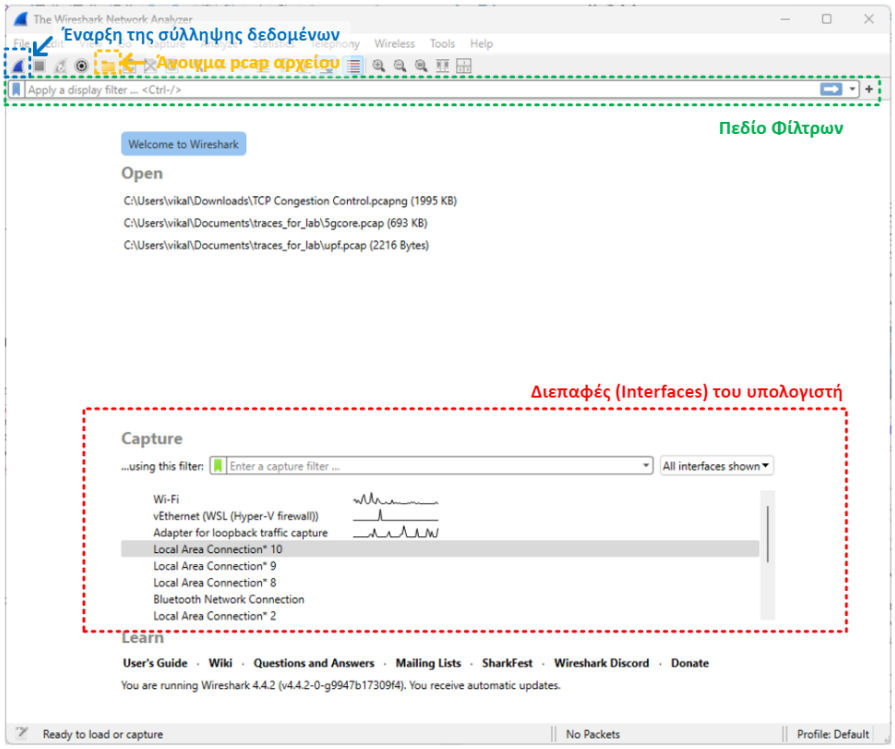
Εργαστηριακή Άσκηση 2

Στόχος:

1. **Έλεγχος Συμφόρησης TCP**
2. **Επίπεδο Δικτύου**
   - Διευθυνσιοδότηση IP (στατική και μέσω DHCP)

Για να μελετήσουμε τους μηχανισμούς ελέγχου συμφόρησης του TCP, θα χρησιμοποιήσουμε ένα άλλο πρόγραμμα, το Wireshark. Το Wireshark είναι ελεύθερο και ανοιχτού κώδικα λογισμικό ανάλυσης πρωτοκόλλων δικτύου υπολογιστών. Χρησιμοποιείται για ανάλυση δικτύου, παρακολούθηση δικτύου, εντοπισμό και αντιμετώπιση προβλημάτων στα δίκτυα και για εκπαίδευση. Μπορείτε να κατεβάστε το πρόγραμμα από την επίσημη ιστοσελίδα (https://www.wireshark.org/#download), και να δείτε τον αναλυτικό οδηγό χρήσης του (https://www.wireshark.org/docs/wsug_html_chunked/).



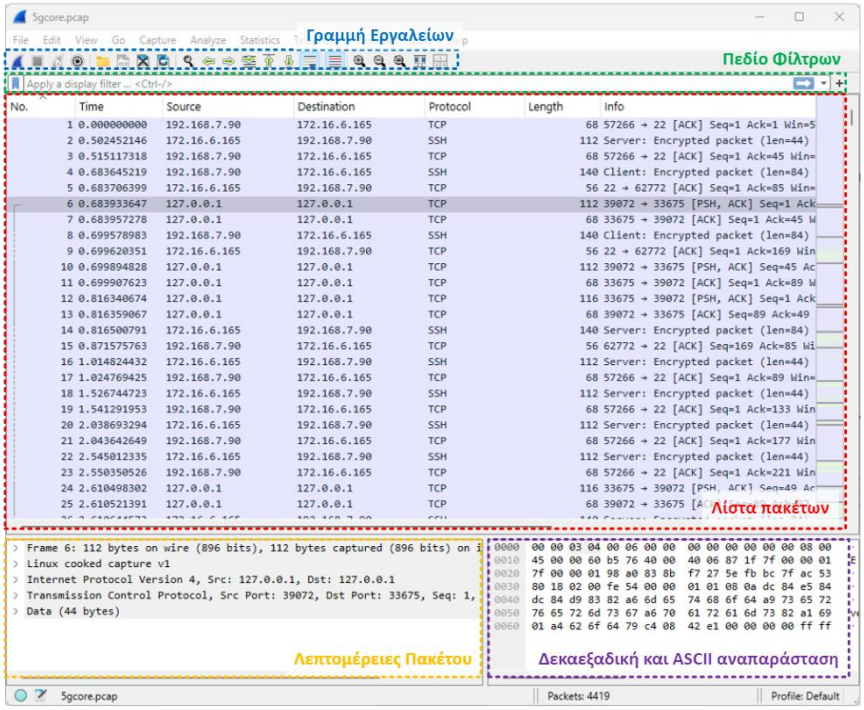
Η αρχική οθόνη του Wireshark φαίνεται στο παραπάνω σχήμα. Όταν ανοίγει το πρόγραμμα, ο χρήστης έχει δύο βασικές επιλογές για να ξεκινήσει την ανάλυσή του. Η επιλογή εξαρτάται από το αν επιθυμεί να εξετάσει τη ζωντανή κίνηση του δικτύου ή να εργαστεί με ένα ήδη καταγεγραμμένο αρχείο.

- Η πρώτη επιλογή είναι η σύλληψη πακέτων δικτύου σε πραγματικό χρόνο. Για να το επιτύχει αυτό, μπορεί να επιλέξει μία από τις διαθέσιμες δικτυακές διεπαφές που εμφανίζονται στην αρχική οθόνη, όπως Wi-Fi ή Ethernet, και να ξεκινήσει τη σύλληψη πατώντας το κουμπί "Start". Κατά τη διάρκεια της σύλληψης, μπορεί να παρακολουθεί ζωντανά την κίνηση του δικτύου που περνά από

τη διεπαφή που έχει επιλεγεί. Με το κουμπί "Stop" η σύλληψη πακέτων σταματάει και τότε μπορεί να γίνει ανάλυση των καταγεγραμμένων πακέτων.

- Η δεύτερη επιλογή είναι η φόρτωση ενός αποθηκευμένου αρχείου PCAP. Τα αρχεία PCAP (Packet Capture) περιέχουν καταγεγραμμένα δεδομένα δικτύου που έχουν συλλεχθεί από εργαλεία παρακολούθησης, όπως το Wireshark. Για να ανοίξει ένα τέτοιο αρχείο, ο χρήστης μπορεί να χρησιμοποιήσει την επιλογή "Open a capture file" και να επιλέξει το αρχείο PCAP που επιθυμεί να αναλύσει. Μόλις φορτωθεί το αρχείο, εμφανίζεται η λίστα των πακέτων, όπου μπορεί να εφαρμόσει φίλτρα ή να μελετήσει συγκεκριμένα δεδομένα.

Όταν ξεκινάει η σύλληψη πακέτων ή ανοίγεται ένα αρχείο PCAP στο Wireshark, η οθόνη χωρίζεται σε τμήματα που παρέχουν λεπτομερείς πληροφορίες για την ανάλυση των πακέτων, όπως φαίνεται στο επόμενο σχήμα.



Η γραμμή εργαλείων βρίσκεται στην κορυφή, όπου υπάρχουν επιλογές για βασικές λειτουργίες, όπως η έναρξη ή διακοπή της σύλληψης και η αποθήκευση αρχείων, και εργαλεία για τη διευκόλυνση της ανάλυσης, όπως η αναζήτηση πακέτων στη λίστα ή η πλοήγηση στο επόμενο ή προηγούμενο πακέτο. Πιο κάτω βρίσκεται το πεδίο φίλτρων, που επιτρέπει την εφαρμογή κριτηρίων για τον περιορισμό των εμφανιζόμενων πακέτων. Κάτω από αυτά, εμφανίζεται η λίστα πακέτων, όπου κάθε γραμμή περιλαμβάνει πληροφορίες όπως διευθύνσεις προέλευσης και προορισμού, το πρωτόκολλο και μια σύντομη περιγραφή του περιεχομένου. Στο κάτω μέρος αριστερά βρίσκονται οι λεπτομέρειες του επιλεγμένου πακέτου, δομημένες σε μορφή δέντρου, επιτρέποντας την ανάλυση κάθε επιπέδου, όπως Ethernet, IP ή TCP/UDP. Τέλος, στο κάτω μέρος δεξιά, εμφανίζεται η δεκαεξαδική και ASCII αναπαράσταση του πακέτου, παρέχοντας ακριβή δεδομένα για περαιτέρω μελέτη.

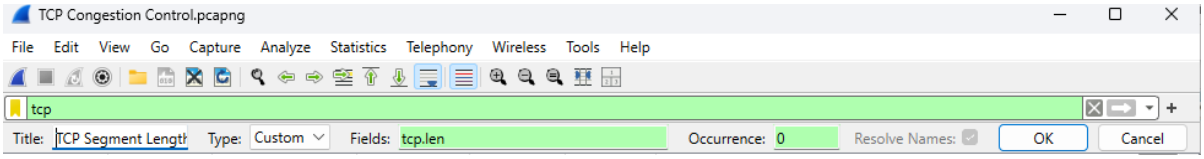
Πρακτικό Μέρος:

A. Έλεγχος συμφόρησης TCP

Στο wireshark, ανοίξτε το αρχείο TCP-Congestion-Control.pcap. Το αρχείο περιλαμβάνει όλα τα μηνύματα κατά την εκτέλεση του προγράμματος iperf. Το iperf βασίζεται σε ένα μοντέλο client-server στο οποίο ο client δημιουργεί ροές TCP (ή UDP) και στέλνει κίνηση στον server, στη συνέχεια, αναφέρει το μέγιστο εύρος ζώνης στον client.

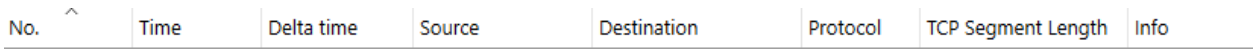
a. Αρχικά, φιλτράρετε τα πακέτα που εμφανίζονται στο παράθυρο του Wireshark πληκτρολογώντας "tcp" στο πεδίο των φίλτρων στην κορυφή του παραθύρου του Wireshark. Το wireshark εμφανίζει τα δικτυακά επίπεδα με σειρά προτεραιότητας από το υψηλότερο προς το χαμηλότερο επίπεδο δικτύου. Αυτό σημαίνει ότι στη στήλη protocol τα μηνύματα μπορεί να εμφανίζονται ως iperf3, αν η έκδοση του wireshark που έχετε αναγνωρίζει το iperf.

b. Επειδή όπως είπαμε θα μιλήσουμε για το TCP, στη στήλη Len, πατήστε δεξί κλικ-> edit column, μετονομάστε τη σε TCP Segment Len, στο πεδίο Type επιλέξτε custom, και στο Field πληκτρολογήστεντο φίλτρο tcp.len. Έπειτα πατήστε OK.



c. Δημιουργήστε μία νέα στήλη (edit -> preferences -> appearance ->columns -> add -> OK). Μια νέα στήλη με όνομα New column θα εμφανιστεί στο κυρίως παράθυρο. Πατήστε δεξί κλικ στη στήλη, edit column στο πεδίο Title πληκτρολογήστε Delta time και στο πεδίο Type επιλέξτε Delta time, και πατήστε OK. Το delta time σε κάθε πακέτο δείχνει το χρόνο που πέρασε από το προηγούμενο πακέτο μέχρι να ληφθεί αυτό το πακέτο.

Στο κυρίως παράθυρο, θα πρέπει να εμφανίζονται οι 8 στήλες Number (No.), Time, Delta time, Source, Destination, Protocol, Len, Info.



Ερωτήσεις

A1. Εντοπίστε τα μηνύματα της 3μερούς χειραψίας TCP.

A2. Ποια είναι η διεύθυνση IP και ο αριθμός θύρας TCP που χρησιμοποιούνται από τους δύο υπολογιστές; Ποιος είναι ο client και ποιος ο server;

A3. Δικαιολογείστε τους αριθμούς ακολουθίας (sequence number - Seq) και επιβεβαίωσης (acknowledgement number -Ack) των μηνυμάτων της 3μερούς χειραψίας. Πώς καθορίστηκαν οι τιμές τους;

A4. Ποιο είναι το μέγιστο μέγεθος του TCP Τμήματος (MSS);

A5. Τι είναι το παράθυρο συμφόρησης (Congestion Window- cwnd); Ποιο είναι το αρχικό του μέγεθος (σε MSS)

A6. Ποιος είναι περίπου ο χρόνος μετ' επιστροφής (RTT) του δικτύου; Εξηγήστε την απάντηση σας.

A7. Ποιος είναι ο αρχικός ρυθμός αποστολής; (σε kbps)

A8. Πόσο μεγαλώνει το cnwd μετά από κάθε ριπή δεδομένων; (Εξετάστε τις επόμενες δύο ρίπες)

A9. Προσθέστε δυο έξτρα στήλες: μία που να δείχνει τα "bytes in flight"και μία που να δείχνει το "calculated window size". Bytes in flight είναι ο όγκος των εκκρεμών δεδομένων που ο αποστολές έχει στείλει στο δίκτυο αλλά δεν έχει λάβει ακόμη επιβεβαίωση, Το calculated window size είναι

το παράθυρο λήψης (receive window-rwnd) του παραλήπτη, δηλαδή πόσα bytes μπορεί να δεχθεί κάθε φορά.

i. Ποιο είναι το μέγεθος του rwnd του client και του server αντίστοιχα; (Για την απάντηση σας, αγνοήστε τα πακέτα της 3μερους χειραψίας)
ii. Πως αυτές οι δύο στήλες μας βοηθούν να βρούμε τη μέγιστη τιμή του congestion window;
iii. Σε ποιο πακέτο αρχίζει να παρατηρείται συμφόρηση;

Υπόδειξη: Για να φτιάξετε τις στήλες αυτές, πηγαίνετε σε ένα οποιοδήποτε πακέτο του client, βρείτε στον TCP header τις μεταβλητές αυτές, δεξί κλικ πάνω τους -> add as column.

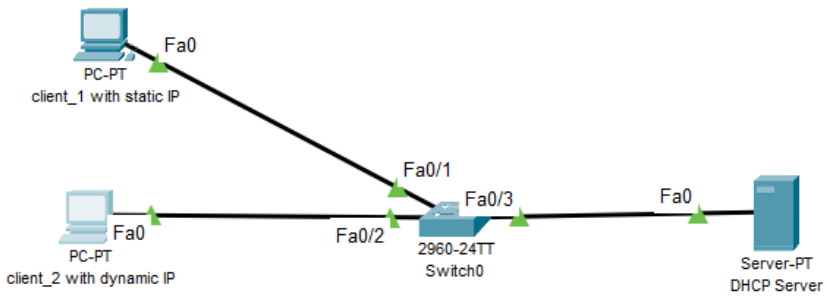
A10. Μεταβείτε στο πακέτο 3358.

i. Τι συνέβη σε αυτό το σημείο;
ii. Τι συμβαίνει με το παράθυρο συμφόρησης; Για να το δείτε αυτό μεταβείτε στο πακέτο 3504, όπου ξαναξεκινά η αποστολή δεδομένων.
iii. Αν τη στιγμή της απώλειας το cnwd ήταν 200 MSS, ποια είναι η μέση ρυθμαπόδοση TCP;

A11. Επιλέξτε ένα πακέτο και μεταβείτε στα Statistics > TCP Stream Graph > Time-Sequence Graph (Stevens). Αυτό το γράφημα δείχνει την εξέλιξη της μεταφοράς δεδομένων με την πάροδο του χρόνου. Πατήστε το κουμπί “Switch Direction”, ώστε η ροή να είναι από τον client στον server. Ο χρόνος (σε δευτερόλεπτα) είναι στον άξονα x και ο σχετικός αριθμός σειράς (sequence number) κάθε πακέτου είναι στον άξονα y. Κάθε κουκκίδα αντιπροσωπεύει ένα πακέτο. Μπορείτε να προσδιορίσετε σε ποια χρονική στιγμή συμβαίνει η απώλεια και πως αντιδρά ο client;

B. IP Διευθυνσιοδότηση

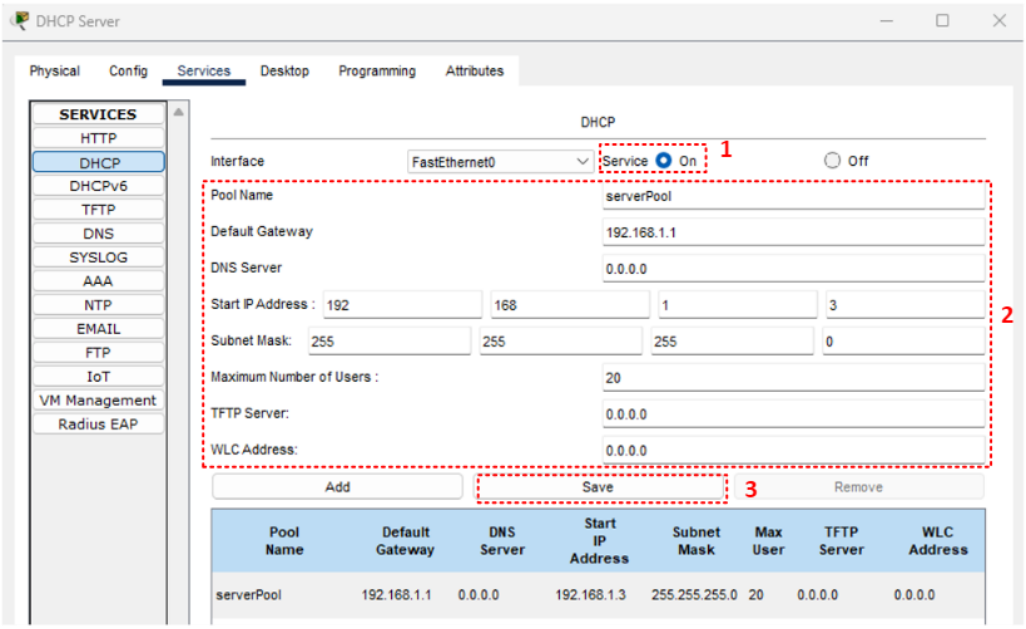
1. Ανοίξτε το πρόγραμμα CPT. Στο χώρο εργασίας, φτιάξτε τη παρακάτω τοπολογία.



2. Επιλέξτε τον DHCP server, μεταβείτε στην επιφάνεια εργασίας (Desktop) του και επιλέξτε το πρόγραμμα IP Configuration. Επιλέξτε Static και συμπληρώστε τα πεδία IPv4 address, Subnet Mask και Default Gateway με βάση τον πίνακα:

IPv4 address	192.168.1.254
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1

3. Επιλέξτε πάλι τον DHCP server, πηγαίνετε στην καρτέλα Services. Επιλέξτε το DHCP και συμπληρώστε το όπως φαίνεται στην εικόνα παρακάτω:



Ερωτήσεις

B1. Με βάση την IP και το subnet mask που δώσατε στον server, ποιο είναι το υποδίκτυο που συνδέεται(σε μορφή x.x.x.x/x); Πόσες είναι οι διαθέσιμες IP διευθύνσεις σε αυτό το υποδίκτυο;

B2. Δώστε τη στατική IP 192.168.1.1 στο client_1 with static IP. Δικαιολογήστε τη τιμή που βάλατε σε κάθε άλλο πεδίο που συμπληρώσατε (IPv4 Address, Subnet Mask, Default Gateway).

B3. Πηγαίνετε στο client_2 with Dynamic IP->Desktop->IP Configuration και επιλέξτε dynamic αντί για static IP. Επιβεβαιώστε ότι το PC λαμβάνει σωστή IP στο επιθυμητό δίκτυο.(Μπορεί να χρειαστεί λίγο χρόνο). Τι IP έλαβε;

B4. Καταγράψτε τα μηνύματα που ανταλλάσσονται μεταξύ του DHCP server και του client_2. Για το σκοπό αυτό:

a) Πηγαίντε σε λειτουργία προσομοίωσης.

b) Πηγαίνετε στο command prompt του client_2 και πληκτρολογήστε την εντολή “ipconfig /renew”. Η εντολή αυτή θα σβήσει την τωρινή IP και θα ξαναζητήσει από τον DHCP server IP διεύθυνση.

c) Στο παράθυρο τη προσομοίωσης, φιλτράρετε τα πακέτα ώστε να δείχνει μόνο το DHCP πρωτόκολλο, και πατήστε το forward τόσες φορές ώστε να εμφανιστεί η απάντηση από την εντολή “ipconfig /renew” στο command prompt.

d) Βρείτε τα μηνύματα του DHCP πρωτοκόλλου (discover, offer, request, ack).

i. Σε ποιο πρωτόκολλο επιπέδου μεταφορά βασίζεται το DHCP?

ii. Σημειώστε και σχολιάστε το source kai destination IP τη κεφαλίδας IP κάθε πακέτου.

iii. Σχεδιάστε το διάγραμμα χρονικής ακολουθίας, σημειώνοντας σε κάθε πακέτο τα source και destination IP.

Για αυτή την εργασία, θα χρειαστεί να γράψετε μια αναφορά που να απαντά προσεκτικά στις ερωτήσεις A (1-11) και B (1-4), όπως περιγράφονται παραπάνω. Σας παρακαλούμε να οργανώσετε την αναφορά σας έτσι ώστε οι απαντήσεις σας να είναι ξεκάθαρα σημειωμένες για κάθε ερώτηση και ενότητα της εργασίας. Όποτε είναι δυνατόν, όταν απαντάτε σε μια ερώτηση, μπορείτε να δίνετε μια εικόνα (screenshot) του πακέτου που σας βοήθησε να απαντήσετε στην ερώτηση. Μπορείτε να σημειώνετε πάνω στην εικόνα για να εξηγείτε την απάντησή σας.