Εργαστηριακή Άσκηση 4
Πρωτόκολλο IPv4 και θρυμματισμός

Ο σκοπός αυτής της εργαστηριακής άσκησης είναι η σε μεγαλύτερο βάθος εξέταση των ιδιοτήτων του πρωτοκόλλου IPv4. Θα παρατηρήσετε τα πακέτα ICMP που παράγονται κατά την εκτέλεση της εντολής ping που χρησιμοποιείται ευρέως για διαγνωστικούς λόγους και για μετρήσεις επίδοσης στο διαδίκτυο. Επιπλέον, θα δείτε με λεπτομέρεια τη λειτουργία του θρυμματισμού (fragmentation) μεγάλων πακέτων IPv4. Περισσότερες πληροφορίες για το πρωτόκολλο IPv4 μπορείτε να βρείτε στο RFC (Request For Comment) 791 στην ιστοθέση https://tools.ietf.org/html/rfc791. Για τη δομή των επικεφαλίδων των πρωτοκόλλων της σουίτας TCP/IP μπορείτε επίσης να 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.

Η εντολή ping ελέγχει εάν μια διεπαφή (interface) με δεδομένη διεύθυνση IP διαδίκτυο είναι ενεργή (*alive* ή *up*). Στην περίπτωση διευθύνσεων IPv4 χρησιμοποιεί το πρωτόκολλο ICMP (Internet Control Message Protocol) για να στείλει ένα μήνυμα *Αίτησης Ηχούς* (*Echo Request)*, έτσι ώστε να λάβει μια *Απάντηση Ηχούς* (*Echo Reply)* από τον συγκεκριμένο κόμβο. Αντίστοιχα, στην περίπτωση διευθύνσεων IPv6 χρησιμοποιείται το ICMPv6. Για τη μεταφορά του στο διαδίκτυο, το μήνυμα ICMP ενθυλακώνεται μέσα σε πακέτο IPv4. Η συνολική χρονική διάρκεια ταξιδιού RTT (Round-Trip Time) των μηνυμάτων *Echo Request* και *Echo Reply* δίνει μια ένδειξη για τη φόρτιση του δικτύου. Στα Windows, το ping στέλνει τέσσερα διαδοχικά πακέτα *Αίτησης Ηχούς* (*Echo Request)*, γι' αυτό βλέπετε τέσσερα αποτελέσματα. Σε συστήματα Unix/Linux στέλνονται συνέχεια πακέτα *Echo Request* μέχρι να σταματήσετε την εκτέλεση της εντολής. Για μια πιο λεπτομερή περιγραφή δείτε το παράδειγμα ping του διαγράμματος ροής μηνυμάτων ICMP στην ιστοσελίδα https://eventhelix.com/Networking/Icmp.pdf.

Όμως τα αποτελέσματα του ping δεν μπορεί να θεωρηθούν σε καμία περίπτωση πλήρως αξιόπιστα, όσον αφορά τη σωστή επικοινωνία και δρομολόγηση πακέτων. Για παράδειγμα, αν με τη βοήθεια της εντολής αυτής, βρεθεί μια επαφή ανενεργή, δεν εξυπακούεται ότι πράγματι είναι. Πιο συγκεκριμένα, αν δε ληφθεί *Echo Reply* από τον προορισμού, υπάρχει πιθανότητα να παρεμβάλλεται στη διαδρομή κάποιο τείχος προστασίας (firewall), που να μπλοκάρει τα μηνύματα του πρωτοκόλλου ICMP. Επίσης είναι δυνατό ο κόμβος προορισμού ή κάποια ενδιάμεση συσκευή να μην είναι επαρκώς πληροφορημένη για το δίκτυο του αποστολέα και έτσι να μην είναι δυνατή η σωστή επιστροφή της απάντησης.

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

1 – Μετρήστε την καθυστέρηση

Στο παρελθόν, κατά την εκτέλεση της εντολής ping προς τον εξυπηρετητή ιστού του MIT, λήφθηκε η επόμενη απάντηση

```
C:\>ping www.mit.edu

Pinging www.mit.edu [18.7.22.83] with 32 bytes of data:

Reply from 18.7.22.83: bytes=32 time=136ms TTL=242
Reply from 18.7.22.83: bytes=32 time=136ms TTL=242
Reply from 18.7.22.83: bytes=32 time=136ms TTL=242
Reply from 18.7.22.83: bytes=32 time=136ms TTL=242

Ping statistics for 18.7.22.83:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 136ms, Maximum = 136ms, Average = 136ms

C:\>
```

που σημαίνει ότι στάλθηκαν 4 πακέτα μήκους 32 bytes στη διεπαφή με IPv4 διεύθυνση 18.7.22.83 του εξυπηρετητή ιστού με όνομα www.mit.edu, που βρίσκεται 13 βήματα μακριά, απαντήθηκαν όλα (0% απώλειες) και μετρήθηκε μέση καθυστέρηση 136 ms.

Στη συνέχεια θα καταγραφούν, με τη βοήθεια του Wireshark, τα πακέτα IPv4 που ανταλλάσσονται όταν εκτελείται η εντολή ping προς το www.mit.edu. Αφού ξεκινήσετε το Wireshark, από το μενού *Capture → Options…* επιλέξτε την κάρτα δικτύου του υπολογιστή σας μέσω της οποίας συνδέεστε στο τοπικό δίκτυο. Στο σχετικό με το φίλτρο σύλληψης πεδίο γράψτε not multicast and not broadcast, προκειμένου να περιορισθεί το πλήθος των πλαισίων που καταγράφονται, και πιέστε το *Start* για να αρχίζει η καταγραφή.

Αφού μελετήσετε τη σύνταξη της εντολής ping στο περιβάλλον λειτουργικού συστήματος του προσωπικού σας υπολογιστή, επαναλάβετε την παραπάνω μέτρηση, χρησιμοποιώντας την κατάλληλη σύνταξή της ώστε να παραχθούν **τρία** πακέτα **IPv4/ICMP**. Σταματήστε την καταγραφή μόλις ολοκληρωθεί η εκτέλεση της εντολής πιέζοντας τον συνδυασμό πλήκτρων <Ctrl>+E.

1.1 Ποια η ακριβής σύνταξη της εντολής ping που χρησιμοποιήσατε;
1.2 Ποια η σημασία του φίλτρου σύλληψης που εφαρμόσατε; *[Υπόδειξη: Ανατρέξτε στην ιστοσελίδα παραδειγμάτων για φίλτρα σύλληψης https://wiki.wireshark.org/CaptureFilters].*
1.3 Με βάση τα αποτελέσματα από την εκτέλεση της εντολής στο παράθυρο εντολών να καταγράψετε το ποσοστό απωλειών πακέτων και τη μέση καθυστέρηση.
1.4 Να καταγραφούν οι τιμές του RTT, όπως εμφανίζονται στο παράθυρο εντολών.
1.5 Να καταγραφούν οι τιμές του RTT για κάθε ζεύγος Echo Request – Reply, με τη βοήθεια του Wireshark. Συμφωνούν με τις αντίστοιχες στο παράθυρο εντολών; *[Υπόδειξη: Από το μενού View→Time Display Format επιλέξτε Seconds Since Previous Displayed Packet.]*
1.6 Ποιο φίλτρο απεικόνισης (Display Filter) πρέπει να εφαρμόσετε προκειμένου να παρατηρείτε μόνο πακέτα IPv4;
1.7 Ποιο φίλτρο απεικόνισης πρέπει να εφαρμόσετε προκειμένου να παρατηρείτε μόνο την κίνηση ICMP που προκάλεσε η εντολή ping;

Παρατηρώντας την καταγεγραμμένη κίνηση στο Wireshark να απαντήσετε στα παρακάτω ερωτήματα:

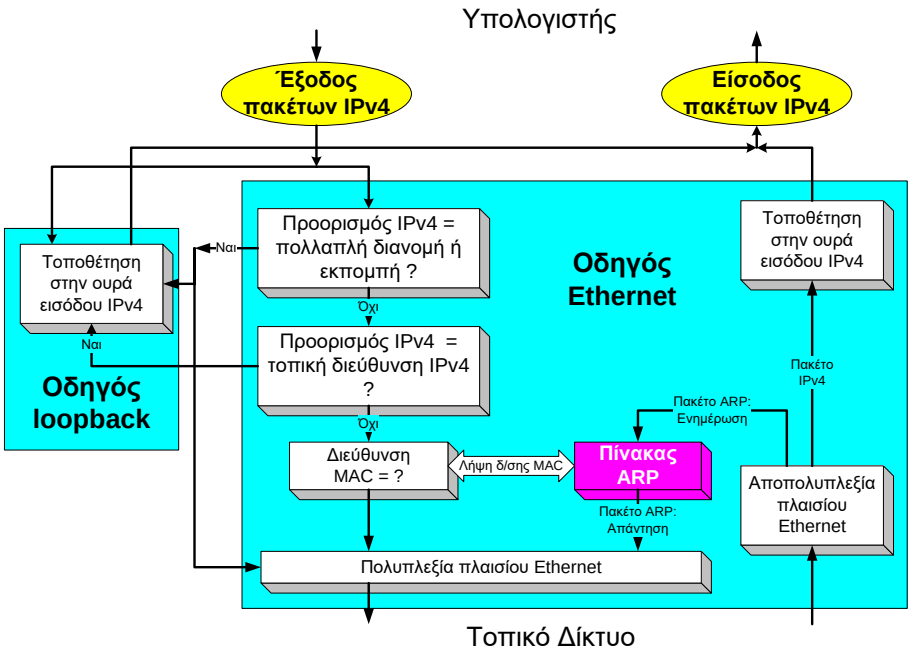
1.8 Τι είδος μηνυμάτων ICMP στάλθηκαν από τον υπολογιστή σας κατά την εκτέλεση της εντολής ping;
1.9 Ποιες οι διευθύνσεις IPv4 πηγής και προορισμού των παραπάνω μηνυμάτων;
1.10 Τι είδος μηνυμάτων ICMP ελήφθησαν από τον υπολογιστή σας κατά την εκτέλεση της εντολής ping;
1.11 Ποιες οι διευθύνσεις IPv4 πηγής και προορισμού των παραπάνω μηνυμάτων;
1.12 Τι έχει αλλάξει σε σχέση με την καταγραφή του παρελθόντος;

2 – Περισσότερα για το Ping

Στο σχήμα της επόμενης σελίδας βλέπετε παραστατικά τον τρόπο με τον οποίο ο οδηγός (driver) της κάρτας Ethernet χειρίζεται τα πακέτα IPv4 ανάλογα με τον προορισμό τους καθώς και τη σχέση του βρόχου επιστροφής, μιας εικονικής διεπαφής που χρησιμοποιείται για την επικοινωνία διεργασιών εντός του υπολογιστή σας, με τον οδηγό Ethernet.

Ξεκινήσετε μια καταγραφή με το Wireshark χρησιμοποιώντας το ίδιο φίλτρο σύλληψης και φίλτρο απεικόνισης όπως προηγουμένως. Στη συνέχεια, από τη γραμμή εντολών, εκτελέστε διαδοχικά ping στέλνοντας **5** πακέτα **ICMP** στις ακόλουθες διευθύνσεις:

i. Τη διεύθυνση IPv4 ενός μηχανήματος του εντός του τοπικού σας δικτύου, π.χ., της προκαθορισμένης πύλης.
ii. Τη διεύθυνση IPv4 της διεπαφής δικτύου του υπολογιστή σας.
iii. Τη διεύθυνση 127.0.0.1 του βρόχου επιστροφής (loopback).



Όταν ολοκληρωθεί η εκτέλεση όλων των εντολών σταματήστε την καταγραφή. Παρατηρώντας την καταγεγραμμένη κίνηση στο Wireshark και συμβουλευόμενοι όπου χρειάζεται το σχήμα απαντήστε στα παρακάτω ερωτήματα:

2.1 Ποια είναι η ακριβής σύνταξη της εντολής ping που χρησιμοποιήσατε;
2.2 Πόσα από τα μηνύματα ICMP *Echo request* που έχουν αποσταλεί από τον υπολογιστή σας έχει καταγράψει το Wireshark;
2.3 Ποιος ήταν ο προορισμός τους;
2.4 Παρατηρήσατε αποστολή μηνυμάτων ICMP *Echo request* στο δίκτυο με πηγή και προορισμό τη διεύθυνση IPv4 του υπολογιστή σας; Εξηγήστε.
2.5 Παρατηρήσατε αποστολή μηνυμάτων ICMP *Echo request* προς τη διεύθυνση του βρόχου επιστροφής; Εξηγήστε.
2.6 Ποια η διαφορά όταν κάνετε ping στη διεπαφή του υπολογιστή σε σχέση με ping στη διεύθυνση loopback αυτού 127.0.0.1; *[Υπόδειξη: Η απάντηση σχετίζεται με το ρόλο του βρόχου επιστροφής σε ένα δικτυωμένο σταθμό εργασίας.]*

Ανοίξτε τον φυλλομετρητή της αρεσκείας σας και επισκεφτείτε την ιστοσελίδα της Netflix (https://www.netflix.com). Μόλις η σελίδα φορτωθεί πλήρως, χρησιμοποιήστε την εντολή ping ώστε να παράγονται πακέτα IPv4/ICMP με προορισμό τον εξυπηρετητή www.netflix.com. Στη συνέχεια επισκεφτείτε την ιστοσελίδα της Amazon (https://www.amazon.com). Μόλις η σελίδα φορτωθεί πλήρως, χρησιμοποιήστε όπως πριν την εντολή ping με προορισμό τον εξυπηρετητή www.amazon.com.

2.7 Τι παράδοξο παρατηρείτε και τι μπορείτε να υποθέσετε για να το εξηγήσετε;

3 – Επικεφαλίδες IPv4

Στη συνέχεια θα κάνετε χρήση των υπηρεσιών Telnet και FTP του υπολογιστή edu-dy.cn.ntua.gr με IPv4 διεύθυνση 147.102.40.15. Ξεκινήστε μια νέα καταγραφή με φίλτρο σύλληψης τη διεύθυνση IPv4 του edu-dy.cn.ntua.gr. Για την υπηρεσία Telnet[1] πληκτρολογήστε `telnet edu-dy.cn.ntua.gr` σε ένα παράθυρο εντολών. Στην προτροπή `login:` πληκτρολογήστε `user` ακολουθούμενο από <Enter>, ενώ στην προτροπή `Password:` πληκτρολογήστε `test` ακολουθούμενο από <Enter>. Τέτοιος χρήστης

[1] Σε συστήματα Windows θα χρειαστεί να την ενεργοποιήσετε από το *Turn Windows features on or off* ακολουθώντας οδηγίες που θα βρείτε με αναζήτηση στο διαδίκτυο ανάλογα με τη συγκεκριμένη έκδοση που διαθέτετε.

δεν υπάρχει και η προσπάθειά σας θα αποτύχει, οπότε πληκτρολογήστε <Ctrl>+] και μετά quit για να τερματίσετε την εφαρμογή telnet. Στη συνέχεια, για την υπηρεσία FTP του ίδιου υπολογιστή, πληκτρολογήστε ftp edu-dy.cn.ntua.gr. Στην προτροπή User: πληκτρολογήστε anonymous ακολουθούμενο από <Enter>, ενώ στην προτροπή Password: πατήστε <Enter>. Εκτελέστε την εντολή ls, ώστε να δείτε τα αρχεία που βρίσκονται στον εξυπηρετητή. Τέλος πληκτρολογήστε bye για να τερματίσετε την εφαρμογή ftp και σταματήστε την καταγραφή των πακέτων.

3.1 Ποια είναι η σύνταξη του φίλτρου σύλληψης που χρησιμοποιήσατε;
3.2 Εφαρμόστε φίλτρο απεικόνισης ώστε να παραμείνουν μόνο τα πακέτα IPv4 που έστειλε ο υπολογιστής σας. Ποια είναι η σύνταξή του;

Με κλικ στο σύμβολο '>' στα αριστερά της επικεφαλίδας Internet Protocol Version 4 (στο παράθυρο με τις λεπτομέρειες) αναπτύξετε τα περιεχόμενά της.

3.3 Καταγράψτε τα ονόματα και το μήκος σε bit των πεδίων της επικεφαλίδας του πακέτου IPv4 και σημειώστε στο σχήμα τις θέσεις τους.

Χρησιμοποιώντας το πλήκτρο ↓ (κάτω βέλος) μετακινηθείτε από το πρώτο στο τελευταίο μήνυμα της σειράς πακέτων IPv4 που έστειλε ο υπολογιστής σας.

3.4 Ποια πεδία της επικεφαλίδας IPv4 αλλάζουν τιμές;
3.5 Είναι το μήκος της επικεφαλίδας IPv4 το ίδιο σε όλα τα πακέτα;
3.6 Ποιο είναι το μικρότερο και ποιο το μεγαλύτερο μήκος πακέτου IPv4 που παρατηρήσατε;
3.7 Τι τιμή έχει το πεδίο *Differentiated Services Field* και σε ποια ποιότητα υπηρεσίας αντιστοιχεί; *[Υπόδ. Δείτε https://en.wikipedia.org/wiki/Differentiated_services.]*
3.8 Τι παρατηρείτε για τις τιμές του πεδίου *Identification*;
3.9 Τι τιμή έχει η σημαία *Don't Fragment*;
3.10 Τι τιμή έχει το πεδίο *Fragment Offset*;
3.11 Τι τιμή έχει το πεδίο *Protocol* και σε ποιο πρωτόκολλο αντιστοιχεί;
3.12 Γιατί σε κάθε πακέτο IPv4 αλλάζει η τιμή του πεδίου *Header Checksum*;

4 – Θρυμματισμός (Fragmentation) στο IPv4

Κάθε δίκτυο επιβάλει ένα μέγιστο μέγεθος στα πακέτα του. Π.χ., το μέγιστο μέγεθος πακέτου IPv4 είναι 65.535 byte. Όμως σε ένα Ethernet LAN το μέγιστο μέγεθος πλαισίου είναι το πολύ 1.518 byte (αλλά κατ' ελάχιστο 64 byte). Ένα προφανές πρόβλημα θα εμφανισθεί όταν ένα μεγάλο πακέτο IPv4 θέλει να ταξιδεύσει μέσω μιας ζεύξης όπου το μέγιστο μέγεθος πλαισίου 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 IPv4. Όταν τα θραύσματα φτάσουν στον τελικό προορισμό τους, ο παραλήπτης φροντίζει για την ανασύνθεση τους στο αρχικό πακέτο IPv4 με τη βοήθεια των ειδικών γι' αυτό τον σκοπό πεδίων (*Identification, More fragments flag* και *Fragment offset*) στην επικεφαλίδα κάθε πακέτου IPv4. Η ανασύνθεση γίνεται μόνο από τον τελικό παραλήπτη, ενώ ο θρυμματισμός μπορεί να γίνει από οποιονδήποτε από τους ενδιάμεσους, στο μονοπάτι δρομολόγησης, σύμφωνα με τις ανάγκες.

Εξ αιτίας του εκάστοτε πρωτοκόλλου στρώματος ζεύξης δεδομένων, κάθε δικτυακή διεπαφή έχει μια μέγιστη μονάδα μεταφοράς MTU (Maximum Transmission Unit) που αντιστοιχεί στο μέγεθος του μεγαλύτερου **πακέτου IPv4** που μπορεί να μεταδοθεί χωρίς θρυμματισμό. Στην τοπική ζεύξη ή το τοπικό LAN, οι κόμβοι μπορούν να στείλουν πακέτα IPv4 μέχρι το μέγεθος της MTU. Στο διαδίκτυο, όλοι οι κόμβοι απαιτείται να δέχονται πακέτα IPv4 μέχρι 576 byte, είτε ολόκληρα είτε θρυμματισμένα. Για να στείλουν πακέτα IPv4 μεγαλύτερου μήκους πρέπει να ελέγχουν αν ο προορισμός μπορεί να τα δεχθεί. Ένας τρόπος για να εξακριβωθεί η τιμή της MTU είναι να σταλθεί ένα μήνυμα ICMP *Echo Request* με ενεργοποιημένη τη σημαία *Don't Fragment* που εμποδίζει τον θρυμματισμό του πακέτου IPv4, και καθορίζοντας ταυτόχρονα το μέγεθος των δεδομένων του. Εάν το συνολικό μήκος πακέτου IPv4 που προκύπτει είναι μεγαλύτερο από την MTU κάποιας

ενδιάμεσης στη διαδρομή διεπαφής, τότε το μήνυμα ICMP δε θα προωθηθεί και θα εμφανιστεί μήνυμα λάθους, ενώ σε αντίθετη περίπτωση θα παραδοθεί.

4.1 Ποια είναι η ακριβής σύνταξη της εντολής ping που πρέπει να χρησιμοποιήσετε ώστε να στείλετε χωρίς θρυμματισμό ένα μόνο πακέτο IPv4 που να μεταφέρει μήνυμα ICMP *Echo request* με συγκεκριμένο μέγεθος δεδομένων; *[Υπόδειξη: Αναζητείστε στην τεκμηρίωση της εντολής ping επιλογή για Don't fragment flag ή για ενεργοποίηση της MTU discovery]*

Εφαρμόζοντας την παραπάνω σύνταξη της εντολής, δοκιμάστε διάφορες τιμές για το μέγεθος δεδομένων ICMP στην περιοχή των 1480 byte κάνοντας ping με προορισμό τη διεύθυνση IPv4 κάποιου ενεργού κόμβου στο τοπικό σας δίκτυο.

4.2 Ποια είναι η μέγιστη τιμή για την οποία επιτυγχάνει η αποστολή;
4.3 Ποια η μικρότερη τιμή για την οποία απαιτείται θρυμματισμός;

Στη συνέχεια χρησιμοποιήστε το Wireshark με φίλτρο σύλληψης ώστε να καταγράφονται μόνο πλαίσια μονο-εκπομπής (unicast) για να παρατηρήσετε τι ακριβώς συμβαίνει. Επαναλάβετε τα ping για τις δύο τιμές που προσδιορίσατε προηγουμένως στα ερωτήματα 4.2 και 4.3, αντίστοιχα. Μόλις ολοκληρωθεί η καταγραφή, εφαρμόστε ένα φίλτρο απεικόνισης ώστε να παραμείνουν μόνο πακέτα IPv4 από και προς τη διεύθυνση IPv4 όπου κάνατε ping.

4.4 Γράψτε τη σύνταξη του φίλτρου σύλληψης που χρησιμοποιήσατε. *[Υπόδειξη: Συμβουλευτείτε τη σελίδα https://wiki.wireshark.org/CaptureFilters]*
4.5 Γράψτε τη σύνταξη του φίλτρου απεικόνισης που εφαρμόσατε.
4.6 Παράγονται πακέτα IPv4 όταν χρησιμοποιείτε την τιμή της ερώτησης 4.3; Γιατί;
4.7 Ποιο είναι το μέγεθος της MTU της διεπαφής του υπολογιστή σας; Αιτιολογήστε.
4.8 Ποια τιμή του μεγέθους δεδομένων ICMP οδηγεί σε πακέτο IPv4 μέγιστου μήκους;
4.9 Για την προηγούμενη τιμή μεγέθους δεδομένων ICMP και με απαίτηση μη θρυμματισμού, επιτυγχάνει το ping προς τη διεύθυνση IPv4 του υπολογιστή σας; Εάν όχι, ποια είναι η μέγιστη τιμή για την οποία είναι επιτυχές;
4.10 Τι μέγεθος έχει το μεγαλύτερο πακέτο IPv4 που μπορεί να παράγει η εντολή ping;

Κατόπιν με τα ίδια φίλτρα σύλληψης και απεικόνισης ξεκινήστε μια καταγραφή και κάντε ping προς προορισμό εντός του τοπικού σας δικτύου στέλνοντας ένα μόνο μήνυμα ICMP με μέγεθος δεδομένων 6.000, χωρίς την απαίτηση μη θρυμματισμού του πακέτου IPv4.

4.11 Βρείτε το πρώτο μήνυμα ICMP *Echo Request* που έστειλε ο υπολογιστής σας. Έχει μεταφερθεί μήνυμα αυτό ως ένα πακέτο IPv4;
4.12 Εάν όχι, πόσα πακέτα IPv4 χρειάσθηκαν και γιατί;
4.13 Για καθένα από αυτά τα πακέτα IPv4, καταγράψτε τις τιμές των πεδίων της επικεφαλίδας που σχετίζονται με τον θρυμματισμό *(Identification, Don't Fragment Bit, More Fragments Bit, Fragment Offset)*.
4.14 Επιλέξτε το πρώτο από τα παραπάνω πακέτα IPv4 (το πρώτο θραύσμα). Ποια πληροφορία της επικεφαλίδας IPv4 δηλώνει ότι το πακέτο έχει θρυμματιστεί;
4.15 Ποια πληροφορία της επικεφαλίδας IPv4 δηλώνει ότι αυτό είναι το πρώτο θραύσμα και όχι ένα μεταγενέστερο;
4.16 Ποιο είναι το μήκος του πρώτου θραύσματος;
4.17 Επιλέξτε το δεύτερο από τα παραπάνω πακέτα IPv4 (το δεύτερο θραύσμα). Ποια πληροφορία της επικεφαλίδας IPv4 δηλώνει ότι δεν είναι το πρώτο θραύσμα;
4.18 Ακολουθούν άλλα θραύσματα;
4.19 Πώς το αναγνωρίζετε από τις πληροφορίες της επικεφαλίδας μόνο;
4.20 Ποια πεδία της επικεφαλίδας IPv4 αλλάζουν μεταξύ του πρώτου και του δεύτερου θραύσματος;
4.21 Δικαιολογήστε τις τιμές του πεδίου Fragment offset για το προτελευταίο και το τελευταίο θραύσμα που στάλθηκε.
4.22 Ποια πεδία της επικεφαλίδας IPv4 αλλάζουν μεταξύ των θραυσμάτων;

Όνοματεπώνυμο: Νίκος Μπέλλος (EL18183)	**Ομάδα:** 3
Όνομα PC/ΛΣ: BELLOS-DELL-G3 / Windows OS	**Ημερομηνία:** 08 / 11 / 2021
Διεύθυνση IP: 192 . 168 . 1 . 8	**Διεύθυνση MAC:** 7C - 2A - 31 - 40 - C9 - AF

Εργαστηριακή Άσκηση 4
Πρωτόκολλο IPv4 και θρυμματισμός

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 ping www.mit.edu -n 3 -4

1.2 Καταγράφεται μόνο η unicast κίνηση του δικτύου, δηλαδή μόνο όσα μηνύματα έχουν συγκεκριμένο παραλήπτη και αποστολέα.

1.3 0% loss, Average = 60ms

1.4 Minimum = 51ms, Maximum = 79ms, Average = 60ms

1.5 Echo 1 RTT : 0.079712 s, Echo 2 RTT : 0.052519 s, Echo 3 RTT : 0.051504 s
Ναί, συμφωνούν (minimum → echo 3, maximum → echo 1)

1.6 Display filter : ip

1.7 Display filter : icmp.type == 8 or icmp.type == 0 (8 → request, 0 → reply)

1.8 Type: 8 (Echo (ping) request)

1.9 Source Address: 192.168.1.8, Destination Address: 184.30.212.47

1.10 Type: 0 (Echo (ping) reply)

1.11 Source Address: 184.30.212.47, Destination Address: 192.168.1.8

1.12 Η IPv4 διεύθυνση του ιστότοπου www.mit.edu έχει αλλάξει από 18.7.22.83 σε 184.30.212.47

2

2.1 ping <address> -n 5 -4

2.2 Έχουν καταγραφεί μόνο 5 (αυτά που στάλθηκαν στο default gateway)

2.3 Destination : 192.168.1.1 (default gateway)

2.4 Όχι, δεν παρατήρησα,. Αυτό διότι τα πακέτα ICMP αυτά περνάνε από τον οδηγό loopback (σύμφωνα με το σχήμα) και δεν βγαίνουν ποτέ στο τοπικό δίκτυο οπότε το wireshark δεν τα εντοπίζει.

2.5 Όχι , δεν παρατήρησα. Τα ICMP μηνύματα αυτά οδηγούνται και αυτά στον οδηγό loopback, οπότε και πάλι δεν παιρνούν από την ουρά εισόδου IPv4 για να τα δει το wireshark.

2.6 Στο ping στο 192.168.1.8 το πακέτο εισέρχεται στον οδηγό Ethernet και αυτός το στέλνει στον οδηγό loopback. Ενώ, στο ping στο 127.0.0.1 το πακέτο εισέργεται κατευθείαν στον οδηγό loopback και στέλνεται πίσω στην είσοδο πακέτων IPv4.

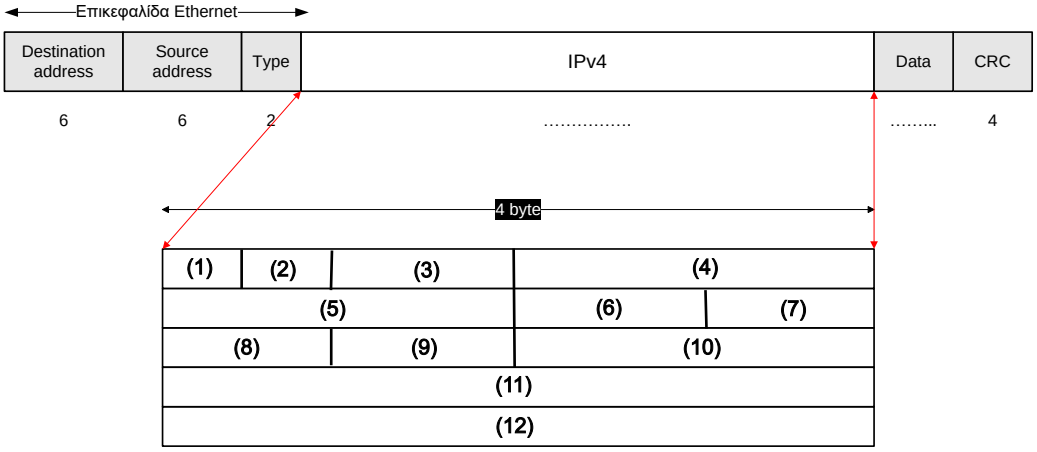
2.7 Όταν κάνω ping το www.netflix.com δεν υπάρχουν ping replies σε αντίθεση με το www.amazon.com και το πιο πιθανό είναι οτι το Netflix (ή κάποιος άλλος ενδιάμεσος) έχει ενεργοποιήσει κάποιο firewall που μπλοκάρει τα ICMP πακέτα.

3

3.1 Capture filter : host 147.102.40.15

3.2 Capture filter : host 147.102.40.15

3.3 1. Version (4 bits), 2. Header Length (4 bits), 3. Differentiated Services Field (1 byte) 4. Total Length (2 bytes), 5. Identification (2 bytes), 6. Flags (1 byte), 7. Fragment Offset (1 byte) 8. Time to Live (1 byte), 9. Protocol (1 byte), 10. Header Checksum (2 bytes), 11. Source Address (4 bytes) 12. Destination Address (4 bytes)



3.4 Αλλάζουν τα πεδία 'Total Length' και 'Identification'

3.5 Ναί, είναι (20 bytes).

3.6 Το μικρότερο είναι : 40 bytes και το μεγαλύτερο : 66 bytes

3.7 Παίρνει τις τιμές 00 (HEX) → CS0 : Standard Service class και b8 (HEX) → EF PHB : Telephony Service class

3.8 Αυξάνονται με έναν μετρητή

3.9 Έχει τιμή 1

3.10 Έχει τιμή 0

3.11 Έχει τιμή 06 (HEX) και αντιστοιχεί στο πρωτόκολλο TCP

3.12 Γιατί αναπαριστά το άθροισμα των λέξεων που περιέχονται στο IPv4 header και από τη στιγμή που υπάρχουν πεδία που αλλάζουν (πχ το identification) αλλάζει και αυτό.

4

4.1 ping <address> -n 1 -4 -f -l <size>

4.2 Η μέγιστη τιμή είναι 1472 bytes

4.3 Η ελάχιστη τιμή για θρυμματισμό είναι τα 1473 bytes

4.4 Capture filter : not multicast and not broadcast

4.5 Display filter : ip.addr == 192.168.1.2

4.6 Όχι, δεν παράγονται. Γιατί το πακέτο που πάει να μεταδοθεί ξεπερνάει το μήκος της MTU και δεν μεταδίδεται.

4.7 Το μέγεθος MTU είναι επομένως 1514 γιατί αυτό είναι το συνολικό μέγεθος του πακέτου IPv4 όπως το κατέγραψε το wireshark

4.8 Από την επικεφαλίδα ICMP και πεδίο Data προκύπτει maximum Length : 1472 bytes

4.9 Για μήκος δεδομένων 1472 και χωρίς τη παράμετρο -f επιτυχγάνεται το ping

4.10 Το μεγαλύτερο πακέτο IPv4 (επικεφαλίδες Ethernet II, IPv4, ICMP) έχει μήκος 1514 bytes

4.11 Όχι, έχει μεταφερθεί ώς πολλά

4.12 Χρειάστηκαν 5 πακέτα γιατί το κάθε ένα έχει μέγιστο μήκος ICMP 1480 bytes και επειδή ceiling(6000/1480) = 5 δημιουργούνται 5 πακέτα

4.13 (Identification, Don't Fragment Bit, More Fragments Bit, Fragment Offset) → { (cb52, 0, 1, 0), (cb52, 0, 1, 1480), (cb52, 0, 1, 2960), (cb52, 0, 1, 4440), (cb52, 0, 0, 5920) }

4.14 Το flag 'More Fragments Bit'

4.15 Το πεδίο 'Fragment Offset' το οποίο είναι 0 (δηλαδή δεν υπάρχει προηγούμενο)

4.16 Μήκος σε δεδομένα είναι 1480 bytes και μήκος πακέτου είναι 1514 bytes

4.17 Το πεδίο 'Fragment Offset' το οποίο δεν είναι 0

4.18 Ναι, ακολουθούν

4.19 Είναι ενεργοποιημένο το flag 'More fragments'

4.20 Μόνο το πεδίο 'Fragment Offset'

4.21 Για το πρωτελευταίο η τιμή είναι 4440 = 3 * 1480 δηλαδή έχουν προηγηθεί 3 θραύσματα με μήκος δεδομένων 1480. Για το τελευταίο η τιμή είναι 5920 = 4 *1480 και προκύπτει αντίστοιχα.

4.22 Τα πεδία : 'Fragment Offset', 'More fragments' και 'Total Length'