληψης για να παρατηρείτε μόνο την κίνηση που σχετίζεται με τη διεύθυνση IP του υπολογιστή σας και ξεκινήστε την καταγραφή. Ανοίξτε ένα παράθυρο εντολών και καθαρίστε την προσωρινή μνήμη DNS (DNS cache) που διατηρεί ο υπολογιστής χρησιμοποιώντας την εντολή φλοιού `ipconfig /flushdns`. Στη συνέχεια εκτελέστε την εντολή `nslookup edu-dy.cn.ntua.gr` ακολουθούμενη από `<Enter>` ώστε να ρωτήσετε τον τοπικό εξυπηρετητή DNS για τη διεύθυνση IP του υπολογιστή `edu-dy.cn.ntua.gr` και τερματίστε την καταγραφή. Στη συνέχεια εφαρμόστε φίλτρο απεικόνισης ώστε να παραμείνουν μόνο πακέτα IP που μεταφέρουν δεδομενογράμματα UDP.

3.1 Ποια είναι η σύνταξη του φίλτρου σύλληψης που χρησιμοποιήσατε;
3.2 Ποια είναι η σύνταξη του φίλτρου απεικόνισης που χρησιμοποιήσατε;

Παρατηρήστε το πρώτο δεδομενόγραμμα UDP που αποστάλθηκε από τον υπολογιστή σας.

3.3 Καταγράψτε τα ονόματα και το μήκος των πεδίων της επικεφαλίδας δεδομενογράμματος UDP.
3.4 Ποιο είναι το συνολικό μέγεθος της επικεφαλίδας UDP;
3.5 Ποιος είναι ο αριθμός πρωτοκόλλου για το UDP;
3.6 Ποιο είναι το μήκος του δεδομενογράμματος βάσει του μεγέθους του πακέτου IP εντός του οποίου ενθυλακώνεται;
3.7 Τι εκφράζει το πεδίο *μήκος (Length)* της επικεφαλίδας UDP;
3.8 Ποιο είναι το μέγιστο μέγεθος δεδομενογράμματος UDP που μπορεί να μεταφερθεί από ένα πακέτο IP; Αιτιολογήστε την απάντησή σας.

Παρατηρήστε τα μηνύματα DNS που ανταλλάχθηκαν.

3.9 Ποιο πρωτόκολλο μεταφοράς χρησιμοποιήθηκε για την επικοινωνία με τον εξυπηρετητή DNS (TCP ή UDP);
3.10 Ποια είναι η διεύθυνση IP του εξυπηρετητή DNS;
3.11 Καταγράψτε τις θύρες (προέλευσης και προορισμού) του πρωτοκόλλου μεταφοράς που χρησιμοποιήθηκαν για την πρώτη ερώτηση (query) και απόκριση (response) τύπου PTR.
3.12 Καταγράψτε τις θύρες (προέλευσης και προορισμού) του πρωτοκόλλου μεταφοράς που χρησιμοποιήθηκαν για τη δεύτερη ερώτηση και απόκριση τύπου A.
3.13 Ποια από τις παραπάνω θύρες αντιστοιχεί στο πρωτόκολλο εφαρμογής DNS;

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

Εργαστηριακή Άσκηση 7
Πρωτόκολλα TCP και UDP

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 .....

.....

1.16 .....

1.17 .....

1.18 .....

.....

1.19 .....

1.20 .....

.....

2

2.1 .....

2.2 .....

3