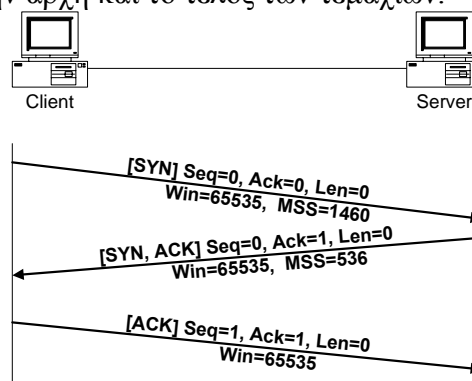


Εργαστηριακή Άσκηση 7 Πρωτόκολλα TCP και UDP

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 συλληθθέντα 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 πιάστε *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 τεμάχια¹. 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 οποιαδήποτε μεταφορά δεδομένων, το TCP εγκαθιστά μια σύνδεση. Η εγκατάσταση της σύνδεσης αρχίζει όταν ο πελάτης TCP στέλνει μια αίτηση σύνδεσης στον εξυπηρετητή TCP². 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

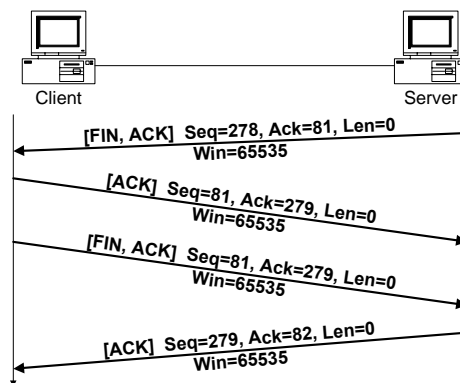
¹ Στο πρωτόκολλο TCP η μονάδα ανταλλασσόμενης πληροφορίας αποκαλείται *τεμάχιο* (segment). Αντιπαραβάλετε, *πακέτο* για το πρωτόκολλο IP και *πλαίσιο* για το Ethernet.

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 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).



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, επιχειρήστε 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 προκειμένου 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 προκειμένου να εγκαταστήσει σύνδεση TCP;
- 1.12 Ποια σημαία μήκους 1 bit ενεργοποιείται για την άρνηση της εγκατάστασης σύνδεσης TCP;
- 1.13 Συγκρίνοντας με την απάντησή σας στο ερώτημα 1.7, τι συμπεραίνετε για το πότε επαναλαμβάνονται οι προσπάθειες εγκατάστασης της σύνδεσης;

2 Εγκατάσταση σύνδεσης, μεταφορά δεδομένων και απόλυση σύνδεσης TCP

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 τον φάκελο του υπολογιστή σας όπου επιθυμείτε να αποθηκεύσετε το πρόγραμμα με την εντολή `lcd` (π.χ. `lcd desktop`) και κατεβάστε το `PCATTCP.exe` με την εντολή `get PCATTCP.exe` [Προσοχή στα μικρά και κεφαλαία γράμματα]. Τέλος, προτού πληκτρολογήσετε `bye` για να τερματίσετε την εφαρμογή `ftp` και σταματήσετε την καταγραφή των πακέτων, σημειώστε το όνομα του φακέλου όπου αποθηκεύθηκε το `PCATTCP.exe`.

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

- 2.1 Σε ποια θύρα (ελέγχου FTP) προσπαθεί να συνδεθεί ο υπολογιστής σας για να αρχίσει η επικοινωνία με τον εξυπηρετητή; [Υπόδειξη: Συμβουλευθείτε την ιστοσελίδα http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers].
- 2.2 Σε ποια θύρα (δεδομένων FTP) γίνεται η σύνδεση για τη μεταφορά των δεδομένων FTP;

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 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 το πρώτου byte στο πεδίο δεδομένων που αποστέλλονται και το πεδίο Acknowledgement number δείχνει τον αύξοντα αριθμό του επόμενου byte δεδομένων που αναμένονται.

- 2.8 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.*]
- 2.9 Πώς προκύπτει ο αριθμός της επιβεβαίωσης (Acknowledgement Number) του τεμαχίου με το οποίο ο εξυπηρετητής FTP δηλώνει ότι αποδέχεται τη σύνδεση;
- 2.10 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;
- 2.11 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 $SeqNo=AckNo, AckNo+1, \dots, AckNo + win - 1$.

- 2.12 Προσδιορίστε το μέγεθος των παραθύρων που ανακοινώνει ο υπολογιστής σας και ο εξυπηρετητής κατά τη διάρκεια της τριπλής χειραψίας.
- 2.13 Σε ποιο πεδίο της επικεφαλίδας μεταφέρεται η σχετική πληροφορία;
- 2.14 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 διαπραγματεύση 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 στη διαδρομή από τον αποστολέα ως τον παραλήπτη, το TCP

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

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.

- 2.15 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].
- 2.16 Πώς προκύπτει η παραπάνω τιμή από την ισχύουσα MTU (1500 byte) για τον υπολογιστή σας;
- 2.17 Σε ποιο πεδίο της επικεφαλίδας TCP μεταφέρεται η τιμή του MSS;
- 2.18 Να καταγραφεί η τιμή του MSS που αντιπροτείνει ο `edu-dy.cn.ntua.gr`.
- 2.19 Πώς προκύπτει η παραπάνω τιμή από την ισχύουσα MTU (576 byte) για τον `edu-dy.cn.ntua.gr`;
- 2.20 Ποια είναι η τιμή του MSS που συμφωνείται κατά την τριμερή χειραψία TCP στη θύρα ελέγχου του FTP;

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

- 2.21 Ποια σημαία μήκους 1 bit ενεργοποιείται για την εκκίνηση της απόλυσης της σύνδεσης TCP;
- 2.22 Ποια πλευρά εκκινεί τη διαδικασία απόλυσης;
- 2.23 Πόσα τεμάχια TCP ανταλλάσσονται συνολικά;
- 2.24 Πόσα byte μεταδόθηκαν συνολικά στη σύνδεση ελέγχου FTP από κάθε πλευρά;
- 2.25 Με ποιο τρόπο προσδιορίσατε το πλήθος τους;

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.

- 2.26 Ποια είναι η σύνταξή του φίλτρου αυτού;
- 2.27 Ποια είναι η τιμή του MSS που συμφωνείται κατά την τριμερή χειραψία TCP στη θύρα δεδομένων FTP;

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

- 2.28 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 ενός από τα μηνύματα FTP.
- 2.29 Πώς προκύπτει το μήκος δεδομένων των μηνυμάτων FTP από τα μήκη των επικεφαλίδων κάθε στρώματος πρωτοκόλλων;
- 2.30 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;
- 2.31 Ποια είναι η μέγιστη τιμή που θα μπορούσε να λάβει το MSS;
- 2.32 Πόσα byte μεταδόθηκαν συνολικά στη σύνδεση δεδομένων από κάθε πλευρά;
- 2.33 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 δεδομένογράμμα UDP αντιμετωπίζεται ανεξάρτητα από τα άλλα. Το UDP είναι ένα λιτό πρωτόκολλο μεταφοράς για να στέλνει κανείς όσο γρήγορα μπορεί.

Για την πραγματοποίηση αυτού του τμήματος της άσκησης θα εγκαταστήσετε επικοινωνία UDP μεταξύ του υπολογιστή σας και του υπολογιστή του διπλανού σας. Για την πραγματοποίηση της επικοινωνίας μεταξύ των δύο υπολογιστών θα χρησιμοποιήσετε το πρόγραμμα PCATTCIP.exe που κατεβάσατε στο δεύτερο τμήμα της άσκησης. Με το πρόγραμμα pcattcp μπορείτε να στείλετε και να λάβετε κίνηση μεταξύ δύο υπολογιστών. Στον ένα θα πρέπει να ξεκινήσει η διαδικασία λήψης και στον άλλο η διαδικασία αποστολής. Για βοήθεια, σε ένα παράθυρο εντολών πληκτρολογήστε pcattcp /?. Για παράδειγμα, πληκτρολογώντας pcattcp -r -l 60 -n 10 -p 4000 και μετά <Enter> σε ένα παράθυρο εντολών, ο υπολογιστής θα “ακούει” στην πόρτα 4000. Ο υπολογιστής, που θα παράγει την κίνηση, θα πρέπει να στείλει την κίνηση στην ίδια πόρτα, οπότε πληκτρολογήστε: pcattcp -t -l 60 -n 10 -p 4000 <IP address> <Enter>, όπου <IP address> είναι η διεύθυνση του υπολογιστή που έχετε επιλέξει για λήψη. Η παραπάνω διαδικασία θα έχει σαν αποτέλεσμα την αποστολή κίνησης, δηλαδή, του περιεχομένου 10 καταχωρητών (buffer) των 60 byte από τον ένα υπολογιστή στην πόρτα 4000 του άλλου χρησιμοποιώντας ως πρωτόκολλο μεταφοράς το TCP. Για να επιλέξετε ως πρωτόκολλο μεταφοράς το UDP, προσθέστε την παράμετρο -u.

Το pcattcp, όταν παράγει κίνηση UDP, χρησιμοποιεί το μέγεθος του δεδομενογράμματος UDP προκειμένου να σηματοδοτήσει την έναρξη και λήξη της μετάδοσης κίνησης. Συγκεκριμένα, το μέγεθος των προς μετάδοση δεδομενογραμμάτων πρέπει να υπερβαίνει ένα προκαθορισμένο ελάχιστο. Η έναρξη προσδιορίζεται με την αποστολή ενός δεδομενογράμματος ελάχιστου μήκους και η λήξη με την αποστολή πολλών τέτοιων δεδομενογραμμάτων. Ο λόγος αυτής της σηματοδότησης σχετίζεται με το γεγονός ότι το πρωτόκολλο UDP δεν υποστηρίζει συνδέσεις (connectionless).

Για να απαντήσετε στις επόμενες ερωτήσεις, ο ένας από τους δυο υπολογιστές (PC1) θα αποστέλλει κίνηση UDP προς τον δεύτερο υπολογιστή PC2, ο οποίος θα τη λαμβάνει. Εκκινήστε την διαδικασία καταγραφής πακέτων στον υπολογιστή PC1, με τη βοήθεια του Wireshark. Στον υπολογιστή PC2, εκκινήστε τον αποδέκτη κίνησης UDP με τη βοήθεια την εντολής pcattcp -r -l 1024 -n 10 -p 4444 -u. Στον υπολογιστή PC1, εκκινήστε τον αποστολέα κίνησης UDP με τη βοήθεια την εντολής pcattcp -t -l 1024 -n 10 -p 4444 -u <PC2 IP address>. Παρατηρήστε τα πακέτα που καταγράφηκαν από το Wireshark.

- 3.1 Εφαρμόστε ένα φίλτρο απεικόνισης ώστε να παρατηρείτε την κίνηση και προς τις δύο κατευθύνσεις. Ποια είναι η σύνταξή του;
- 3.2 Ποιο είναι το συνολικό μέγεθος της επικεφαλίδας UDP;
- 3.3 Καταγράψτε τα ονόματα και το μήκος των πεδίων της επικεφαλίδας ενός δεδομενογράμματος UDP.
- 3.4 Ποιος είναι ο αριθμός πρωτοκόλλου για το UDP;

Παρατηρήστε το πρώτο δεδομένογραμμα UDP που αποστάλθηκε.

- 3.5 Ποιο είναι το μήκος του δεδομένογραμματος βάσει του μεγέθους του πακέτου IP εντός του οποίου ενθυλακώνεται;
- 3.6 Τι εκφράζει το πεδίο *μήκος (Length)* της επικεφαλίδας UDP;
- 3.7 Να καταγραφούν τα στοιχεία της υποδοχής (socket) που ανοίγει για την επικοινωνία στην πλευρά του αποστολέα. [*Υπόδειξη: Ζητούνται η Διεύθυνση IP, το Πρωτόκολλο Μεταφοράς και ο Αριθμός Θύρας*].
- 3.8 Να καταγραφούν τα στοιχεία της υποδοχής (socket) που ανοίγει για την επικοινωνία στην πλευρά του παραλήπτη. [*Υπόδειξη: Ζητούνται η Διεύθυνση IP, το Πρωτόκολλο Μεταφοράς και ο Αριθμός Θύρας*].
- 3.9 Πόσα δεδομένογραμμα UDP στάλθηκαν από τον αποστολέα;
- 3.10 Πόσα από αυτά τα δεδομένογραμμα UDP μεταφέρουν την κίνηση;
- 3.11 Ποιο είναι το μέγεθος αυτών των δεδομένογραμμάτων UDP;
- 3.12 Ποιο είναι το μέγεθος του ωφέλιμου φορτίου αυτών των δεδομένογραμμάτων UDP;
- 3.13 Ποιο είναι το μέγεθος των πακέτων IP που τα μεταφέρουν και ποιο το μέγεθος των αντίστοιχων πλαισίων;
- 3.14 Ποιο είναι το μέγιστο μέγεθος δεδομένογραμματος UDP που μπορεί να μεταφερθεί από ένα πακέτο IP; Αιτιολογήστε την απάντησή σας.
- 3.15 Ποιο είναι το πλήθος και ποιο το μήκος των δεδομένογραμμάτων που σηματοδοτούν το τέλος της μετάδοσης; Αιτιολογήστε την απάντησή σας.
- 3.16 Ποιο είναι το ελάχιστο μήκος δεδομένογραμμάτων της διαδικασίας σηματοδότησης που περιγράφηκε πριν;
- 3.17 Παρατηρείτε κίνηση από την πλευρά του παραλήπτη προς τον αποστολέα; Αιτιολογήστε.
- 3.18 Καταγράψτε το πλήθος των byte που μεταδόθηκαν, και στις δύο κατευθύνσεις, συμπεριλαμβανομένου του μήκους των επικεφαλίδων Ethernet, IP και UDP. [*Υπόδειξη: Συμβουλευτείτε το μενού Statistics → Conversations, στην καρτέλα που αντιστοιχεί στο UDP*].
- 3.19 Πώς προκύπτει το παραπάνω πλήθος byte συναρτήσεως των μηκών των επικεφαλίδων Ethernet, IP, UDP και του μεγέθους του ωφέλιμου φορτίου των δύο τύπων καταγεγραμμένων δεδομένογραμμάτων (σηματοδότησης και κίνησης);

Στη συνέχεια, παρατηρήστε την κίνηση που καταγράφεται από το Wireshark, όταν με τη βοήθεια του προγράμματος PCATTCIP.exe προσπαθήσετε να στείλετε συνολικά 2048 byte δεδομένων με buffer μεγέθους 2048 byte στην πόρτα 5555 του υπολογιστή 147.102.40.1, χρησιμοποιώντας το UDP ως πρωτόκολλο μεταφοράς.

- 3.20 Καταγράψτε τη σύνταξη της εντολής που χρησιμοποιήσατε.
- 3.21 Πόσα πακέτα στάλθηκαν από τον υπολογιστή σας;
- 3.22 Ποια από τα πακέτα που στάλθηκαν περιέχουν τα προς μετάδοση 2048 byte;
- 3.23 Πώς εξηγείται το μέγεθός τους;
- 3.24 Με τι είδους πακέτα απάντησε ο υπολογιστής προορισμού;
- 3.25 Τι είδους λάθος υποδεικνύουν;

Όνοματεπώνυμο:		Αρ. ΡC:	
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

2

- 2.1
- 2.2
- 2.3
- 2.4
- 2.5
- 2.6
- 2.7
- 2.8
-
- 2.9
-
- 2.10

2.11
2.12
2.13
2.14
2.15
2.16
.....
2.17
2.18
2.19
.....
2.20
2.21
2.22
2.23
2.24
.....
2.25
.....
2.26
2.27
2.28
.....
2.29
.....
2.30
2.31
.....
2.32
.....
2.33
.....
3

3.1
3.2

3.3
.....
3.4
3.5
.....
3.6
.....
3.7
3.8
3.9
3.10
3.11
3.12
3.13
3.14
.....
3.15
3.16
3.17
.....
3.18
.....
3.19
.....
3.20
3.21
3.22
3.23
.....
3.24
.....
3.25
.....