ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΣΙΤΩΝ
ΡΟΗ Δ - ΔΙΚΤΥΑ ΥΠΟΛΟΓΙΣΤΩΝ (COMPUTER NETWORKS)

ΓΕΩΡΓΑΚΟΠΟΥΛΟΣ ΓΕΩΡΓΙΟΣ 03120827

# ΑΝΑΦΟΡΑ 6ΗΣ ΕΡΓΑΣΤΗΡΙΑΚΗΣ ΑΣΚΗΣΗΣ

**Ομάδα:** 2
**Λογισμικο:** Linux Ubuntu 20.04
**Ονομα PC:** glaptop
**Διεύθυνση IP:** 147.102.239.235
**Διεύθυνση MAC:** 70:9c:d1:03:b0:15

## ΑΣΚΗΣΗ 1: Εντολή ping στο τοπικό υποδίκτυο

**1.1** Το φίλτρο σύλληψης που χρησιμοποίησα είναι:
ether host 70:9c:d1:03:b0:15

**1.2** Το φίλτρο απεικόνισης είναι: arp or icmp

**1.3** Τα πακέτα arp που καταγράφηκαν έχουν ως σκοπό την συμπλήρωση του arp table. Όλα αυτά τα μηνύματα έχουν την MAC μου ως Destination. Επίσης είναι όλα replies (Opcode = 2).

**1.4** Το πεδίο που προσδιορίζει ότι πρόκειται για ICMP είναι το πεδίο protocol και έχει τιμή 1

**1.5** Το μήκος της επικεφαλίδας των μηνυμάτων ICMP echo request είναι 8 bytes

**1.6** Τα πεδία της επικεφαλίδας ενός τέτοιου μηνύματος είναι:
Type: 1 byte
Code: 1byte
Checksum: 2bytes
Identifier: 2bytes
Sequence Number: 2bytes

**1.7** Για το ICMP echo request είναι: Type = 8 (0x08) και Code = 0 (0x00)

**1.8** Για το ICMP echo request είναι: Identifier = 0x0001 και Sequence Number = 0x0002

**1.9** Το μήκος των ICMP echo request είναι 48 bytes (για Ubuntu Linux) και το περιεχόμενο είναι:
9b a6 09 00 00 00 00 00 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 .. 37

**1.10** Το μήκος της επικεφαλίδας των μηνυμάτων ICMP echo reply είναι 8 bytes. Επίσης έχει την ίδια δομή με τα μηνύματα ICMP echo request.

**1.11** Για το ICMP echo request είναι: Type = 0 (0x00) και Code = 0 (0x00)

**1.12** Το είδος του μηνύματος ICMP καθορίζεται από το πεδίο Type

**1.13** Για ένα μήνυμα ICMP echo reply είναι: Identifier = 0x0002 και Sequence Number = 0x0003

**1.14** Οι αντίστοιχες τιμές των πεδίων ταυτότητας του μηνύματος ICMP echo request σε απάντηση του οποίου παράχθηκε το προηγούμενο μήνυμα ICMP echo reply είναι: Identifier = 0x0002 και
Sequence Number = 0x0003

**1.15** Τα πεδία αυτά χρησιμοποιούνται για να αντιστοιχίζονται τα ICMP echo requests με τα ICMP echo replies.

**1.16** Το μήκος των  είναι 48 bytes (για Ubuntu Linux) και το περιεχόμενο είναι d8 5a 0d 00 00 00 00 00 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 .. 37

**1.17** Ναι διαφέρει, αλλά μόνο στα πρώτα 3 bytes

**1.18** Η εντολή ping παρουσιάζει δεδομένα όπως ο χρόνος απάντησης, τα οποία τα παίρνει από τα μηνύματα που έρχονται

**1.19** Η εντολή που χρησιμοποίησα είναι: ping –c 2 –4 147.102.236.252

**1.20** Στάλθηκαν 3 τέτοια πακέτα

**1.21** Αυτά στέλνονται κάθε περίπου 1 δευτερόλεπτο

**1.22** Δεν στάλθηκε κανένα πακέτο ICMP

**1.23** Εφόσον ο υπολογιστής αυτός δεν είναι ενεργός είναι  λογικό να μην υπάρχει arp reply και άρα να μην μπορεί να σταλθεί ICMP echo request. Ετσι η εντολή ping δεν βγάζει κανένα αποτέλεσμα (στα ubuntu linux)

**ΑΣΚΗΣΗ 2: Εντολή ping σε άλλο υποδίκτυο**

**2.1** Ο πίνακας μετά την καταγραφή έχει και πάλι τις ίδιες διευθύνσεις. Ουσιαστικά αφαιρέσαμε την MAC της προκαθωρισμένης πύλης και έπειτα ξαναμπήκε.

**2.2** Για ένα μήνυμα ICMP echo request ισχύει ότι: Source = 70:9c:d1:03:b0:15 και Destination = 08:ec:f5:d0:d9:1d

**2.3** Για το ίδιο μήνυμα: Source Address: 147.102.239.235 και Destination Address: 147.102.1.1

**2.4** Η MAC του αποστολέα (δηλαδή η δικιά μου) αντιστοιχεί στην 147.102.239.235 αι η MAC του προορισμού αντιστοιχεί στην 147.102.1.1

**2.5** Ναι, παρατήρησα πακέτα ARP

**2.6** Ο σκοπός αυτών των πακετων, είναι να ξαναβάλλουν στον ARP πίνακα την MAC της προκαθωρισμένης θύρας, εφόσον πριν την καταγραφή τον είχα καθαρίσει.

**2.7** Το φίλτρο που χρησιμοποίησα είναι: icmp.type==0

**2.8** Σε όλα τα μηνύματα ICMP echo reply, η τιμή του πεδίου Time to Live είναι 63. Αυτό συμβαίνει καθώς το μήνυμα ξεκινάει από τον server με 64 και παρεμβάλεται 1 κομβος.

**2.9** Εμφανίζονται μόνο μηνύματα ICMP echo request

**2.10** Και στις 2 περιπτώσεις ο υπολογιστής με τον οποίο επικοινωνούμε δεν είναι ενεργός. Στην προηγούμενη περίπτωση στέλνουμε arp μηνύματα για να μάθουμε την MAC διευθυνση του αλλά δεν υπαρχει απάντηση και άρα δεν στέλνουμε και ICMP echo requests. Σε αυτή την περίπτωση (διαφορετικό υποδίκτυο)  δεν στένουμε ARP καθώς επικοινωνούμε μέσω

της προκαθωρισμένης πύλης για την οποία έχουμε την MAC διευθυνση και άρα στέλνουμε μόνο ICMP echo requests. Ωστόσο δεν παίρνουμε απάντηση.

**ΑΣΚΗΣΗ 3: Εντολή tracert/traceroute**

**3.1** Το μήκος των ICMP echo request είναι 24 bytes (για Ubuntu Linux) και το περιεχόμενο είναι:
08090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f

**3.2** Σε σύγκριση με την ping, το μήκος δεδομένων είναι το μισό, αλλά το περιεχόμενο έχει την ίδια μορφή (σειρά αριθμων)

**3.3** Το ICMP μήνυμα λαθους που παρατηρούμε στους ενδιάμεσους κόμβους είναι το Time-to-Live Exceeded

**3.4** Για το προηγούμενο μήνυμα ισχυει: Type = 11 και Code = 0

**3.5** Στην επικεφαλίδα υπάρχουν επίσης (πριν τα δεδομένα) τα πεδία:
Checksum (2 bytes)
Unused (1 byte)
Length (1 byte)

**3.6** Για το μήνυμα λάθους ισχύει ότι:
Μήκος Επικεφαλίδας: 8 bytes
Μήκος Δεδομένων: 20 + 32 = 52 bytes
Επίσης υπάρχουν έξτρα 16 bytes μηδενικών στο τέλος
Επομένως σύνολο 68 bytes

**3.7** Το περιεχόμενο του πεδίου δεδομένων του ICMP μηνύματος λάθους είναι αντιγραφή του πακέτου IPv4 και του ICMP μηνύματος του ICMP echo request του οποίου αποτελεί απάντηση

**ΑΣΚΗΣΗ 4: Ανακάλυψη MTU διαδρομής**

**4.1** Οι τιμές μήκους δεδομένων ICMP που χρησιμοποίησα είναι:
1472, 1464, 978, 548. Οι τιμές αυτές προκύπτουν από τις τιμές της εκφώνησης αφαιρώντας 28 bytes λογω των επικεφαλίδων

**4.2** Όχι, στην δικιά μου καταγραφή δεν παρατήρησα μήνυμα λαθους ICMP Destination Unreachable

**4.3** Χρησιμοποιώντας την καταγραφή mtu.pcap, για το μήνυμα λάθους ισχύει ότι:
Type = 3 (Destination Unreachable) και
Code = 4 (Fragmentation needed)

**4.4** Το πεδίο που δηλώνει ότι το λάθος οφείλεται στην απαίτηση μη θρυμματισμού είναι το Code. Η επικεφαλίδα MTU of next hop έχει τιμή 1492.

**4.5** Το πεδίο δεδομένων περιέχει την επικεφαλίδα IPv4 και ICMP του αρχικού μηνύματος ICMP echo request.

**4.6** Χρησιμοποιώντας πάλι την δικια μου καταγραφή, η πρώτη MTU για την οποία δεν λαμβάνω μήνυμα λαθους είναι 1500.

**4.7** Ο 147.102.40.15 δεν απαντά για τις τιμές 1500, 1492, 978
**4.8** Η πρώτη τιμή για την οποία λαμβάνω απάντηση είναι η 576
**4.9** Αυτή η τιμή είναι είναι η MTU της δικτυακής διεπαφής του 147.102.40.15 καθώς αν ήταν κάποιου ενδιάμεσου κόμβου θα έπρεπε να παίρναμε καποιο μήνυμα destination unreachable (σύμφωνα με το RFC 1191)
**4.10** Ναι, η απαίτηση μη θρυμματισμου παραμένει στην απάντηση του 147.102.40.15 (το βλεπουμε από τα flags)
**4.11** Το 147.102.40.15 δεν παράγει ICMP Destination Unreachable όταν λαμβάνει πακέτα IPv4 μεγέθους μεγαλύτερου από την MTU της διεπαφής το, καθώς η διεπαφή του έχει μικρότερο MTU από τους ενδιάμεσους κόμβους (από άκρη σε άκρη σε μια επικοινωνία γίνεται μια "συμφωνια" για το MTU) και όντως ο τελικός προορισμός δεν χρειάζεται να θρυμματίσει το πακετο.
**4.12** Το μέγεθος του 1ου θραύσματος είναι 572 bytes. Είναι δηλαδή κατά 4 bytes μικρότερο από την MTU που καταγράψαμε προηγουμένως. Αυτό συμβαίνει διότι το μήκος δεδομένων ενός θραυσματος είναι πολλαπλάσιο του 8 (552 bytes δεδομένα και όχι 556)

**ΑΣΚΗΣΗ 5: Απρόσιτη Θύρα**
**5.1** Το φίλτρο σύλληψης που χρησιμοποίησα είναι: host 147.102.40.15
**5.2** Χρησιμοποίησα την εντολή: host 147.102.40.15 edu-dy.cn.ntua.gr
**5.3** Η απάντηση που έλαβα είναι: communications error / connecion refused / no servers could be reached.Αυτο σημαίνει ότι το μήνυμα δεν έφτασε ποτέ στον προορισμό του.
**5.4** Ναι καταγράφηκαν μηνύματα DNS
**5.5** Το πρωτόκολλο μεταφοράς τους είναι UDP και η θύρα προορισμού η 53
**5.6** Ναι παρατήρησα μηνύματα λάθους ICMP Destinaion Unreachable με πηγ το 147.102.40.15
**5.7** Για τα μηνύματα αυτά ισχύει ότι:
Type: 3 (Destination unreachable)
Code: 3 (Port unreachable)
**5.8** Το πεδίο που δηλώνει ότι ο λόγος αποτυχίας είναι κάποια απρόσιτη θύρα είναι το πεδίο code.
**5.9** Τα μηνύματα DNS έχουν πάντα θύρα προορισμού την 53 (πασιγνωστη θυρα)
**5.10** Και πάλι, χρησιμοποιώντας μηνύματα UDP κατά την traceroute, η απάντηση που παίρνουμε είναι ICMP Destination Unreachable ή ICMP Time to Live Exceeded

**ΑΚΣΗΣΗ 6: IPv6 και ICMPv6**
*Για την άσκηση 6 θα χρησιμοποιηθεί η καταγραφή icmpv6.pcap !!*

**6.1** Η σύνταξη των εντολών είναι: ping –6 <addr> / traceroute –I <addr>
**6.2** Το φίλτρο σύλληψης είναι: ip6. Το φίλτρο απεικόνισης είναι: icmpv6
**6.3** Το πεδίο type της επικεφαλίδας ethernet έχει τιμή: 0x86dd

**6.4** Το μήκος της επικεφαλίδας των πακέτων IPv6 είναι 40 bytes

**6.5** Πεδία επικεφαλίδας Ethernet:

Version
Traffic Class
Flow Label

*Αυτά τα 3 είναι μικτά στα πρώτα 4 bytes. Η σειρα που εμφανίζονται είναι από αριστερά προς τα δεξιά.*

Payload Length (2 bytes)
Next Header (1 byte)
Hop Limit (1 byte)
Source Address (16 bytes)
Destination Address (16 bytes)

**6.6** Το Hop Limit είναι αντίστοιχο με το TTL στο IPv4

**6.7** Η επικεφαλίδα που δείχνει το πρωτόκολλο τα δεδομένα του οποίου μεταφέρει το πακέτο IPv6 είναι η Next Header. Για το ICMPv6 η τιμή της είναι 58 (0x3a)

**6.8** Ναι , η δομή της επικεφαλίδας ειναι ίδια με αυτή στην ερώτηση 1.6

**6.9** Η τιμή του πεδίου type είναι 128 (0x80). Το μήκος δεδομένων που μεταφέρει το ICMPv6 Echo Requests είναι 32 bytes

**6.10** Ναι, η δομή της επικεφαλίδας του μηνύματος ICMP echo reply είναι ίδια με αυτή του μηνύματος ICMP echo request

**6.11** Η τιμή του πεδίου type είναι 129 (0x81). Το μήκος των δεδομένων είναι 32 bytes

**6.12** Διαφέρει στο μήκος δεδομένων (τώρα είναι 64 bytes)

**6.13** Η μόνη διαφορά είναι ότι στο ICMPv6 Time Exceeded έχει προστεθεί το πεδίο Reserved

**6.14** Η τιμή του πεδιου type είναι 3 (0x03). Το μήκος δεδομένων είναι 64 bytes

**6.15** Το πεδίο δεδομένων περιέχει μόνο μηδενικά

**6.16** Στην καταγραφή επίσης παρατηρούνται μηνύματα Neighbor Solicitation και Neighbor Advertisement

**6.17** Neighbor Advertisement: Type = 136 (0x88) / Length = 86 bytes
Neighbor Solicitation: Type = 135 (0x87) / Length = 86 bytes