Εργαστηριακή Άσκηση 7
Πρωτόκολλα TCP και UDP

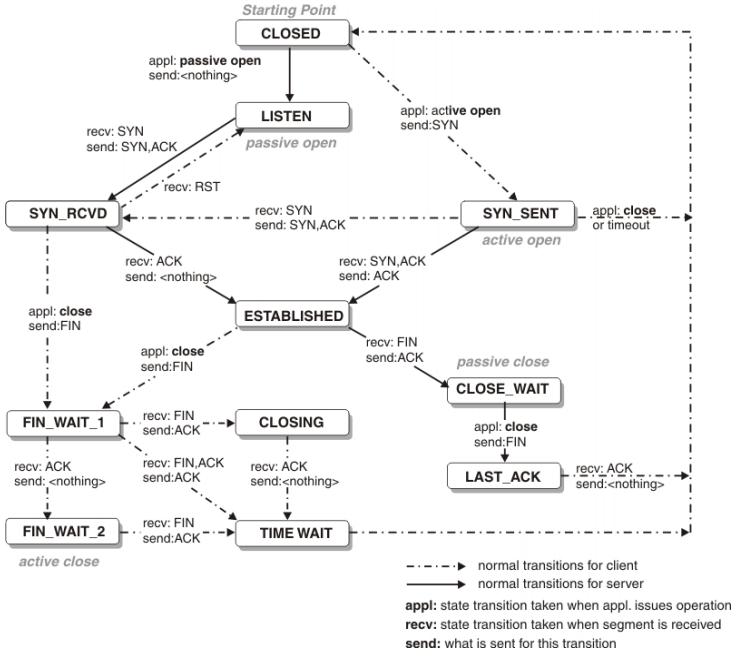
Ο σκοπός αυτής της εργαστηριακής άσκησης είναι η εξέταση των βασικών ιδιοτήτων των πρωτοκόλλων μεταφοράς TCP και UDP του Internet. Το TCP είναι κατάλληλο για μεταφορά μεγάλης ποσότητας δεδομένων, όπως το κατέβασμα με ftp ενός μεγάλου αρχείου, όπου πρέπει να εξασφαλιστεί ότι το αρχείο θα ληφθεί σωστά χωρίς λάθη. Επίσης δουλεύει πολύ καλά σε διαδραστικές εφαρμογές, όπου κάθε πλευρά στέλνει μικρά πακέτα, όπως η απομακρυσμένη πρόσβαση σε παράθυρο εντολών με εφαρμογές ftp, telnet, ssh, κα. Το βασικό μειονέκτημα του TCP είναι ότι πρέπει να προηγηθεί εγκατάσταση σύνδεσης μεταξύ των δύο άκρων. Σε αντίθεση, το UDP επιτρέπει την άμεση επικοινωνία δύο κόμβων μέσω της ανταλλαγής δεδομενογραμμάτων, χωρίς όμως να εγγυάται αξιόπιστη παράδοση. Θέματα όπως παράδοση εκτός σειράς και απώλειες θα πρέπει να αντιμετωπισθούν από τις εφαρμογές.

Για τις παρακάτω ασκήσεις απαντήστε στο συνοδευτικό φυλλάδιο, το οποίο θα υποβάλλετε ως αρχείο pdf.

1 Μετάδοση δεδομένων με TCP

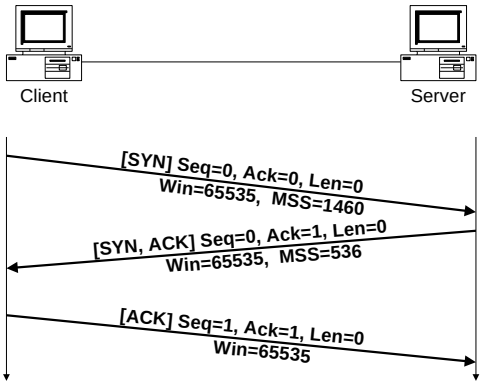
Το TCP είναι πρωτόκολλο με συνδέσεις (connection-oriented). Παρέχει αξιόπιστη (reliable) μετάδοση συρμού byte απ' άκρη σ' άκρη πάνω από μη αξιόπιστο δίκτυο. Είναι ένα πρωτόκολλο ολισθαίνοντος παραθύρου (sliding window) που χρησιμοποιεί αύξοντες αριθμούς, ώστε να εξασφαλίζει τη σωστή σειρά παράδοσης, και διαθέτει μηχανισμό τόσο για εκπνοές χρόνου (timeouts) όσο και αναμεταδόσεις (retransmissions), ώστε να μη χάνονται δεδομένα. Τέλος, χρησιμοποιεί τον μηχανισμό ολισθαίνοντος παραθύρου, ώστε να επιτυγχάνει ρυθμό μετάδοσης πλησίον του μέγιστου διαθέσιμου. Το TCP παραδίδει τα δεδομένα προς το IP σε τεμάχια[1]. Όμως, προς τα ανώτερα στρώματα, το TCP παραδίδει τα δεδομένα ως συρμό byte χωρίς να καθορίζει όρια μεταξύ των byte. Έτσι τα ανώτερα στρώματα δεν γνωρίζουν την αρχή και το τέλος των τεμαχίων.

Η λειτουργία του TCP υλοποιείται ως μηχανή πεπερασμένων καταστάσεων. Χρησιμοποιεί σημαίες μήκους 1 bit (TCP flags) στην επικεφαλίδα TCP για να μεταφέρει την πληροφορία ελέγχου σχετικά με την εγκατάσταση και απόλυση των συνδέσεων ή την επαλήθευση δεδομένων.



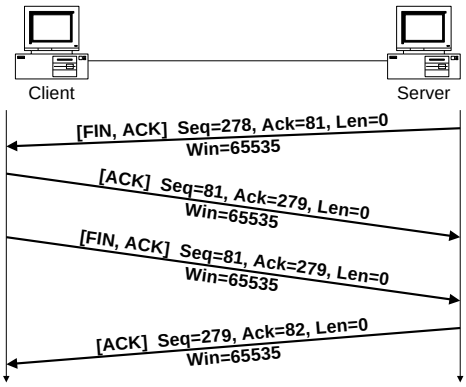
[1] Στο πρωτόκολλο TCP η μονάδα ανταλλασσόμενης πληροφορίας αποκαλείται *τεμάχιο (segment)*. Αντιπαραβάλετε, *πακέτο* για το πρωτόκολλο IP και *πλαίσιο* για το Ethernet.

Πριν από οποιανδήποτε μεταφορά δεδομένων, το TCP εγκαθιστά μια σύνδεση μεταξύ δύο ακραίων σημείων. Κάθε ακραίο σημείο προσδιορίζεται από την IP διεύθυνσή του και τον αριθμό μιας θύρας TCP. Η εγκατάσταση της σύνδεσης αρχίζει όταν ο πελάτης TCP στέλνει μια αίτηση σύνδεσης στον εξυπηρετητή TCP. Για την εγκατάσταση μιας σύνδεσης TCP ανταλλάσσονται τρία τεμάχια, σύμφωνα με μια διαδικασία που είναι γνωστή ως *τριπλή χειραψία* (*3-way handshake*). Για την εγκατάσταση σύνδεσης χρησιμοποιούνται οι σημαίες SYN και ACK όπως στο σχήμα. Κατά τη διάρκεια της τριπλής χειραψίας δεν μεταφέρονται δεδομένα (τα τεμάχια έχουν μηδενικό μήκος δεδομένων), αλλά γίνεται διαπραγμάτευση για βασικές παραμέτρους της σύνδεσης TCP, όπως οι αρχικοί αύξοντες αριθμοί, το μέγιστο μέγεθος τεμαχίου και το μέγεθος του παραθύρου για τον έλεγχο ροής.



Μετά την τριπλή χειραψία ακολουθεί αμφίδρομη ροή δεδομένων. 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 Seq (sequence number) στην επικεφαλίδα TCP δηλώνει τον αριθμό του πρώτου byte στα δεδομένα του τεμαχίου. Ο αριθμός επαλήθευσης Ack (acknowledgement number) είναι ο αύξων αριθμός του επόμενου byte που αναμένεται από την άλλη πλευρά. Το μέγεθος παραθύρου Win (window size) καθορίζει τον αριθμό των byte δεδομένων που μπορούν να σταλούν πριν απαιτηθεί επαλήθευση από τον παραλήπτη. Οι επαληθεύσεις δηλώνονται με τη σημαία ACK και είναι συσσωρευτικές, 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) χρησιμοποιώντας τη σημαία FIN.



Άλλες σημαίες που χρησιμοποιεί το TCP είναι: η RST, για την απόρριψη μιας σύνδεσης, η PSH, για να εξωθήσει τον παραλήπτη να αδειάσει τον χώρο αποθήκευσης διαβάζοντας τα δεδομένα και η URG, που δηλώνει ότι ο δείκτης Urgent της επικεφαλίδας TCP είναι σημαντικός (περιέχει πληροφορία). Για περισσότερες λεπτομέρειες σχετικά με τα πεδία της επικεφαλίδας του TCP ανατρέξτε στην ιστοσελίδα http://www.networksorcery.com/enp/protocol/tcp.htm.

Στην ιστοσελίδα https://www.eventhelix.com/networking/tcp/Tcp.pdf θα βρείτε ένα πλήρες παράδειγμα ανταλλαγής τεμαχίων για την εγκατάσταση σύνδεσης TCP, μεταφορά δεδομένων και την απόλυση σύνδεσης μεταξύ ενός πελάτη και ενός εξυπηρετητή.

Δημιουργήστε ένα φίλτρο σύλληψης στο Wireshark ώστε να καταγράφονται μόνο πακέτα IPv4 που περιλαμβάνουν τη διεύθυνση IPv4 του υπολογιστή σας, ανοίξτε ένα παράθυρο εντολών και καταγράψτε την κίνηση που παράγεται όταν κάνετε telnet στον υπολογιστή 1.1.1.1, που υπάρχει αλλά δεν απαντά, και περιμένετε μέχρι να τερματίσει η εντολή *[Περίπτωση Α]*. Μετά επιχειρήστε telnet στον υπολογιστή 2.2.2.2, που εάν υπάρχει δεν απαντά, και περιμένετε μέχρι να τερματίσει η εντολή *[Περίπτωση Β]*. Τέλος, επιχειρήστε telnet στον υπολογιστή 147.102.40.1, όπου όμως δεν γίνονται δεκτές τέτοιες συνδέσεις *[Περίπτωση Γ]*. 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 IPv4 του υπολογιστή σας.
1.2 Εφαρμόστε φίλτρο απεικόνισης ώστε να παραμείνουν μόνο πακέτα προς κάποιον από τους παραπάνω προορισμούς. Ποια είναι η σύνταξή του;
1.3 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* https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers*]*.
1.4 Εφαρμόστε ένα φίλτρο απεικόνισης ώστε να παραμείνουν μόνο τα τεμάχια TCP 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 γράφοντας tcp στο πεδίο για την εισαγωγή φίλτρου απεικόνισης]*.
1.5 Ποια σημαία μήκους 1 bit ενεργοποιείται για την εκκίνηση της εγκατάστασης της σύνδεσης TCP;
1.6 Πόσες προσπάθειες κάνει ο υπολογιστής σας προκείμενου να εγκαταστήσει σύνδεση TCP στις Περιπτώσεις Α και Β;
1.7 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]*.
1.8 Τι παρατηρείτε συγκρίνοντας τα αποτελέσματα των περιπτώσεων Α και Β;
1.9 Ποια βήματα της τριπλής χειραψίας παρατηρήσατε;
1.10 Ο υπολογιστής σας απολύει τη σύνδεση ή απλώς εγκαταλείπει την προσπάθεια;

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

1.11 Ποια είναι η σύνταξή του;
1.12 Πόσες προσπάθειες κάνει ο υπολογιστής σας προκείμενου να εγκαταστήσει σύνδεση TCP;
1.13 Συγκρίνοντας με την απάντηση σας στο ερώτημα 1.8, ποιες διαφορές παρατηρείτε;

Επιλέξτε ένα (ή το μοναδικό) από τα τεμάχια TCP που στέλνει ο 147.102.40.1 στον υπολογιστή σας προκειμένου να απορρίψει τη σύνδεση TCP.

1.14 Ποιες σημαίες μήκους 1 bit περιλαμβάνει;
1.15 Ποια εξ αυτών δηλώνει άρνηση της εγκατάστασης σύνδεσης TCP;
1.16 Ποιο είναι το μέγεθος της επικεφαλίδας και ποιο το μέγεθος του πεδίου δεδομένων αυτού του τεμαχίου TCP;
1.17 Καταγράψτε τα ονόματα και το μήκος σε bit των πεδίων της επικεφαλίδας του τεμαχίου TCP και σημειώστε στο σχήμα τις θέσεις τους.
1.18 Ποιο είναι το όνομα του πεδίου 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;

1.19 Πώς προκύπτει το μήκος της επικεφαλίδας TCP από την τιμή που παρατηρείτε στα περιεχόμενα πακέτου σε δεκαεξαδική τιμή;
1.20 Υπάρχει πεδίο της επικεφαλίδας TCP που να δηλώνει το μήκος του τεμαχίου;
1.21 Πώς προκύπτει το μήκος αυτό με βάση τα στοιχεία των επικεφαλίδων IPv4 και TCP;
1.22 Ποιο είναι το μέγεθος της επικεφαλίδας του πρώτου ή μοναδικού τεμαχίου TCP που στέλνει ο υπολογιστής σας στον 147.102.40.1 για την εγκατάσταση σύνδεσης TCP;
1.23 Υπάρχει διαφορά στο μέγεθος της επικεφαλίδας TCP των δύο παραπάνω τεμαχίων; Εάν ναι, που οφείλεται;

2 Εγκατάσταση σύνδεσης, μεταφορά δεδομένων και απόλυση σύνδεσης TCP

Χρησιμοποιώντας το κατάλληλο φίλτρο σύλληψης στο Wireshark, αφού ανοίξετε ένα παράθυρο εντολών, θα καταγράψετε τα διερχόμενα τεμάχια TCP όταν χρησιμοποιώντας την εφαρμογή ftp συνδέστε στον υπολογιστή edu-dy.cn.ntua.gr. Στην προτροπή User: πληκτρολογήστε anonymous ακολουθούμενο από <Enter>, ενώ στην προτροπή Password: πληκτρολογήστε τη διεύθυνση e-mail σας ακολουθούμενη από <Enter>. Στη συνέχεια, πληκτρολογήστε την εντολή bin, ώστε η μεταφορά αρχείων να γίνει σε δυαδική μορφή. Επιλέξτε με την εντολή lcd desktop την επιφάνεια εργασίας ως τον προορισμό όπου επιθυμείτε να αποθηκεύσετε το αρχείο που θα κατεβάσετε στη συνέχεια. Κατεβάστε το αρχείο PCATTCP.exe με την εντολή get PCATTCP.exe *[Προσοχή στα μικρά και κεφαλαία γράμματα]*. Τέλος, πληκτρολογήστε bye για να τερματίσετε την εφαρμογή ftp και σταματήστε την καταγραφή των πακέτων.

2.1 Ποιο φίλτρο σύλληψης χρησιμοποιήσατε για την καταγραφή της κίνησης;

Εγκατάσταση σύνδεσης

Παρατηρήστε τα τεμάχια TCP που ανταλλάχθηκαν και εντοπίστε τα σχετικά με την τριπλή χειραψία. 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 ή απόλυσης σύνδεσης έχουν διαφορετικό χρώμα]*.

2.2 Σε ποια θύρα (ελέγχου FTP) 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* https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers *για τη θύρα ελέγχου FTP]*.
2.3 Με ποια θύρα (δεδομένων FTP) του υπολογιστή edu-dy.cn.ntua.gr γίνεται η σύνδεση για τη μεταφορά 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*.

2.4 Ποια είναι η σύνταξη του φίλτρου;
2.5 Πόσα τεμάχια TCP ανταλλάσσονται για την εγκατάσταση της σύνδεσης ελέγχου FTP;
2.6 Ποιες σημαίες χρησιμοποιούνται για την εγκατάσταση της σύνδεσης TCP;
2.7 Ποιο είναι το μέγεθος των επικεφαλίδων TCP των τεμαχίων αυτών;
2.8 Ποιο είναι το μέγεθος δεδομένων των τεμαχίων αυτών;
2.9 Πόσο διαρκεί η διαδικασία της τριπλής χειραψίας; *[Υπόδειξη: Από το μενού View μπορείτε να επιλέξετε Time Display Format → Seconds Since Beginning of Capture]*.
2.10 Συμφωνεί η τιμή που βρήκατε προηγουμένως με το iRTT που εμφανίζει το Wireshark κάτω από το [SEQ/ACK analysis] στο παράθυρο με τις λεπτομέρειες επικεφαλίδας;

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 (αριθμός σειράς) στην επικεφαλίδα TCP δείχνει τον αύξοντα αριθμό του πρώτου byte στο πεδίο δεδομένων που αποστέλλονται και το πεδίο Acknowledgement Number (αριθμός επιβεβαίωσης) δείχνει τον αριθμό σειράς του επόμενου byte δεδομένων που αναμένεται.

2.11 Ποιοι είναι οι αρχικοί αριθμοί σειράς (Sequence Number) που ανακοινώνει η κάθε πλευρά; *[Υπόδειξη: Το Wireshark για ευκολία εμφανίζει τους απόλυτους και τους σχετικούς αύξοντες αριθμούς.]*
2.12 Πώς προκύπτει ο αριθμός επιβεβαίωσης (Acknowledgement Number) του τεμαχίου TCP με το οποίο ο εξυπηρετητής FTP δηλώνει ότι αποδέχεται τη σύνδεση;
2.13 Πώς προκύπτουν ο αριθμός σειράς και ο αριθμός επιβεβαίωσης (Sequence Number και Acknowledgement Number) του τελευταίου τεμαχίου TCP της τριπλής χειραψίας με το οποίο ολοκληρώνεται η εγκατάσταση της σύνδεσης;
2.14 Ποιο είναι το μήκος δεδομένων των τριών τεμαχίων της τριπλής χειραψίας;
2.15 Ποια είναι η μέγιστη τιμή που μπορεί να λάβουν οι αριθμοί σειράς και επιβεβαίωσης;
2.16 Ποιο φίλτρο απεικόνισης θα εφαρμόσετε ώστε να παραμείνουν μόνο τα τεμάχια TCP για την τριπλή χειραψία. *[Υποδ. Εκτός από τη σημαία SYN θα χρειαστεί να φιλτράρετε για τεμάχια ACK με τους σωστούς σχετικούς αύξοντες αριθμούς σειράς, επιβεβαίωσης και μήκος τεμαχίου.]*

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 λήψης ίσο με τον ελεύθερο χώρο προσωρινής μνήμης που διαθέτει και ο αποστολέας δεν στέλνει περισσότερα ανεπιβεβαίωτα byte από όσο ορίζει το παράθυρο αυτό.

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

Το TCP προσπαθεί να αποφύγει τον θρυμματισμό (fragmentation) των πακέτων IPv4. Όταν εγκαθίσταται η σύνδεση TCP, γίνεται ανακοίνωση του μέγιστου μεγέθους τεμαχίου (MSS – Maximum Segment Size). Το MSS είναι το μέγιστο μέγεθος δεδομένων (σε byte) του στρώματος εφαρμογής που μπορεί να δεχθεί ο προορισμός από την πηγή σε ένα πακέτο IP, δηλαδή, η τιμή της MTU μείον το ελάχιστο μήκος επικεφαλίδας των πρωτοκόλλων IP και TCP. Επομένως, MSS = MTU – 40 στην περίπτωση IPv4 και MSS = MTU – 60 στην περίπτωση IPv6. Τόσο ο πελάτης όσο και ο εξυπηρετητής TCP μπορούν να ανακοινώσουν το MSS σε μία επιλογή (option) της επικεφαλίδας TCP του πρώτου τεμαχίου TCP που μεταδίδεται. Έτσι, ο αποστολέας της πληροφορίας στέλνει τεμάχια μεγέθους τέτοιου ώστε να γίνονται αποδεκτά από τον παραλήπτη χωρίς να απαιτηθεί θρυμματισμός στη διεπαφή αυτού. Η ανταλλαγή των MSS αφορά μόνο στα δύο άκρα, και όχι στους ενδιάμεσους δρομολογητές από όπου θα διέλθει το πακέτο IPv4. Για να διαπιστωθεί η μικρότερη MTU (Maximum Transmission Unit) της διαδρομής από τον αποστολέα ως τον παραλήπτη, το TCP χρησιμοποιεί τη διαδικασία **Path MTU Discovery** που είδατε στην Εργαστηριακή Άσκηση 6.

Με βάση την προηγούμενη καταγραφή της κίνησης FTP, απαντήστε στα παρακάτω ερωτήματα.

2.20 Ποια τιμή του MSS ανακοινώνει ο υπολογιστής σας κατά την εγκατάσταση της σύνδεσης ελέγχου. *[Υπόδειξη: Αναζητήστε μεταξύ των παραμέτρων που εμφανίζονται στο παράθυρο με τη λίστα καταγεγραμμένων πακέτων]*.
2.21 Πώς προκύπτει η παραπάνω τιμή από την MTU της διεπαφής του υπολογιστή σας;
2.22 Σε ποιο πεδίο της επικεφαλίδας TCP μεταφέρεται η τιμή του MSS;
2.23 Ποια τιμή του MSS ανακοινώνει ο edu-dy.cn.ntua.gr.
2.24 Πώς προκύπτει αυτή από την MTU (576 byte) της διεπαφής του edu-dy.cn.ntua.gr;

2.25 Ποιο είναι το μέγεθος του μεγαλύτερου τεμαχίου TCP που μπορεί να στείλει ο υπολογιστής σας προς τον εξυπηρετητή στη σύνδεση που εγκαταστάθηκε κατά την τριπλή χειραψία TCP στη θύρα ελέγχου του FTP;

Απόλυση σύνδεσης

Στη συνέχεια, αφού ακυρώσετε το τρέχον *φίλτρο απεικόνισης*, εντοπίστε τα τεμάχια TCP που σχετίζονται με την απόλυση της σύνδεσης ελέγχου FTP.

2.26 Ποια σημαία μήκους 1 bit ενεργοποιείται για την εκκίνηση της απόλυσης της σύνδεσης TCP;
2.27 Εφαρμόστε φίλτρο απεικόνισης ώστε να παραμείνουν μόνο τεμάχια TCP που φέρουν τη σημαία αυτή. Ποια η σύνταξή του;
2.28 Ποια πλευρά εκκινεί τη διαδικασία απόλυσης;
2.29 Πόσα τεμάχια TCP ανταλλάσσονται συνολικά;
2.30 Ποιο είναι το μέγεθος των επικεφαλίδων TCP των τεμαχίων αυτών;
2.31 Ποιο είναι το μέγεθος δεδομένων των τεμαχίων αυτών;
2.32 Δικαιολογήστε το μήκος του πακέτου IPv4 που μεταφέρει το τεμάχιο TCP με το οποίο απολύει τη σύνδεση ο υπολογιστής σας.
2.33 Δικαιολογήστε το μήκος του πακέτου IPv4 που μεταφέρει το αντίστοιχο τεμάχιο TCP από τον edu-dy.cn.ntua.gr.
2.34 Πόσα byte μεταδόθηκαν συνολικά στη σύνδεση ελέγχου FTP από κάθε πλευρά;
2.35 Με ποιο τρόπο προσδιορίσατε το πλήθος τους;

Μεταφορά δεδομένων

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

2.36 Ποια είναι η σύνταξή του φίλτρου αυτού;
2.37 Ποια τιμή του MSS ανακοινώνει η κάθε πλευρά κατά την τριπλή χειραψία TCP στη θύρα δεδομένων FTP;
2.38 Ποιο είναι το μέγεθος του μεγαλύτερου τεμαχίου TCP που μπορεί να στείλει ο εξυπηρετητής προς τον υπολογιστή σας στη σύνδεση που εγκαταστάθηκε κατά την τριπλή χειραψία TCP στη θύρα δεδομένων του FTP;
2.39 Ποια είναι η τιμή του RTT όπως αυτή προκύπτει από την ανταλλαγή των δύο πρώτων τεμαχίων της τριπλής χειραψίας;
2.40 Ο υπολογιστής σας στέλνει επιβεβαιώσεις για κάθε τεμάχιο TCP που λαμβάνει; Εάν όχι, περίπου κάθε πόσα τεμάχια στέλνει;
2.41 Αλλάζουν οι τιμές του παραθύρου (window), που ανακοινώνει ο υπολογιστής σας καθώς προχωρά η μεταφορά του αρχείου; Ποια είναι η μικρότερη τιμή που παρατηρήσατε;

Εφαρμόστε φίλτρο απεικόνισης ftp-data ώστε να εμφανίζονται μόνο τα τεμάχια TCP που αφορούν μεταφορά δεδομένων FTP και επιλέξτε το πρώτο που στέλνει ο edu-dy.cn.ntua.gr.

2.42 Να καταγραφεί το μέγεθος πλαισίου (frame) σε byte και το μήκος των επικεφαλίδων Ethernet, IP και TCP.
2.43 Είναι το μέγεθος των δεδομένων του τεμαχίου TCP το αναμενόμενο βάσει της τιμής του ερωτήματος 2.38;
2.44 Εάν για κάποιο λόγο έπρεπε ο εξυπηρετητής να αποστείλει δεδομένα μεγαλύτερα από την τιμή που βρήκατε πριν, τι θα συνέβαινε; *[Υπόδειξη: Αναζητήστε Source Fragmentation στο RFC 879.]*
2.45 Πόσα byte δεδομένων μεταδόθηκαν συνολικά στη σύνδεση δεδομένων από κάθε πλευρά; *[Υπόδειξη: Χρησιμοποιήστε τους αριθμούς επιβεβαίωσης των τεμαχίων για τον υπολογισμό.]*
2.46 Ποιος ήταν ο ρυθμός μεταφοράς δεδομένων σε kbyte/sec από τον εξυπηρετητή στο PC σας;

2.47 Υπήρξαν αναμεταδόσεις τεμαχίων κατά τη μεταφορά δεδομένων; Εάν ναι, πώς το αντιληφτήκατε;

Προτού προχωρήσετε στο επόμενο μέρος ***αποθηκεύεστε*** την καταγραφή που κάνατε σε κάποιο αρχείο.

3 Αποφυγή συμφόρησης στο TCP

Καθώς το διαδίκτυο άρχισε να διαδίδεται παρατηρήθηκαν φαινόμενα συμφόρησης που οφείλονταν στην απώλεια πακέτων λόγω υπερχείλισης των χώρων αποθήκευσης στους δρομολογητές. Για προληφθούν τέτοιες καταστάσεις τροποποιήθηκε εκ των υστέρων η λειτουργία του TCP με την εισαγωγή ενός αλγόριθμου ελέγχου και αποφυγής συμφόρησης. Προς τούτο χρησιμοποιήθηκε ο μηχανισμός ολισθαίνοντος παραθύρου του TCP που αρχικά είχε σκοπό τον έλεγχο ροής, δηλαδή, να μην στέλνει η πηγή πιο γρήγορα από ότι μπορεί να δεχθεί ο προορισμός. Η κεντρική ιδέα είναι να εκτιμά η πηγή τη φόρτιση του δικτύου μέσω ενός παραθύρου συμφόρησης και να μην στέλνει περισσότερα byte από όσα μπορεί να προωθήσει το δίκτυο και δεχθεί ο προορισμός. Η εκτίμηση του παραθύρου συμφόρησης βασίζεται στην ανάδραση που λαμβάνει η πηγή από το δίκτυο. Μια μέθοδος είναι ο μηχανισμός εκκίνησης που αποκαλείται αργή αρχή (slow start) και περιγράφεται στο RFC 5681. Συγκεκριμένα, η πηγή ξεκινά με αρχικό παράθυρο μερικών MSS, δύο έως τέσσαρα ανάλογα με το μέγεθος του MSS, και στη συνέχεια για κάθε ACK που λαμβάνει, αυξάνει το παράθυρο συμφόρησης κατά ένα MSS.

Για το μέρος αυτό της άσκησης θα χρησιμοποιήσετε μια έτοιμη καταγραφή και αυτήν που αποθηκεύσατε προηγουμένως. Συνδεθείτε όπως πριν με ftp στον edu-dy.cn.ntua.gr και, αφού αλλάξετε σε δυαδικό τρόπο μεταφοράς, κατεβάστε το αρχείο pcattcp.pcap. Το αρχείο περιέχει μια καταγραφή, από την πλευρά του edu-dy.cn.ntua.gr, του κατεβάσματος με ftp του αρχείου PCATTCP.exe.

3.1 Ανοίξτε το αρχείο pcattcp.pcap στο Wireshark και εφαρμόστε φίλτρο απεικόνισης ώστε να παραμείνουν μόνο τα τεμάχια TCP που σχετίζονται με τη θύρα δεδομένων FTP. Ποια η σύνταξή του;

3.2 Εντοπίστε τα τεμάχια της τριπλής χειραψίας. Ποια η διεύθυνση IPv4 του υπολογιστή που κατέβασε το αρχείο PCATTCP.exe;

3.3 Ποιο είναι το RTT της σύνδεσης όπως προκύπτει από την ανταλλαγή των δύο πρώτων τεμαχίων της τριπλής χειραψίας; Συγκρίνετε με αυτήν που βρήκατε προηγουμένως στο ερώτημα 2.39.

Εμφανίστε το διάγραμμα αριθμών σειράς συναρτήσει του χρόνου από το μενού *Statistics → TCP Stream Graphs → Time Sequence (Stevens)*. Κάθε τελεία στο διάγραμμα αντιστοιχεί ένα τεμάχιο TCP. Όπου οι τελείες εμφανίζονται η μία πάνω από την άλλη, τα αντίστοιχα τεμάχια στάλθηκαν τα ένα πίσω από το άλλο.

3.4 Από το κουμπί *Switch Direction* επιλέξτε ως πηγή των τεμαχίων τον edu-dy.cn.ntua.gr. Παρατηρώντας προσεκτικά το διάγραμμα, τι συμπεραίνετε σχετικά με τον τρόπο που στέλνονται τα τεμάχια TCP από τον edu-dy.cn.ntua.gr;

3.5 Πόσα τεμάχια έστειλε ο edu-dy.cn.ntua.gr στο πρώτο RTT; Είναι το πλήθος τους σύμφωνο με ότι προβλέπει το RFC 5681 στην παρ. 3.1;

3.6 Πόσα έστειλε κατά το δεύτερο και το τρίτο RTT; Γιατί; *[Υπόδειξη: Δείτε το αντίστοιχο διάγραμμα για την κίνηση από την άλλη πλευρά κάνοντας κλικ στο Switch Direction.]*

3.7 Επιλέξτε το πρώτο τεμάχιο δεδομένων FTP από τον edu-dy.cn.ntua.gr στη δική σας καταγραφή και εμφανίστε το αντίστοιχο διάγραμμα αριθμών σειράς συναρτήσει του χρόνου από το edu-dy.cn.ntua.gr προς τον υπολογιστή σας. Είναι παρόμοιο με αυτό του αρχείου που κατεβάσατε; Συγκρίνετε με τις απαντήσεις στα δύο προηγούμενα ερωτήματα;

4 Μετάδοση δεδομένων με UDP

Το πρωτόκολλο μεταφοράς UDP παρέχει μια υπηρεσία "καλύτερης προσπάθειας" χωρίς σύνδεση (connectionless) που δεν εγγυάται την παράδοση των δεδομένων. Είναι μια μινιμαλιστική επέκταση της υπηρεσίας "best-effort" του IP που δίνει στις εφαρμογές άμεση πρόσβαση σε μια υπηρεσία δεδομενογραμμάτων. 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. Χρησιμοποιείται από εφαρμογές που δεν απαιτούν το επίπεδο υπηρεσίας που προσφέρει το TCP ή θέλουν να χρησιμοποιήσουν υπηρεσίες χωρίς σύνδεση (π.χ. εκπομπή ή πολλαπλή διανομή). Το UDP είναι ένα λιτό πρωτόκολλο μεταφοράς για να στέλνει κανείς όσο γρήγορα μπορεί. Οι μόνες επιπλέον υπηρεσίες που παρέχει σε σχέση με το IP είναι το πεδίο ελέγχου για τα δεδομένα και η πολυπλεξία μέσω της θύρας UDP. Έτσι οποιαδήποτε εφαρμογή το χρησιμοποιεί πρέπει να χειρισθεί απευθείας τα από άκρο σε άκρο προβλήματα της επικοινωνίας εάν αυτό είναι απαραίτητο. Για περισσότερες λεπτομέρειες σχετικά με τα πεδία της επικεφαλίδας του UDP ανατρέξτε στην ιστοσελίδα http://www.networksorcery.com/enp/protocol/udp.htm.

Με τη βοήθεια του Wireshark να καταγράψετε την κίνηση ενώ κάνετε χρήση της υπηρεσίας DNS. Εφαρμόστε φίλτρο σύλληψης για να παρατηρείτε μόνο κίνηση του πρωτοκόλλου UDP και ξεκινήστε την καταγραφή. Ανοίξτε ένα παράθυρο εντολών και καθαρίστε την προσωρινή μνήμη DNS (DNS cache) που διατηρεί ο υπολογιστής. Εάν χρησιμοποιείτε Windows, σε ένα παράθυρο εντολών εκτελέστε την εντολή ipconfig /flushdns. Σε Ubuntu εκτελέστε την εντολή sudo systemd-resolve --flush-caches. Σε συστήματα Unix/Linux, εν γένει δεν χρησιμοποιείται προσωρινή αποθήκευση για την επίλυση ονομάτων. Εάν όμως την έχετε ενεργοποιήσει, διαγράψτε τα περιεχόμενά της επανεκκινώντας την αντίστοιχη υπηρεσία, π.χ. nscd, unbound, κλπ.

Στη συνέχεια τρέξτε το πρόγραμμα nslookup σε περιβάλλον Windows, dig σε περιβάλλον Linux ή host σε περιβάλλον Unix, για να ζητήσετε τη διεύθυνση IP του edu-dy.cn.ntua.gr.

4.1 Ποια είναι η σύνταξη του φίλτρου σύλληψης που χρησιμοποιήσατε;

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

4.2 Καταγράψτε τα ονόματα και το μήκος των πεδίων της επικεφαλίδας δεδομενογράμματος UDP.
4.3 Ποιο είναι το συνολικό μέγεθος της επικεφαλίδας UDP;
4.4 Ποιο είναι το μήκος του συγκεκριμένου δεδομενογράμματος βάσει του μεγέθους του πακέτου IPv4 ή IPv6 εντός του οποίου ενθυλακώνεται;
4.5 Τι εκφράζει το πεδίο *μήκος (Length)* της επικεφαλίδας UDP;
4.6 Ποιο είναι το ελάχιστο και ποιο το μέγιστο μέγεθος δεδομενογράμματος UDP που μπορεί να μεταφερθεί από ένα πακέτο IPv4; Αιτιολογήστε την απάντησή σας.
4.7 Δοθέντος ότι όλοι οι κόμβοι στο διαδίκτυο οφείλουν να δέχονται πακέτα IPv4 μεγέθους μέχρι 576 byte (θρυμματισμένα ή μη), ποιο είναι το μέγιστο μήκος πακέτου UDP που μπορεί να σταλεί και παραληφθεί με βεβαιότητα.
4.8 Παρατηρήσατε στην καταγραφή σας να μεταφέρονται με δεδομενογράμματα UDP μηνύματα άλλων πλην του DNS πρωτοκόλλων; Εάν ναι, για ποια πρωτόκολλα πρόκειται;

Εφαρμόστε φίλτρο απεικόνισης ώστε να παραμείνουν μόνο μηνύματα DNS.

4.9 Ποια είναι η σύνταξη του φίλτρου απεικόνισης που χρησιμοποιήσατε;
4.10 Ποια είναι η διεύθυνση IPv4 ή IPv6 του εξυπηρετητή DNS που απάντησε στην ερώτηση για τη διεύθυνση του edu-dy.cn.ntua.gr;
4.11 Καταγράψτε τις θύρες (προέλευσης και προορισμού) του πρωτοκόλλου μεταφοράς που χρησιμοποιήθηκαν για ερώτηση (query) στον εξυπηρετητή DNS.
4.12 Καταγράψτε τις θύρες (προέλευσης και προορισμού) του πρωτοκόλλου μεταφοράς που χρησιμοποιήθηκαν στην απόκριση (response) του εξυπηρετητή DNS.
4.13 Ποια από τις παραπάνω θύρες αντιστοιχεί στο πρωτόκολλο εφαρμογής DNS;

Ονοματεπώνυμο:		**Ομάδα:**
Όνομα PC/ΛΣ:	**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 .....

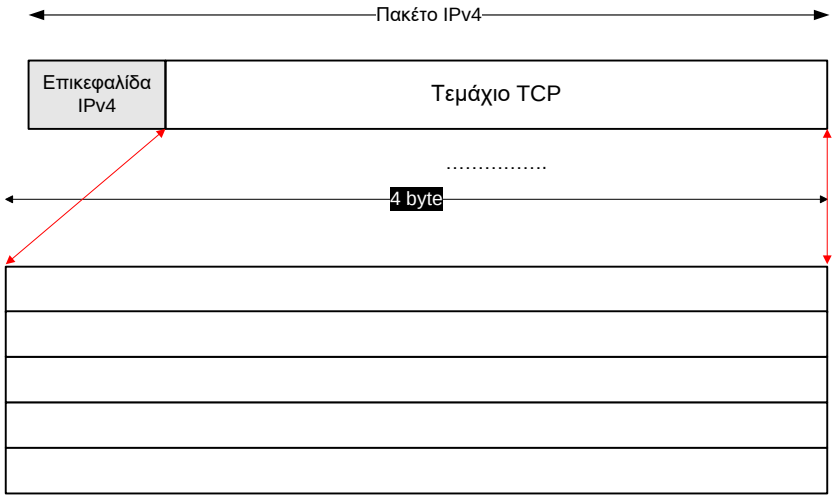
.....

.....

.....

.....

.....



2