Εργαστηριακή Άσκηση 6
Πρωτόκολλο ICMP

ΟΝΟΜΑΤΕΠΩΝΥΜΟ: ΚΟΥΣΤΕΝΗΣ ΧΡΙΣΤΟΣ (03120227)

ΟΜΑΔΑ: 3

ΟΝΟΜΑ PC/ΛΣ: LAPTOP-TK5Q3T95 / WINDOWS 11

ΗΜΕΡΟΜΗΝΙΑ: 7/11/2023

ΔΙΕΥΘΥΝΣΗ IP: 147.102.201.6 (PC LAB 1.1-1.18, 5) / 192.168.1.14 (HOME NETWORK 1.19-1.23, 2, 3, 4, 6)

ΔΙΕΥΘΥΝΣΗ MAC: B4-B5-B6-79-4B-09

1 Εντολή ping στο τοπικό υποδίκτυο

Ξεκινήστε μια καταγραφή με φίλτρο σύλληψης, ώστε να καταγράφονται μόνο τα πλαίσια που περιλαμβάνουν τη διεύθυνση MAC του υπολογιστή σας. Καταγράψτε τα διερχόμενα πλαίσια όταν κάνετε ping σε μια διεύθυνση IPv4 υπολογιστή εντός του τοπικού δικτύου, π.χ. την προκαθορισμένη πύλη. Αφού τελειώσει η καταγραφή, εφαρμόστε ένα φίλτρο απεικόνισης, ώστε να παραμείνουν μόνο πλαίσια σχετιζόμενα με τα πρωτόκολλα ARP και ICMP.

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

```
Capture filter : ether host  B4-B5-B6-79-4B-0A
```

1.2 Καταγράψτε τη σύνταξη του φίλτρου απεικόνισης ώστε να παραμείνουν μόνο πλαίσια σχετιζόμενα με τα πρωτόκολλα ARP και ICMP.

```
Display filter : arp or icmp
```

1.3 Εάν καταγράφηκαν, εξηγήστε τον σκοπό των πακέτων πρωτοκόλλου ARP που ανταλλάχθηκαν.

Αφού κάναμε ping στην IPv4 διεύθυνση ενός άλλου υπολογιστή συνδεδεμένου στο δίκτυου του PC Lab παρατηρήσαμε τα ακόλουθα ARP πακέτα στην καταγραφή μας.

30	1.958938	b4:b5:b6:79:4b:09	0c:e4:41:e1:6c:74	ARP	Who has 147.102.203.111? Tell 147.102.201.6
31	0.075939	0c:e4:41:e1:6c:74	b4:b5:b6:79:4b:09	ARP	147.102.203.111 is at 0c:e4:41:e1:6c:74

Ο σκοπός της ανταλλαγής των πακέτων αυτών είναι η συμπλήρωση του ARP table του υπολογιστή μας με την MAC address της συσκευής στην οποία κάναμε ping.

1.4 Βρείτε το πρώτο μήνυμα Echo request του πρωτοκόλλου ICMP. Ποιο είναι το όνομα και η τιμή του πεδίου της επικεφαλίδας IPv4 που προσδιορίζει ότι πρόκειται για μήνυμα ICMP;
Protocol: ICMP (1)

Η δομή της επικεφαλίδας των μηνυμάτων ICMP εξαρτάται από το είδος τους. Τα πεδία στην πρώτη λέξη 32 bit είναι ταυτόσημα για όλα τα είδη. Μετά, ανάλογα το είδος ακολουθούν λέξεις 32 bit είτε το 0x00000000 (unused) ώστε το ελάχιστο μήκος μηνύματος ICMP να είναι 8 byte.

1.5 Ποιο είναι το μήκος της επικεφαλίδας των μηνυμάτων ICMP Echo request;
Header Length : 8 bytes

1.6 Καταγράψτε τα ονόματα και το μήκος σε byte των πεδίων της επικεφαλίδας του μηνύματος ICMP Echo request και σημειώστε στο σχήμα τις θέσεις τους.

Type | 1 byte

Code | 1 byte

Checksum | 2 bytes

Identifier (BE) + Identifier (LE) | 2 bytes total

Sequence Number (BE) + Sequence Number (LE) | 2 bytes total

1.7 Καταγράψτε την τιμή των πεδίων τύπου (Type) και κωδικού (Code) της επικεφαλίδας των μηνυμάτων ICMP Echo request.
Type: 8 (Echo (ping) request)

Code: 0

1.8 Καταγράψτε τις τιμές των πεδίων ταυτότητας (Identifier) και του αύξοντα αριθμού (Sequence number) της επικεφαλίδας ενός μηνύματος ICMP Echo request.

- Identifier (BE): 1 (0x0001)
- Identifier (LE): 256 (0x0100)

- Sequence Number (BE): 605 (0x025d)
- Sequence Number (LE): 23810 (0x5d02)

1.9 Ποιο είναι το μήκος και ποιο το περιεχόμενο του πεδίου δεδομένων των μηνυμάτων ICMP Echo request που παράγει η εντολή ping;
Data Length : 32 bytes

Data Content : abcdefghijklmnopqrstuvwabcdefghi

Δηλαδή οι λατινικοί χαρακτήρες a-w και a-i.

1.10 Βρείτε ένα μήνυμα Echo reply του πρωτοκόλλου ICMP. Ποιο είναι το μήκος της επικεφαλίδας μηνυμάτων ICMP Echo reply; Έχει την ίδια δομή με αυτή του Echo request;
Header Length : 8 bytes

Ναι, έχει την ίδια δομή.

1.11 Καταγράψτε την τιμή των πεδίων τύπου (Type) και κωδικού (Code) της επικεφαλίδας ICMP των μηνυμάτων Echo reply.

Type: 0 (Echo (ping) reply)

Code: 0

1.12 Με βάση τις απαντήσεις σας στις ερωτήσεις 0 και 1.11, ποιο από τα πεδία Type και Code καθορίζει το είδους του μηνύματος ICMP;

Το πεδίο Type καθορίζει το είδος του μηνύματος.

1.13 Καταγράψτε τις τιμές των πεδίων ταυτότητας (Identifier) και αύξοντα αριθμού (Sequence number) της επικεφαλίδας ICMP ενός μηνύματος Echo reply.

- Identifier (BE): 1 (0x0001)
- Identifier (LE): 256 (0x0100)

- Sequence Number (BE): 605 (0x025d)
- Sequence Number (LE): 23810 (0x5d02)

1.14 Εντοπίστε το μήνυμα ICMP Echo request σε απάντηση του οποίου παράχθηκε το προηγούμενο μήνυμα ICMP Echo reply. Ποιες είναι οι αντίστοιχες τιμές των πεδίων ταυτότητας και αύξοντα αριθμού. [Υπόδειξη: Στο παράθυρο με τις λεπτομέρειες κάντε κλικ στη γραμμή Response Frame και θα μεταφερθείτε στο σωστό πλαίσιο.]

Οι τιμές που έχουν request και reply στα πεδία Identifier και Sequence Number ταυτίζονται.

1.15 Ποιος νομίζετε ότι είναι ο ρόλος των πεδίων ταυτότητας και αύξοντα αριθμού στην επικεφαλίδα των μηνυμάτων ICMP Echo request και Echo reply; [Υπόδειξη: Συμβουλευθείτε την ιστοσελίδα http://www.networksorcery.com/enp/default0604.htm στο Internet Archive επιλέγοντας το “IP protocol suite” από το αριστερό της μέρος και στη συνέχεια το πρωτόκολλο ICMP στο δεξιό της μέρος. Διαβάστε τις λεπτομέρειες που αφορούν τα μηνύματα ICMP Echo request]

Χρησιμοποιούνται για να αντιστοιχίσουν echo request με echo reply.

Όπως στο Internet Archive:

“The identifier and sequence number may be used by the echo sender to aid in matching the replies

with the echo requests. For example, the identifier might be used like a port in TCP or UDP to

identify a session, and the sequence number might be incremented on each echo request sent. The

echoing node returns these same values in the echo reply.”

1.16 Ποιο είναι το μήκος και ποιο το περιεχόμενο του πεδίου δεδομένων των μηνυμάτων ICMP Echo reply;

Data Length : 32 bytes

Data Content : abcdefghijklmnopqrstuvwabcdefghi

Δηλαδή οι λατινικοί χαρακτήρες a-w και a-i.

1.17 Διαφέρει αυτό το περιεχόμενο από το αντίστοιχο του μηνύματος ICMP Echo request;
Όχι, δε διαφέρει είναι ίδιο.

1.18 Πώς σχετίζονται οι ανταλλαγές των μηνυμάτων ICMP με τα αποτελέσματα της εντολής ping στο παράθυρο εντολών;
Στο cmd εμφανίζονται οι τιμές TTL, ο χρόνος που κάνει κάθε reply να επιστρέψει στον υπολογιστή μας μετρώντας από τη χρονική στιγμή που στέλνουμε το request σε ms καθώς και το μέγεθος κάθε reply ICMP μηνύματος σε bytes.

Ξεκινήστε πάλι τη διαδικασία καταγραφής των πακέτων με το ίδιο φίλτρο σύλληψης και εκτελέστε την εντολή ping προς μια διεύθυνση IPv4 που δεν αντιστοιχεί σε ενεργό υπολογιστή του τοπικού σας δικτύου ζητώντας να παραχθούν δύο μηνύματα ICMP Echo request. Αφού τελειώσει η καταγραφή, εφαρμόστε ένα φίλτρο απεικόνισης, ώστε να παραμείνουν μόνο πλαίσια σχετιζόμενα με τα πρωτόκολλα ARP και ICMP.

1.19 Ποια σύνταξη της εντολής ping χρησιμοποιήσατε ώστε να παραχθούν δύο μηνύματα ICMP;
ping -n 2 <ip.address>

1.20 Πόσα πακέτα ARP request στάλθηκαν για την ανεύρεση της διεύθυνσης MAC του μη ενεργού υπολογιστή;
4 arp requests

1.21 Κάθε πότε στέλνονται; [Υπόδειξη: Από το μενού View μπορείτε να επιλέξετε Time Display Format-> Seconds Since Previous Displayed Packet.]
Το πρώτο και το δεύτερο με απόσταση 1 δευτερολέπτου περίπου τα υπόλοιπα σε πολύ πιο κοντινα χρονικά διαστήματα.

43	0.000000	b4:b5:b6:79:4b:09	ff:ff:ff:ff:ff:ff	ARP	Who has 192.168.1.201? Tell 192.168.1.14
50	0.992959	b4:b5:b6:79:4b:09	ff:ff:ff:ff:ff:ff	ARP	Who has 192.168.1.201? Tell 192.168.1.14
56	1.000520	b4:b5:b6:79:4b:09	ff:ff:ff:ff:ff:ff	ARP	Who has 192.168.1.201? Tell 192.168.1.14
57	1.004070	b4:b5:b6:79:4b:09	ff:ff:ff:ff:ff:ff	ARP	Who has 192.168.1.201? Tell 192.168.1.14

1.22 Πόσα μηνύματα ICMP στάλθηκαν;
Κανένα.

1.23 Πώς σχετίζονται τα προηγούμενα με τα αποτελέσματα της εντολής ping στο παράθυρο εντολών;
Στο terminal για κάθε ping request εμφανίζεται, Destination Host Unreachable κάτι που είναι λογικό επειδή δεν απαντώνται τα ARP request και η εντολή ping δεν έχει προορισμό διαθέσιμο να στείλει τα icmp πακέτα της.

2 Εντολή ping σε άλλο υποδίκτυο

Προτού ξεκινήσετε την άσκηση, αδειάστε τον πίνακα arp του υπολογιστή σας (προς τούτο στα μηχανήματα του PC Lab εκτελέστε την εντολή arpclear). Στη συνέχεια, χρησιμοποιώντας το φίλτρο σύλληψης των προηγούμενων ερωτήσεων, καταγράψτε τα διερχόμενα πλαίσια όταν κάνετε ping σε έναν υπολογιστή εκτός του τοπικού δικτύου σε μία από τις ακόλουθες IPv4 διευθύνσεις 147.102.1.1, 147.102.7.1 ή 147.102.40.1. Αφού τελειώσει η καταγραφή εφαρμόστε φίλτρο απεικόνισης, ώστε να παραμείνουν μόνο πλαίσια σχετιζόμενα με τα πρωτόκολλα ARP και ICMP.

2.1 Καταγράψτε τις διευθύνσεις IPv4 που περιέχει ο πίνακας arp μετά την παραπάνω καταγραφή.

```
C:\Windows\System32>arp -a


Interface: 192.168.1.14 --- 0x10
  Internet Address      Physical Address      Type
  192.168.1.1           58-76-ac-4a-62-a0     dynamic
  192.168.1.103         30-de-4b-46-c1-93     dynamic
  192.168.1.119         00-12-15-51-9c-06     dynamic
  192.168.1.190         5c-c5-63-3e-5d-ff     dynamic
  192.168.1.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

2.2 Επιλέξτε ένα μήνυμα ICMP Echo request. Καταγράψτε τη διεύθυνση MAC του αποστολέα και του παραλήπτη του αντίστοιχου πλαισίου.

Source: b4:b5:b6:79:4b:09

Destination: 58:76:ac:4a:62:a0

2.3 Καταγράψτε τις διευθύνσεις IPv4 (αποστολέα και παραλήπτη) του πακέτου IPv4 που μεταφέρει το μήνυμα ICMP Echo request;

Source : 192.168.1.14

Destination : 147.102.1.1

2.4 Οι παραπάνω διευθύνσεις MAC σε ποιες διευθύνσεις IPv4 αντιστοιχούν;

b4:b5:b6:79:4b:09 --> 192.168.1.14

58:76:ac:4a:62:a0 --> 192.168.1.1(router-default gateway)

2.5 Παρατηρήσατε πακέτα πρωτοκόλλου ARP κατά την καταγραφή;
Όχι.

2.6 Αν ναι, ποιος ήταν ο σκοπός τους; Εάν όχι, αιτιολογήστε γιατί δεν υπήρξαν.
Γιατί η διεύθυνση 147.102.1.1 βρίσκεται εκτός τοπικού δικτύου οπότε τα ARP request θα τα στείλει κάποιος ενδιάμεσος δρομολογητής αν χρειαστεί και ο ARP table του υπολογιστή μας δε θα περιλαμβάνει την αντιστοίχιση της 147.102.1.1 σε κάποιο MAC address.

Αφού απενεργοποιήσετε το προηγούμενο φίλτρο απεικόνισης, εφαρμόστε ένα νέο φίλτρο απεικόνισης, ώστε να παραμείνουν μόνο μηνύματα ICMP Echo reply.

2.7 Να καταγραφεί η σύνταξη του. [Υπόδειξη: Συμβουλευτείτε τις απαντήσεις σας στις ερωτήσεις 1.11 και 1.12]
icmp.type == 0

2.8 Παρατηρώντας τις τιμές των πεδίων της επικεφαλίδας των πακέτων IPv4 που μεταφέρουν το μήνυμα ICMP Echo reply, εξηγήστε πώς προκύπτει η τιμή της παραμέτρου TTL που εμφανίζεται στις απαντήσεις του παραθύρου εντολών.
Προκύπτει από το πεδίο Time to Live της επικεφαλίδας IPv4 που έχει τιμή 57.

Ξεκινήστε μια νέα καταγραφή με το προηγούμενο φίλτρο σύλληψης, όταν εκτελείτε την εντολή ping σε έναν υπολογιστή εκτός του υποδικτύου σας, που δεν είναι ενεργός (π.χ. κάποιον από τους 147.102.7.85 έως 89). Όταν τελειώσει η καταγραφή εφαρμόστε ένα φίλτρο απεικόνισης, ώστε να παραμείνουν μόνο πλαίσια σχετιζόμενα με το πρωτόκολλο ICMP.

2.9 Ποιοι τύποι μηνυμάτων ICMP εμφανίζονται;
Εμφανίζονται μόνο ICMP requests.

2.10 Σε τι διαφέρει η κίνηση που καταγράψατε σε σχέση με την αντίστοιχη όταν εκτελέσατε την προηγουμένως ping προς μια διεύθυνση IPv4 εντός του υποδικτύου σας, που δεν αντιστοιχεί σε ενεργό υπολογιστή. Αιτιολογήστε τη διαφορά.
Δεν έχουμε ICMP replies αφού δεν βρίσκουν destination τα ping requests που στέλνουμε και δεν έχουμε ούτε arp requests ενώ στον ερώτημα 1.23 είχαμε παρατηρήσει arp requests. Αυτό οφείλεται στο γεγονός ότι αυτή τη φορά κάνουμε ping σε μη ενεργό υπολογιστή, γι’αυτό εξάλλου σε καμία περίπτωση δεν έχουμε icmp replies, ο υπολογιστής όμως στο 1.23 ανήκε στο υποδίκτυο μας και άρα έγιναν αιτήματα προσθήκης των ip και mac διευθύνσεων του στο arp table της συσκευής μας. Αντιθέτως, στην περίπτωση του δεύτερου μέρους η ανενεργή διεύθυνση ip ανήκε σε ξένο υποδίκτυο άρα απλά στείλαμε icmp requests ελπίζοντας για κάποια απάντηση…

3 Εντολή tracert/traceroute

Στην Εργαστηριακή Άσκηση 5 είδατε πώς μπορείτε να βρείτε τη διαδρομή που ακολουθεί ένα πακέτο στο διαδίκτυο με την εντολή tracert ή traceroute. Εδώ θα εξετάσετε με περισσότερη λεπτομέρεια τα ICMP μηνύματα λαθών. Ιστορικά, τα ICMP μηνύματα λάθους επέστρεφαν την επικεφαλίδα IPv4 του πακέτου που τα προκάλεσε μαζί με τα πρώτα 8 byte δεδομένων του. Αργότερα θεσπίστηκαν νέοι κανόνες ώστε να περιλαμβάνεται το περισσότερο δυνατό από το αρχικό πακέτο, χωρίς το μήκος του πακέτου ICMP να ξεπερνά τα 576 byte (το επίσημο μήκος πακέτου στο Internet). Τέλος, στο RFC 4884 προστέθηκε ένα πεδίο 8 bit που δείχνει το μήκος του αρχικού πακέτου σε λέξεις των 32 bit.

Ξεκινήστε μια νέα καταγραφή της δικτυακής κίνησης με φίλτρο σύλληψης ώστε να συλλαμβάνετε μόνο πακέτα IPv4 που περιέχουν την IPv4 διεύθυνση του υπολογιστή σας. Σε παράθυρο εντολών εκτελέστε την εντολή tracert ή traceroute χωρίς επίλυση ονομάτων με προορισμό το μηχάνημα με IPv4 διεύθυνση 147.102.40.15. Στην περίπτωση της traceroute χρησιμοποιήστε στην κατάλληλη σύνταξη ώστε να παραχθούν μηνύματα ICMP Echo request. Όταν τελειώσει η εκτέλεση της εντολής σταματήστε την καταγραφή και εφαρμόστε φίλτρο απεικόνισης, ώστε να παραμείνουν μόνο πλαίσια σχετιζόμενα με το πρωτόκολλο ICMP.

3.1 Ποιο είναι το μήκος και το περιεχόμενο του πεδίου δεδομένων των μηνυμάτων ICMP Echo request που παράγει η εντολή tracert ή traceroute;

Το μήκος του πεδίου δεδομένων Data των ICMP Echo requests που παράγει η εντολή tracert είναι 64 bytes και αποτελείται μόνο από μηδενικά.(64 φορές “00_{16}”)

3.2 Συγκρίνετε το παραπάνω μήκος και περιεχόμενο του πεδίου δεδομένων με τα αντίστοιχα στην περίπτωση της εντολής ping (Ερώτηση 1.9);

Παρατηρούμε πως σε σχέση με τα ICMP μηνύματα του ping, διαφέρουν και ως προς το μήκος των δεδομένων (64 bytes αντί 32 bytes) αλλά και ως προς το περιεχόμενο (0000… αντί για abcd….) (βλ. 1.9)

3.3 Ποιο ICMP μήνυμα λάθους παρατηρείτε στις απαντήσεις των ενδιάμεσων κόμβων (πριν τον 147.102.40.15);

Το μήνυμα λάθους : “Time-to-live exceeded (Time to live exceeded in transit)”

3.4 Ποια είναι η τιμή των πεδίων τύπου (Type) και κωδικού (Code) της επικεφαλίδας ICMP για το προηγούμενο μήνυμα λάθους;

Type: 11 (Time-to-live exceeded)

Code: 0 (Time to live exceeded in transit)

3.5 Ποια άλλα πεδία έχει η επικεφαλίδα του μηνύματος λάθους πριν τα δεδομένα και ποιο το μέγεθός τους;

Πριν τα δεδομένα, η επικεφαλίδα του μηνύματος λάθους για πακέτα μέχρι τον δρομολογητή έχει επιπλέον τα πεδία:

- Checksum (2 bytes)
- Unused (4 bytes).

και για πακέτα μετά τον δρομολογητή τα πεδία:

- Checksum (2 bytes)
- Length (1 byte)
- Unused (1+2 bytes)

3.6 Ποιο είναι το μήκος της επικεφαλίδας και ποιο των δεδομένων του ICMP μηνύματος λάθους της ερώτησης 3.3;

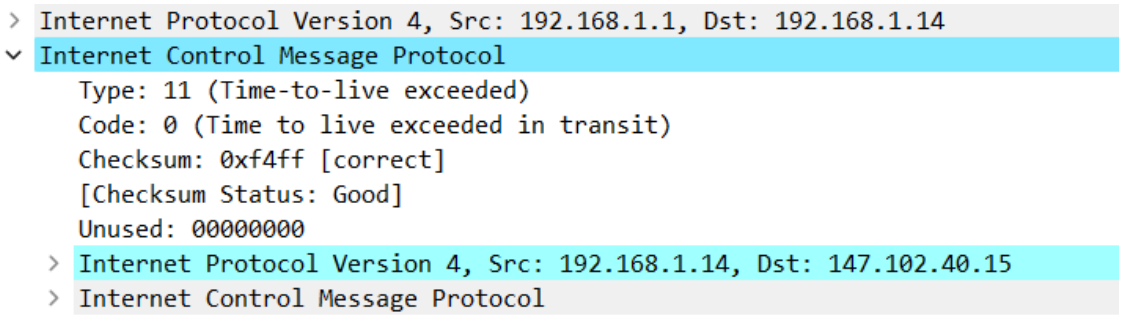
Header Length : 8 bytes

Data Length : 100-8 = 92 bytes

3.7 Τι είναι το περιεχόμενο του πεδίου δεδομένων του προηγούμενου ICMP μηνύματος λάθους και ποια η σχέση του με το πακέτο IPv4 εξ αιτίας του οποίου παράχθηκε;

[Υπόδειξη: Συμβουλευθείτε την παράγραφο 4.2 του RFC 4884.]

Τα δεδομένα του ICMP μηνύματος λάθους που εξετάσαμε είναι ουσιαστικά το IPv4 πακέτο που προκάλεσε το εν λόγω μήνυμα (IPv4 Header + τα πρώτα byte του αρχικού μηνύματος, μέχρι το ICMP πακέτο να φτάσει μέγιστο τα 576 bytes) με την προσθήκη του ICMP header του σφάλματος και της δικίας του IPv4 επικεφαλίδας.



4 Ανακάλυψη MTU διαδρομής(Path MTU Discovery)

Η διαδικασία ανακάλυψης MTU διαδρομής, που ορίζεται στο RFC 1191, έχει σκοπό την αποφυγή του αχρείαστου θρυμματισμού κατά την επικοινωνία δύο κόμβων, ειδικά στην περίπτωση συνδέσεων TCP, όπου υφίσταται ένας παρόμοιος του θρυμματισμού μηχανισμός, γνωστός ως τεμαχισμός (segmentation). Προς τούτο αποστέλλονται πακέτα IPv4 με ενεργοποιημένη τη σημαία μη θρυμματισμού (Don't fragment flag), όπως κάνατε στην Εργαστηριακή Άσκηση 4. Αν κάποιος υπολογιστής ή δρομολογητής δεν μπορεί να προωθήσει χωρίς θρυμματισμό ένα τέτοιο πακέτο IPv4, οφείλει να στείλει στην πηγή ένα ICMP μήνυμα λάθους τύπου Destination Unreachable, υποπερίπτωση Fragmentation needed, δηλώνοντας την τιμή της MTU της απερχόμενης ζεύξης. Ο έλεγχος αυτός γίνεται εύκολα γιατί κάθε πρωτόκολλο στρώματος ζεύξης δεδομένων έχει ένα συγκεκριμένο μέγεθος μέγιστου πλαισίου, π.χ. 1.518 byte για το Ethernet. Έτσι δεν υπάρχει λόγος να γίνει διεξοδικό ψάξιμο, αρκεί να αναζητηθούν τα συνήθη μεγέθη MTU, όπως 1500, 1492, 1006, 576, 552, 544, 512, 508 και 296. Με τον τρόπο αυτό οι υπολογιστές και οι δρομολογητές μπορούν να εντοπίσουν την PMTU (Path MTU), δηλαδή, τη μέγιστη MTU για την οποία δεν εμφανίζεται θρυμματισμός (ισοδύναμα τη ζεύξη με τη μικρότερη MTU κατά μήκος της διαδρομής). Η PMTU που βρέθηκε ισχύει για κάποιο μικρό διάστημα γιατί οι διαδρομές στο διαδίκτυο αλλάζουν συχνά. Εάν στο μέλλον μικρύνει, αυτό θα γίνει αντιληπτό αμέσως, δεν ισχύει όμως το ίδιο εάν μεγαλώσει, οπότε η διαδικασία θα πρέπει να επαναληφθεί. Για να αποφευχθούν άσκοπες επαναλήψεις, αυτό γίνεται μόνο αφού λήξει η χρονική διάρκεια της ήδη ευρεθείσας PMTU, τυπικά 10 min. Θα βρείτε τώρα την MTU της διαδρομής από τον υπολογιστή σας προς τον edu-dy.cn.ntua.gr. Προς τούτο ξεκινήστε μια νέα καταγραφή με φίλτρο σύλληψης ώστε να συλλαμβάνετε μόνο μηνύματα ICMP και μετά εκτελέστε διαδοχικά την εντολή ping στέλνοντας χωρίς θρυμματισμό ένα μόνο πακέτο για τιμές μεγέθους δεδομένων ICMP σύμφωνες με τις συνήθεις τιμές MTU που δίδονται πιο πάνω, ξεκινώντας από τη μεγαλύτερη προς τη μικρότερη. Σταματήστε τα ping και την καταγραφή όταν λάβετε επιτυχή απάντηση από το 147.102.40.15.

4.1. Ποιες τιμές μήκους δεδομένων ICMP χρησιμοποιήσατε για να παράγετε πακέτα IPv4 με μήκος τις επιθυμητές τιμές MTU;

Ισχύει:

MTU = IPv4 header length (20) + ICMP header length (8) + ICMP Payload Length

=> ICMP Payload length = MTU – 28 bytes

Άρα χρησιμοποιήθηκαν οι ακόλουθες τιμές:

1500-28 = 1472 bytes (no reply)

1492-28 = 1464 bytes (no reply)

1006-28 = 978 bytes (no reply)

576-28 = 548 bytes (reply received)

Μέσω της εντολής: ***ping -4 -f -l <size> -n 1 edu-dy.cn.ntua.gr***

4.2. Παρατηρήσατε μήνυμα λάθους ICMP Destination Unreachable; Εάν ναι, ποιος κόμβος της διαδρομής το παρήγαγε;

Ναι, ο κόμβος με διεύθυνση 192.168.1.1

4.3. Εάν το παρατηρήσατε, ποια είναι η τιμή των πεδίων Type και Code της επικεφαλίδας του ICMP Destination Unreachable; Εάν όχι, χρησιμοποιήστε για αυτή και τις επόμενες δύο ερωτήσεις την καταγραφή στο αρχείο mtu.pcap που θα βρείτε στην ιστοσελίδα του μαθήματος.

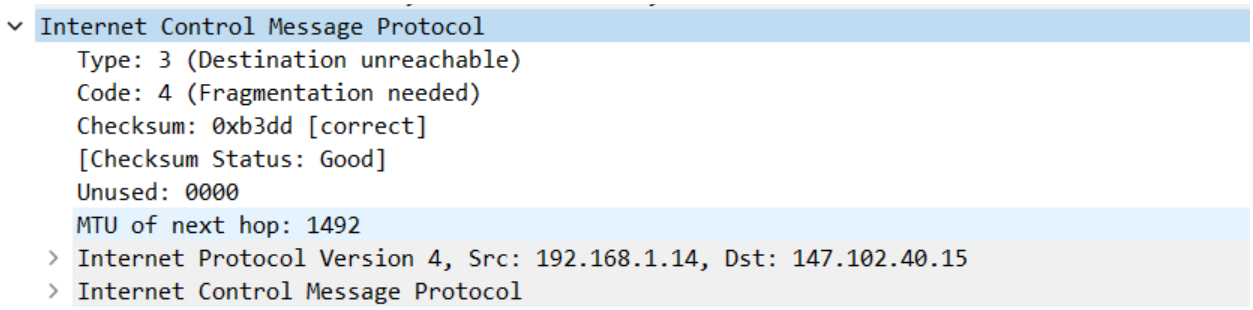
- Type: 3 (Destination unreachable)
- Code: 4 (Fragmentation needed)

4.4. Ποιο πεδίο δηλώνει ότι το λάθος οφείλεται στην απαίτηση μη θρυμματισμού του πακέτου IPv4 και ποια τιμή έχει η επικεφαλίδα Next-Hop MTU;

Το πεδίο Code με τιμή 4 που αντιστοιχεί στο σφάλμα : Fragmentation Needed

MTU of next hop: 1492

4.5. Ποιο μέρος από το πακέτο που προκάλεσε το μήνυμα λάθους περιέχει το πεδίο των δεδομένων;



Το IPv4 και το ICMP header του πακέτου που προκάλεσε το λάθος εμπεριέχεται στο πεδίο δεδομένων του μηνύματος λάθους όπως φαίνεται στην παραπάνω εικόνα καθώς επίσης και τα πρώτα 520 bytes από data.

4.6. Ποια είναι η MTU για την οποία δεν λαμβάνετε για πρώτη φορά μήνυμα λάθους ICMP Destination Unreachable, άσχετα από το εάν απαντά ή όχι το 147.102.40.15;

Για MTU 1492 bytes.

4.7. Για ποιες άλλες τιμές MTU δεν απαντά το 147.102.40.15;

1492 και 1006.

4.8. Ποια είναι η τιμή MTU για την οποία λαμβάνετε απάντηση από το 147.102.40.15;

576 bytes.

4.9. Είναι αυτή η MTU της δικτυακής διεπαφής του 147.102.40.15 ή κάποιου άλλου ενδιάμεσου κόμβου; Γιατί; [Υπόδειξη: Δείτε παράγραφο 4 στο RFC 1191.]

Είναι η MTU της δικτυακής διεπαφής 147.102.40.15, γιατί στην αμέσως επόμενη μεγαλύτερη τιμή της MTU δεν είχε υπάρξει σφάλμα host unreachable σε ενδιάμεσο κόμβο.

4.10. Παραμένει η απαίτηση μη θρυμματισμού του πακέτου IPv4 στην απάντηση του 147.102.40.15;

Ναι, παραμένει.

4.11. Για ποιο λόγο νομίζετε ότι το 147.102.40.15 δεν παράγει ICMP Destination Unreachable όταν λαμβάνει πακέτα IPv4 μεγέθους μεγαλύτερου από την MTU της διεπαφής του;

Επειδή είναι ο τελικός κόμβος και δε χρείαζεται να θρυμματίσει το πακέτο για περαιτέρω προώθηση.

Ξεκινήστε μια νέα καταγραφή και κάντε ping στο 147.102.40.15 στέλνοντας ένα μόνο πακέτο ICMP μεγέθους αντίστοιχου της MTU της ερώτησης 4.6 χωρίς την απαίτηση μη θρυμματισμού. Προσοχή, σε περιβάλλον Linux πρέπει να δηλωθεί ρητά.

4.12. Καταγράψτε το μέγεθος του πρώτου θραύσματος που λαμβάνει ο υπολογιστής σας. Είναι το ίδιο με την MTU που προσδιορίσατε προηγουμένως; Γιατί; [Υπόδειξη: Αναζητείστε Fragment Offset στην ιστοσελίδα https://en.wikipedia.org/wiki/IPv4.]

Το μέγεθος data του πρώτου θραύσματος που λαμβάνει ο υπολογιστής μου είναι 552 bytes και προκύπτει ως εξής σύμφωνα με την πηγή της υπόδειξης:

(1492-20)/8 = 184

184*3 = 552

When a router receives a packet, it examines the destination address and determines the outgoing interface to use and that interface's MTU. If the packet size is bigger than the MTU, and the Do not Fragment (DF) bit in the packet's header is set to 0, then the router may fragment the packet.The router divides the packet into fragments. The maximum size of each fragment is the outgoing MTU minus the IP header size (20 bytes minimum; 60 bytes maximum). The router puts each fragment into its own packet, each fragment packet having the following changes:

- ✓ The total length field is the fragment size.
- ✓ The more fragments (MF) flag is set for all fragments except the last one, which is set to 0.
- ✓ The fragment offset field is set, based on the offset of the fragment in the original data payload. This is measured in units of 8-byte blocks.
- ✓ The header checksum field is recomputed.

For example, for an MTU of 1,500 bytes and a header size of 20 bytes, the fragment offsets would be multiples of (1,500 – 20)/8 = 185

5 Απρόσιτη θύρα (Port Unreachable)

Ένα άλλο συνηθισμένο ICMP μήνυμα λάθους είναι το ICMP Destination Unreachable, αυτό της απρόσιτης θύρας. Τυπικά παράγεται όταν ένα πρόγραμμα πελάτης προσπαθεί να επικοινωνήσει με κάποιον εξυπηρετητή, αλλά δεν υπάρχει διεργασία που να ακούει στη συγκεκριμένη θύρα, π.χ. στη θύρα 80 για εξυπηρετητές ιστού ή στη θύρα 53 για εξυπηρετητές DNS. Ξεκινήστε μια καταγραφή με φίλτρο ώστε να συλλαμβάνετε μόνο πακέτα IPv4 από και προς το μηχάνημα με IPv4 διεύθυνση 147.102.40.15. Στη συνέχεια τρέξτε το πρόγραμμα nslookup σε περιβάλλον Windows, dig σε περιβάλλον Linux ή host σε περιβάλλον Unix, για να ζητήσετε από τον εξυπηρετητή DNS 147.102.40.15 τη διεύθυνση IPv4 του edu-dy.cn.ntua.gr.

5.1 Ποιο φίλτρο σύλληψης χρησιμοποιήσατε;

Capture filter : ***ip and host 147.102.40.15***

5.2 Ποια η ακριβής σύνταξη της εντολής nslookup, dig ή host που χρησιμοποιήσατε;

nslookup edu-dy.cn.ntua.gr 147.102.40.15

5.3 Λάβατε κάποια απάντηση στο παράθυρο εντολών; Ποιο το νόημά της;

```
C:\Windows\System32>nslookup edu-dy.cn.ntua.gr 147.102.40.15
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  147.102.40.15

DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
*** Request to UnKnown timed-out
```

Παραπάνω φαίνεται το αποτέλεσμα εκτέλεσης της εντολή του 5.2 ερωτήματος στο cmd. Ο λόγος που το DNS request γίνεται timed out είναι ότι δεν υπάρχει διεργασία που να ακούει στη συγκεκριμένη θύρα (53) του εξυπηρετητή DNS.

5.4 Παρατηρήσατε μηνύματα DNS στην καταγραφή;

Ναι παρατήρηθηκαν μηνύματα DNS.

No.	Time	Source	Destination	Protocol	Info
1	0.000000	147.102.200.102	147.102.40.15	DNS	Standard query 0x0001 PTR 15.40.102.147.in-addr.arpa
2	0.002285	147.102.40.15	147.102.200.102	ICMP	Destination unreachable (Port unreachable)
3	2.003225	147.102.200.102	147.102.40.15	DNS	Standard query 0x0002 A edu-dy.cn.ntua.gr
4	0.002787	147.102.40.15	147.102.200.102	ICMP	Destination unreachable (Port unreachable)
5	2.010981	147.102.200.102	147.102.40.15	DNS	Standard query 0x0003 AAAA edu-dy.cn.ntua.gr
6	0.002265	147.102.40.15	147.102.200.102	ICMP	Destination unreachable (Port unreachable)
7	2.012037	147.102.200.102	147.102.40.15	DNS	Standard query 0x0004 A edu-dy.cn.ntua.gr
8	0.002260	147.102.40.15	147.102.200.102	ICMP	Destination unreachable (Port unreachable)
9	1.999856	147.102.200.102	147.102.40.15	DNS	Standard query 0x0005 AAAA edu-dy.cn.ntua.gr
10	0.002666	147.102.40.15	147.102.200.102	ICMP	Destination unreachable (Port unreachable)

5.5 Ποιο είναι το πρωτόκολλο μεταφοράς και ποια είναι η θύρα προορισμού τους;
Transport Protocol : UDP και Destination Port: 53

5.6 Παρατηρήσατε μηνύματα λάθους ICMP Destination Unreachable με πηγή το 147.102.40.15;
Ναι παρατηρήθηκαν(βλ. εικόνα στο 5.4)

5.7 Καταγράψτε την τιμή των πεδίων Type και Code της επικεφαλίδας των.
Type: 3 (Destination unreachable)

Code: 3 (Port unreachable)

5.8 Ποιο πεδίο δηλώνει ότι ο λόγος αποτυχίας είναι κάποια απρόσιτη θύρα;
Το Code με τιμή 3.

5.9 Πώς προκύπτει ότι πρόκειται για τη θύρα προορισμού των μηνυμάτων DNS;
Το port 53 είναι προκαθαρισμένη θύρα προορισμού(destination port) για DNS queries

Στα συστήματα Unix/Linux η εντολή traceroute παράγει εξ ορισμού μηνύματα UDP, με θύρες προορισμού στην περιοχή από 33434 έως 33534, αντί μηνυμάτων ICMP.

5.10 Όταν αυτά φτάνουν στον προορισμό τους με ποιο μήνυμα ICMP απαντά αυτός;

Με μήνυμα ***icmp destination unreachable***

6 IPv6 και ICMPv6

Στη χρήση των εντολών ping και tracert/traceroute που κάνατε μέχρι τώρα δόθηκε προσοχή να παράγετε πακέτα IPv4 και να παρατηρείτε ICMP μηνύματα ερωτημάτων ή λαθών. Στα τρέχοντα όμως λειτουργικά συστήματα υποστηρίζεται και η έκδοση 6 του πρωτοκόλλου IP, γνωστή ως IPv6. Στο IPv6 η βασική αλλαγή είναι ότι η επικεφαλίδα του πακέτου IP έχει πλέον σταθερό μήκος και απλούστερη δομή. Ταυτόχρονα το μήκος των αντίστοιχων διευθύνσεων μεγάλωσε από 4 byte σε 16 byte ώστε να αντιμετωπιστεί το πρόβλημα έλλειψης διευθύνσεων IPv4. Παράλληλα, όμως άλλαξε ο τρόπος λειτουργίας του ICMP. Το ICMPv6, το αντίστοιχο με το ICMP πρωτόκολλο, προσφέρει ανάλογες λειτουργίες και αντικαθιστά το ARP όσον αφορά το θέμα της ανεύρεσης γειτόνων. Στο μέρος αυτό της άσκησης θα δείτε τις λεπτομέρειες της επικεφαλίδας του IPv6 και των μηνυμάτων ICMPv6 που παράγονται από τις εντολές ping και tracert/traceroute. Για τη συνέχεια, εάν ο υπολογιστής σας ή το δίκτυο που χρησιμοποιείτε δεν υποστηρίζει το πρωτόκολλο IPv6, θα χρησιμοποιήσετε την καταγραφή στο αρχείο icmpv6.pcap που θα βρείτε στην ιστοσελίδα του μαθήματος.

Ξεκινήστε μια νέα καταγραφή με φίλτρο ώστε να συλλαμβάνετε μόνο πακέτα IPv6. Στη συνέχεια κάντε ping προς το μηχάνημα με IPv6 διεύθυνση 2001:648:2000:329::101 και μετά tracert ή traceroute στην ίδια διεύθυνση. Στην περίπτωση της traceroute σιγουρευτείτε ότι χρησιμοποιήσατε την κατάλληλη παράμετρο ώστε να παραχθούν πακέτα ICMPv6, αντί UDP. Περιμένετε να ολοκληρωθεί η εκτέλεση των εντολών, σταματήστε την καταγραφή και εφαρμόστε φίλτρο ώστε να παρατηρείτε μόνο μηνύματα ICMPv6.

6.1 Ποια είναι η σύνταξη των ping, tracert ή traceroute που χρησιμοποιήσατε;

ping -n 1 2001:648:2000:329::101

tracert 2001:648:2000:329::101

6.2 Ποια είναι η σύνταξη του φίλτρου σύλληψης που χρησιμοποιήσατε και ποια του φίλτρου απεικόνισης;

`Capture filter : ip6`

`Display filter : icmpv6`

6.3 Τι τιμή έχει το πεδίο Type της επικεφαλίδας Ethernet όταν μεταφέρονται πακέτα IPv6;

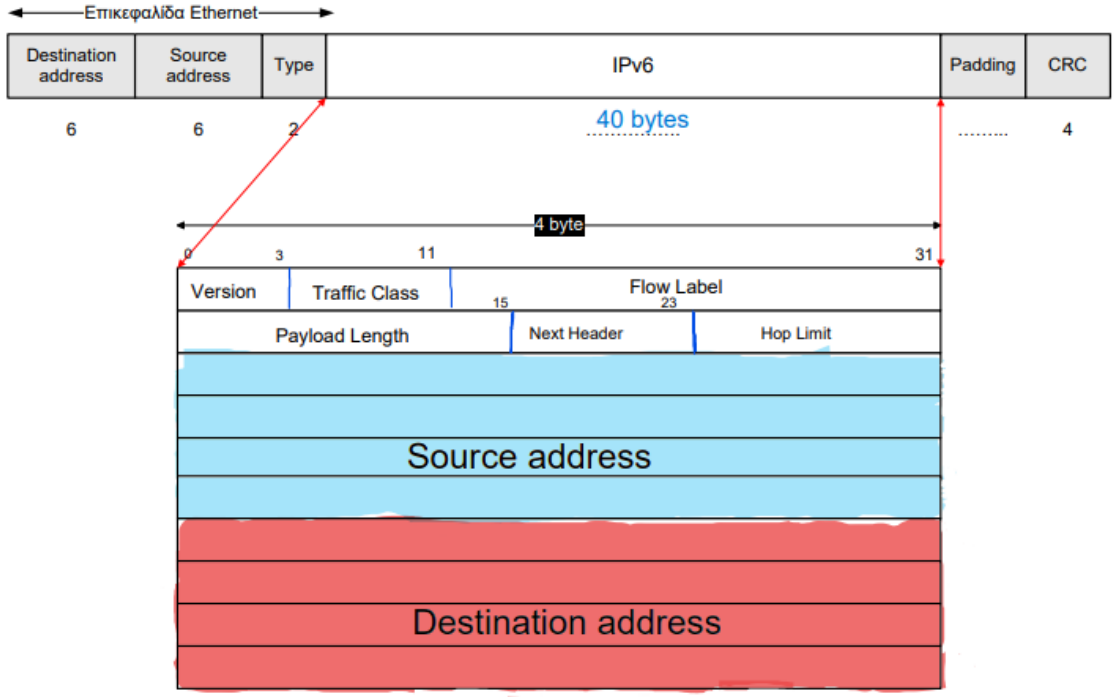
`Type: 86dd`$_{16}$ `(IPv6)`

6.4 Ποιο είναι το μήκος επικεφαλίδας των πακέτων IPv6;

`40 bytes`

6.5 Καταγράψτε τα ονόματα και το μήκος σε byte των πεδίων της επικεφαλίδας του μηνύματος IPv6 και σημειώστε στο σχήμα τις θέσεις τους.

- Version | 4 bits = 0.5 bytes
- Traffic Class | 1 byte = 8 bits
- Flow Label | 20 bits = 2.5 bytes
- Payload Length | 2 bytes
- Next Header | 1 byte
- Hop Limit | 1 byte
- Source Address | 16 bytes
- Destination Address | 16 bytes



6.6 Ποια επικεφαλίδα είναι η αντίστοιχη της TTL των πακέτων IPv4;
To Hop Limit

6.7 Ποια επικεφαλίδα δείχνει το πρωτόκολλο τα δεδομένα του οποίου μεταφέρει το πακέτο IPv6 και ποια η τιμή της για το ICMPv6;
Next Header: ICMPv6 (58)

6.8 Εντοπίστε ένα μήνυμα ICMPv6 Echo request που να έχει παραχθεί από την εντολή ping. Είναι η δομή της επικεφαλίδας του ίδια με αυτήν που βρήκατε προηγουμένως για το ICMP Echo request στην ερώτηση 1.6;
Ναι, έχουν ίδια δομή.

6.9 Ποια η τιμή του πεδίου Type και ποιο το μήκος δεδομένων που μεταφέρει το ICMPv6 Echo request;
Type: Echo (ping) request (128) ---> 80_{16}

Data size : 32 bytes

6.10 Εντοπίστε το μήνυμα ICMPv6 Echo reply που παράχθηκε σε απάντηση του προηγούμενου ICMPv6 Echo request. Είναι η δομή της επικεφαλίδας του ίδια με αυτήν του ICMP Echo request;
Ναι, είναι ίδια.

6.11 Ποια η τιμή του πεδίου Type και ποιο το μήκος δεδομένων που μεταφέρει το ICMPv6 Echo reply;
Type: Echo (ping) reply (129) ---> 81_{16}

Data size : 32 bytes

6.12 Εντοπίστε ένα μήνυμα ICMPv6 Echo request που να έχει παραχθεί από την εντολή tracert ή traceroute. Σε τι διαφέρει από το αντίστοιχο που παράγει η εντολή ping;
Το Data size είναι διπλάσιο και ίσο με 64 bytes. Επίσης, τα requests της tracert ξεκινάνε από hop limit : 1 το οποίο διαδοχικά αυξάνεται ανά τρία αποτυχημένα requests.

6.13 Εντοπίστε ένα μήνυμα λάθους ICMPv6 Time exceeded. Είναι η δομή της επικεφαλίδας του ίδια με αυτήν που βρήκατε προηγουμένως για το ICMP Time exceeded στις ερωτήσεις 3.4 και 3.5;
Όχι, έχει και το πεδίο Reserved ενώ απουσιάζει το πεδίο Unused.

6.14 Ποια η τιμή του πεδίου Type και ποιο το μήκος δεδομένων που μεταφέρει το ICMPv6 Time exceeded;
Type: Time Exceeded (3) ---> 03_{16}

Data length : 64 bytes

6.15 Τι περιέχει το πεδίο δεδομένων του;
Περιέχει μηδενικά. Σε μεγαλύτερη ανάλυση, εμπεριέχει το πακέτο ping request το οποίο απέτυχε και προκάλεσε το σφάλμα με την προσθήκη της ICMPv6 επικεφαλίδας σφάλματος.

6.16 Παρατηρήσατε άλλα ICMPv6 μηνύματα; Εάν ναι, τι είδους είναι;
Ναι παρατήρηρησα τα εξής επιπλέον είδη μηυνμάτων :

- Neighbor Advertisement
- Neighbor Solicitation
- Router Advertisement

6.17 Ποια η τιμή του πεδίου Type και ποιο το μήκος αυτών των μηνυμάτων ICMPv6;

- Neighbor Advertisement
  - Type : 136 --> 88_{16}
  - Length : 86 bytes
- Neighbor Solicitation
  - Type : 135 --> 87_{16}
  - Length :
- Router Advertisement
  - Type : 134 --> 86_{16}
  - Length : 182 bytes