Ονοματεπώνυμο: Αλεξάνδρα Μωραϊτάκη	**Όνομα PC:**
Ομάδα: 1	**Ημερομηνία: 25/02/2025**

Εργαστηριακή Άσκηση 2
Δικτύωση συστημάτων στο VirtualBox

ΑΣΚΗΣΗ 1 Δημιουργία εικονικού μηχανήματος FreeBSD

ΑΣΚΗΣΗ 2 Ανάλυση δικτυακών πρωτοκόλλων με το TCPDUMP

Δημιουργία vm FreeBSD: PC1

ΕΡΩΤΗΣΗ 2.1

Εμφάνιση καρτών δικτύου

```
ifconfig
```

- em0
- lo0 (loopback)

ΕΡΩΤΗΣΗ 2.2

Απενεργοποίηση και ενεργοποίηση κάρτας em0

```
ifconfig em0 down
ifconfig em0 up
```

ΕΡΩΤΗΣΗ 2.3

Πληροφορίες

```
man tcpdump
man pcap
man pcap-filter
```

tcpdump

ΕΡΩΤΗΣΗ 2.4

Σύλληψη όλων των πλαισίων από την em0 χωρίς επίλυση διευθύνσεων IP (χωρίς να μετατρέπει τις IP σε ονόματα host -> -n)

```
tcpdump -i em0 -n
```

ΕΡΩΤΗΣΗ 2.5

Σύλληψη όλων των πλαισίων από την em0 μαζί με περιεχόμενα σε ASCII και hex

```
tcpdump -i em0 -X
```

`-X` → Εμφανίζει το περιεχόμενο των πακέτων σε ASCII και δεκαεξαδική μορφή.

ΕΡΩΤΗΣΗ 2.6

Σύλληψη όλων των πλαισίων από την em0 μαζί με MAC source,destination addresses

```
tcpdump -i em0 -e
```

`-e` → Εμφανίζει τις MAC διευθύνσεις στο Ethernet πλαίσιο.

ΕΡΩΤΗΣΗ 2.7

Σύλληψη των πρώτων 68 byte όλων των πλαισίων από την em0

```
tcpdump -i em0 -s 68
```

`-s 68` → Καταγραφή μόνο των πρώτων 68 byte κάθε πακέτου.

ΕΡΩΤΗΣΗ 2.8

Σύλληψη όλων των πακέτων IPv4 με 10.0.0.1 μαζί με λεπτομέρειες των επικεφαλίδων τους

```
tcpdump -i em0 -n host 10.0.0.1 -vv
```

`-vv` → Εμφάνιση λεπτομερειών για τις επικεφαλίδες.

ΕΡΩΤΗΣΗ 2.9

Σύλληψη πακέτων επικοινωνίας 2 vm με διευθύνσεις 10.0.0.1 και 10.0.0.2 από την em0

```
tcpdump -i em0 -n host 10.0.0.1 and host 10.0.0.2
```

ΕΡΩΤΗΣΗ 2.10

Σύλληψη πακέτων IPv4 για το δίκτυο 1.1.0.0/16 και περιεχόμενο τους

```
tcpdump -i em0 -n net 1.1.0.0/16 -X
```

`net 1.1.0.0/16` → Φιλτράρει όλα τα πακέτα που ανήκουν στο συγκεκριμένο υποδίκτυο.

ΕΡΩΤΗΣΗ 2.11

Σύλληψη πακέτων IPv4 που δεν ανήκουν στο τοπικό δίκτυο (πχ 192.168.1.0/24) και περιεχόμενο τους μαζί με επικεφαλίδες Ethernet

```
tcpdump -i em0 -n not net 192.168.1.0/24 -e
```

`not net 192.168.1.0/24` → Φιλτράρει μόνο την εξωτερική κίνηση (όχι τοπική).

ΕΡΩΤΗΣΗ 2.12

Σύλληψη πακέτων IPv4 εκπομπής ή πολλαπλής διανομής

```
tcpdump -i em0 -n broadcast or multicast
```

ΕΡΩΤΗΣΗ 2.13

Σύλληψη πακέτων IPv4 μήκους μεγαλύτερου των 576 byte

```
tcpdump -i em0 -n greater 576
```

ΕΡΩΤΗΣΗ 2.14

Σύλληψη πακέτων IPv4 με τιμές TTL μικρότερες του 5

```
tcpdump -i em0 -n 'ip[8] < 5'
```

Το πεδίο TTL (Time To Live) βρίσκεται στο 9ο byte (ξεκινώντας από 0, δηλαδή στο offset 8).

ΕΡΩΤΗΣΗ 2.15

Σύλληψη πακέτων IPv4 με προαιρετικές επικεφαλίδες

```
tcpdump -i em0 -n 'ip[0] & 0x0F > 5'
```

Το πρώτο byte της επικεφαλίδας IPv4 περιέχει δύο τιμές:

- Τα πρώτα 4 bits είναι η έκδοση του πρωτοκόλλου (π.χ. IPv4=4).
- Τα τελευταία 4 bits είναι το μήκος της επικεφαλίδας σε 32-bit λέξεις.

Χρησιμοποιούμε ip[0] & 0x0F για να απομονώσουμε αυτά τα 4 τελευταία bits.
Αν το μήκος της επικεφαλίδας είναι μεγαλύτερο από 5 (δηλαδή πάνω από 20 bytes, αφού 5 × 4 = 20), σημαίνει ότι το πακέτο περιέχει προαιρετικές επικεφαλίδες

ΕΡΩΤΗΣΗ 2.16

Σύλληψη πακέτων ICMP με αποστολέα την IP 10.0.0.1

```
tcpdump -i em0 -n 'icmp and src host 10.0.0.1'
```

ΕΡΩΤΗΣΗ 2.17

Σύλληψη τεμαχίων TCP με παραλήπτη την IP 10.0.0.2

```
tcpdump -i em0 -n 'tcp and dst host 10.0.0.2'
```

ΕΡΩΤΗΣΗ 2.18

Σύλληψη datagrams UDP με θύρα προορισμού 53 (DNS)

```
tcpdump -i em0 -n 'udp and port 53'
```

ΕΡΩΤΗΣΗ 2.19

Σύλληψη τεμαχίων TCP με διεύθυνση αποστολέα ή παραλήπτη 10.0.0.10

```
tcpdump -i em0 -n ‘tcp and host 10.0.0.10’
```

ΕΡΩΤΗΣΗ 2.20

Σύλληψη τεμαχίων TCP με διεύθυνση αποστολέα ή παραλήπτη 10.0.0.10 με θύρα 23 και αποθήκευση αποτελεσμάτων στο αρχείο “sample_capture”

```
tcpdump -i em0 -n ‘tcp and host 10.0.0.10 and port 23’ -w sample_capture
```

ΕΡΩΤΗΣΗ 2.21

Σύλληψη τεμαχίων TCP μόνο με σημαία SYN

```
tcpdump -i em0 -n 'tcp[tcpflags] & tcp-syn != 0'
```

Το πεδίο TCP flags βρίσκεται στο 13ο byte της TCP επικεφαλίδας (`tcp[13]`).
Η σημαία SYN είναι το δεύτερο bit (τιμή `0x02`).
`tcp[13] & 0x02 != 0` → Φιλτράρει πακέτα όπου το SYN είναι ενεργοποιημένο.

ΕΡΩΤΗΣΗ 2.22

Σύλληψη πρώτων δύο τεμαχίων της τριμερούς χειραψίας TCP

```
tcpdump -i em0 -n ‘tcp[tcpflags] & (tcp-syn|tcp-ack) != 0’
```

Το πεδίο TCP flags βρίσκεται στο 13ο byte της TCP επικεφαλίδας (`tcp[13]`).
Η σημαία SYN είναι το δεύτερο bit (τιμή `0x02`).
`tcp[13] & 0x02 != 0` → Φιλτράρει πακέτα όπου το SYN είναι ενεργοποιημένο.

ΕΡΩΤΗΣΗ 2.23

Σύλληψη τεμαχίων TCP σχετικά με την απόλυση μιας σύνδεσης

```
tcpdump -i em0 -n ‘tcp[tcpflags] & (tcp-fin|tcp-rst) != 0’
```

`FIN` → `0x01`, `RST` → `0x04`
Φιλτράρει πακέτα που περιέχουν FIN ή RST, που σηματοδοτούν το κλείσιμο μιας σύνδεσης.

ΕΡΩΤΗΣΗ 2.24

Φίλτρο σύλληψης τεμαχίων TCP: ((tcp[12:1] & 0xf0) >> 2)

Αυτή η παράσταση εξάγει το μέγεθος της επικεφαλίδας TCP, επειδή:

- tcp[12:1] → Αναφέρεται στο 12ο byte της TCP επικεφαλίδας, το οποίο περιέχει το offset της επικεφαλίδας.
- & 0xf0 → Απομονώνει τα 4 υψηλότερα bits, που αποθηκεύουν το μήκος της επικεφαλίδας.
- >> 2 → Μετατρέπει το μήκος της επικεφαλίδας από λέξεις των 4 byte σε bytes.

ΕΡΩΤΗΣΗ 2.25

Σύλληψη τεμαχίων TCP με προαιρετικές επικεφαλίδες(options)

```
tcpdump -i em0 -n 'tcp[12:1] & 0xf0 > 0x50'
```

Αν το μήκος της TCP επικεφαλίδας είναι πάνω από 20 bytes (0x50 σε hex), σημαίνει ότι το πακέτο περιέχει TCP Options.

ΕΡΩΤΗΣΗ 2.26

Σύλληψη μηνυμάτων HTTP και περιεχόμενο τους ως ASCII

```
tcpdump -i em0 -n -A 'tcp port 80'
```

-A → Εκτυπώνει το περιεχόμενο σε **ASCII**

ΕΡΩΤΗΣΗ 2.27

Σύλληψη μηνυμάτων telnet προς το edu-dy.cn.ntua.gr

```
tcpdump -i em0 -n 'host edu-dy.cn.ntua.gr and port 23'
```

ΕΡΩΤΗΣΗ 2.28

Σύλληψη πακέτων IPv6

```
tcpdump -i em0 -n ip6
```

ΑΣΚΗΣΗ 3 Δικτύωση Host-only

ΕΡΩΤΗΣΗ 3.1

Host-only Ethernet adapter IPv4: 192.168.56.1

ΕΡΩΤΗΣΗ 3.2

DHCP IPv4: 192.168.56.100
Lower address bound: 192.168.56.101
Upper address bound: 192.168.56.254

ΕΡΩΤΗΣΗ 3.3

```
dhclient em0
```

στα PC1, PC2

ΕΡΩΤΗΣΗ 3.4

PC1 IPv4: 192.168.56.103
PC2 IPv4: 192.168.56.102

ΕΡΩΤΗΣΗ 3.5

PC1: `ping 192.168.56.103`
PC2: `ping 192.168.56.102`
Αφού επιτυγχάνουν και τα 2, τα vm επικοινωνούν μεταξύ τους.

ΕΡΩΤΗΣΗ 3.6

cmd (host):

```
ping 192.168.56.102
ping 192.168.56.103
```

Αφού επιτυγχάνουν και τα 2, τα vm επικοινωνούν με τον host.

ΕΡΩΤΗΣΗ 3.7

Εμφάνιση προεπιλεγμένης πύλης

```
netstat -r
```

ΕΡΩΤΗΣΗ 3.8

Όχι, δεν υπάρχει προεπιλεγμένη πύλη στο Host-Only δίκτυο.

- Το Host-Only network είναι απομονωμένο από το υπόλοιπο δίκτυο.
- Δεν συνδέεται ούτε στο Internet ούτε σε άλλους δρομολογητές.
- Δεν υπάρχει router που να λειτουργεί ως gateway.

ΕΡΩΤΗΣΗ 3.9

cmd:

```
ping 192.168.56.1
```

Ναι γίνεται ping στην IPv4 της φυσικής κάρτας δικτύου του φιλοξενούντος μηχανήματος (host).

ΕΡΩΤΗΣΗ 3.10

```
hostname
```

PC1: PC.ntua.lab
PC2: PC.ntua.lab

ΕΡΩΤΗΣΗ 3.11

```
hostname PC1
hostname PC2
```

ΕΡΩΤΗΣΗ 3.12

prompt lab@PC1:
prompt lab@PC2:

ΕΡΩΤΗΣΗ 3.13

```
cat /etc/rc.conf | grep hostname
```

Εμφανίζεται hostname=PC.ntua.lab στα PC1, PC2.

ΕΡΩΤΗΣΗ 3.14

Μόνιμη αλλαγή ονομάτων

```
vi /etc/rc.conf
```

Αλλαγή σε PC1/PC2

ΕΡΩΤΗΣΗ 3.15

Συμπληρώνουμε στα PC1, PC2 στο /etc/hosts:

```
192.168.56.101  PC1
192.168.56.102  PC2
```

ΕΡΩΤΗΣΗ 3.16

Επιβεβαίωση λειτουργίας με παράδειγμα εντολής:

```
ping -c 4 PC2
```

ΕΡΩΤΗΣΗ 3.17

Ping στο ίδιο το PC1 (localhost):

```
ping -c 4 127.0.0.1
```

64 bytes & TTL: 64
Ping στο PC2:

```
ping -c 4 192.168.56.102
```

64 bytes & TTL: 64
Ping στη διεύθυνση του Host-Only Adapter του host

```
ping -c 4 192.168.56.1
```

64 bytes & TTL: 128
Ping στη διεύθυνση του DHCP Server

```
ping -c 4 192.168.56.100
```

64 bytes & TTL: 255

ΕΡΩΤΗΣΗ 3.18

Σύλληψη πακέτων με τη διεύθυνση IPv4 του PC1 χωρίς επίλυση διευθύνσεων IPv4 σε ονόματα:

```
tcpdump -i em0 -n src host 192.168.56.101 -vv
```

ΕΡΩΤΗΣΗ 3.19

Ping στο PC2:

```
ping -c 4 192.168.56.102
```

84 bytes & TTL=64

ΕΡΩΤΗΣΗ 3.20

Σύλληψη μηνυμάτων ICMP με πολλές λεπτομέρειες:

```
tcpdump -i em0 -n icmp -vvv
```

ΕΡΩΤΗΣΗ 3.21

ping από το Host προς το PC2

```
ping -c 4 192.168.56.102
```

length 48
Η διαφορά οφείλεται στις διαφορετικές προεπιλεγμένες ρυθμίσεις του `ping` στα Windows και στο FreeBSD/Linux.

ΕΡΩΤΗΣΗ 3.22

Όταν κάνουμε `ping` μεταξύ δύο FreeBSD/Linux μηχανών, το TTL είναι 64.

Όταν κάνουμε `ping` από Windows προς FreeBSD, το TTL ξεκινά από 128 λόγω προεπιλογών των Windows.

ΕΡΩΤΗΣΗ 3.23

Καταγραφή κίνησης σε αρχείο ενώ παράλληλα παρατηρούμε την οθόνη
1ος τρόπος:

```
tcpdump -i em0 -n -l icmp | tee capture.log
```

- `tcpdump -i em0 -n -l icmp` → Καταγράφει ICMP πακέτα (π.χ. `ping`) στη διεπαφή `em0`, χωρίς να επιλύει IP (`-n`), και με γραμμική έξοδο (`-l`).
- `| tee capture.log` → Στέλνει την έξοδο ταυτόχρονα στην οθόνη και στο αρχείο `capture.log`.

2ος τρόπος:

```
tcpdump -i em0 -w capture.pcap
```

```
tcpdump -r capture.pcap -l
```

ΕΡΩΤΗΣΗ 3.24

```
tcpdump -i em0 -n icmp -vvv
```

Όχι δεν παρατηρούμε κίνηση.

ΕΡΩΤΗΣΗ 3.25

Καμία κίνηση.

ΕΡΩΤΗΣΗ 3.26

Πριν την αλλαγή του `Promiscuous Mode`, το PC1 έβλεπε μόνο πακέτα που το αφορούσαν. Μετά την αλλαγή (`Allow VMs`), το PC1 βλέπει όλη την ICMP κίνηση μεταξύ των VM.

ΑΣΚΗΣΗ 4 Δικτύωση Internal

PC2-> Internal Network με όνομα εσωτερικού δικτύου LAN.

ΕΡΩΤΗΣΗ 4.1

Στο PC1:

```
ifconfig em0 192.168.56.103/24
```

Στο PC2:

```
ifconfig em0 192.168.56.102/24
```

ΕΡΩΤΗΣΗ 4.2

Δεν εμφανίστηκε μήνυμα λάθους.

ΕΡΩΤΗΣΗ 4.3

Καταγραφή με εμφάνιση πληροφοριών στο PC1:

```
tcpdump -i em0 -n -vvv
```

ΕΡΩΤΗΣΗ 4.4

ping από host στο PC2:

```
ping 192.168.56.102 -n 4
```

Όχι. Destination host unreachable.

ΕΡΩΤΗΣΗ 4.5

Ναι καταγράφηκαν πακέτα ICMP(ping) και ARP(το PC1 μαθαίνει τη MAC διεύθυνση του PC2 μέσω ARP).

ΕΡΩΤΗΣΗ 4.6

Όχι δεν γίνεται ping από PC2 στο PC1.

ΕΡΩΤΗΣΗ 4.7

Όχι δεν παρατηρώ κάποια κίνηση.

ΕΡΩΤΗΣΗ 4.8

Τώρα ναι επικοινωνούν.

ΕΡΩΤΗΣΗ 4.9

Δεν μπορώ να επικοινωνήσω από το host με τα PC1, PC2 γιατί αυτά βρίσκονται σε internal δίκτυο.

ΕΡΩΤΗΣΗ 4.10

```
tcpdump -i em0 -n -vvv
```

ΕΡΩΤΗΣΗ 4.11

Καθαρισμός πίνακα arp στο PC2:

```
arp -d -a
```

ping στο host-only adapter στο PC2:

```
ping -c 4 192.168.56.1
```

ARP Requests who has

ΕΡΩΤΗΣΗ 4.12

Το PC2 δεν μπορεί να επικοινωνήσει με το Host.

ΕΡΩΤΗΣΗ 4.13

PC1: `ifconfig em0 10.11.12.61/26`
PC2: `ifconfig em0 10.11.12.62/26`

ΕΡΩΤΗΣΗ 4.14

Ναι επικοινωνούν μεταξύ τους.

ΑΣΚΗΣΗ 5 Δικτύωση NAT

ΕΡΩΤΗΣΗ 5.1

Απόδοση IP μέσω DHCP στη διεπαφή em0

```
dhclient em0
```

ΕΡΩΤΗΣΗ 5.2

```
ifconfig em0
```

PC1->10.0.2.15
PC2->10.0.2.15
PC3->10.0.2.15

ΕΡΩΤΗΣΗ 5.3

```
netstat -r
```

default gateway: 10.0.2.2

ΕΡΩΤΗΣΗ 5.4

```
cat /etc/resolv.conf
```

nameserver 10.02.3

ΕΡΩΤΗΣΗ 5.5

```
cat /var/db/dhclient.leases.em0
```

ΕΡΩΤΗΣΗ 5.6

Επικοινωνία με προεπιλεγμένη πύλη.

```
ping -c 4 10.0.2.2
```

Ναι γίνεται ping κανονικά.

ΕΡΩΤΗΣΗ 5.7

Επικοινωνία με το Internet.

```
ping -c 4 8.8.8.8
```

Ναι γίνεται ping κανονικά.

ΕΡΩΤΗΣΗ 5.8

```
ping -c 4 10.0.2.1
ping -c 4 10.0.2.2
ping -c 4 10.0.2.3
ping -c 4 10.0.2.4
```

Γίνονται κανονικά στα `10.0.2.2, 10.0.2.3.`

ΕΡΩΤΗΣΗ 5.9

Όχι γιατί έχουμε NAT.

Ξεκίνημα καταγραφής Wireshark και PC3 `tcpdump -i em0 -n icmp -w data`
Αποστολή ping από δεύτερη κονσόλα στο PC3

```
ping -n -c 3 -m 64 9.9.9.9
```

Σταμάτημα καταγραφών και άνοιγμα αρχείου data: `tcpdump -r data -n`

ΕΡΩΤΗΣΗ 5.10

Αποστολή ping από δεύτερη κονσόλα στο PC3

```
ping -n -c 3 -m 64 9.9.9.9
```

`-n`: Απενεργοποιεί την ανάλυση ονομάτων (DNS lookup), ώστε να εμφανίζονται μόνο οι IP διευθύνσεις αντί για ονόματα host.
`-c 3`: Καθορίζει ότι θα σταλούν τρία ICMP Echo Request πακέτα και μετά θα σταματήσει η εκτέλεση της εντολής.
`-m 64`: Ορίζει την αρχική τιμή TTL σε 64. Το TTL καθορίζει τον μέγιστο αριθμό hops (δρομολογητών) που μπορεί να περάσει το πακέτο πριν απορριφθεί.
-Η διεύθυνση `9.9.9.9` είναι ο προορισμός των ICMP Echo Request πακέτων, που θα απαντήσει με ICMP Echo Reply αν υπάρχει συνδεσιμότητα στο διαδίκτυο.

ΕΡΩΤΗΣΗ 5.11

```
tcpdump -r data -n | grep "ICMP echo request"
```

IPv4 source address: 10.0.2.15
TTL: 64

ΕΡΩΤΗΣΗ 5.12

Wireshark
IPv4 source address: 192.168.61.44
TTL: 128

ΕΡΩΤΗΣΗ 5.13

Wireshark
IPv4 destination address: 9.9.9.9
TTL: 56

ΕΡΩΤΗΣΗ 5.14

```
tcpdump -r data -n | grep "ICMP echo reply"
```

IPv4 destination address: 10.0.2.15
TTL: 64

ΕΡΩΤΗΣΗ 5.15

```
tracert -d 9.9.9.9
```

9 hops

ΕΡΩΤΗΣΗ 5.16

64-56 = 8 σωστό γιατί έχουμε και ενδιάμεσο δρομολογητή.

ΕΡΩΤΗΣΗ 5.17

```
traceroute -I -n -q 1 9.9.9.9
```

`-I`: Χρησιμοποιεί ICMP Echo Request αντί για τα προεπιλεγμένα UDP πακέτα.
`-n`: Εμφανίζει μόνο IP διευθύνσεις, χωρίς να κάνει ανάλυση DNS (όπως `-d` στο `tracert`).
`-q 1`: Στέλνει μόνο 1 πακέτο ανά hop.

ΕΡΩΤΗΣΗ 5.18

1 hop
Ναι συμφωνεί.

ΑΣΚΗΣΗ 6 Δικτύωση NAT Network

ΕΡΩΤΗΣΗ 6.1

Network address: 10.0.2.0/24

ΕΡΩΤΗΣΗ 6.2

Διαγραφή IP στα PC1, PC2:

```
ifconfig em0 delete
```

Διαγραφή αρχείου προηγούμενων DHCP leases στα PC1, PC2:

```
rm -f /var/db/dhclient.leases.em0
```

ΕΡΩΤΗΣΗ 6.3

Απόδοση IP μέσω DHCP στη διεπαφή em0 στα PC1, PC2:

```
dhclient em0
```

ΕΡΩΤΗΣΗ 6.4

Εμφάνιση νέων διευθύνσεων στα PC1, PC2:

```
ifconfig em0
```

IPv4 PC1: 10.0.2.15
IPv4 PC2: 10.0.2.4 καινούρια.

ΕΡΩΤΗΣΗ 6.5

```
cat /var/db/dhclient.leases.em0
```

IPv4 DHCP server: 10.0.2.3

ΕΡΩΤΗΣΗ 6.6

```
cat /etc/resolv.conf
```

nameserver 192.168.61.89

ΕΡΩΤΗΣΗ 6.7

```
netstat -rn
```

default gateway: 10.0.2.1

ΕΡΩΤΗΣΗ 6.8

Επικοινωνία PC1, PC2 με default gateway:

```
ping -c 4 10.0.2.3
```

Επιτυχής

ΕΡΩΤΗΣΗ 6.9

Επικοινωνία PC1, PC2 με DHCP server:

```
ping -c 4 10.0.2.1
```

Επιτυχής

ΕΡΩΤΗΣΗ 6.10

```
ping -c 4 10.0.2.2
```

Επιτυχής επικοινωνία.

```
arp -a
```

Απαντά default gateway.

ΕΡΩΤΗΣΗ 6.11

Επικοινωνία με το Internet:

```
ping -c 4 google.com
```

Επιτυχής

ΕΡΩΤΗΣΗ 6.12

Επικοινωνία μεταξύ PC1,PC2:
ping στην IP του άλλου
Επιτυχής

ΕΡΩΤΗΣΗ 6.13

Επικοινωνία PC3 με PC1,PC2:
ping στην IP τους
Ανεπιτυχής αφού βρίσκονται σε διαφορετικό NAT.

ΕΡΩΤΗΣΗ 6.14

```
arp -a
```

Πρέπει να κάνουμε καταγραφή.

ΕΡΩΤΗΣΗ 6.15

Ξεκίνημα καταγραφής Wireshark και PC1 `tcpdump -i em0 -n icmp`

Νέα κονσόλα PC1:

```
traceroute -I -n -q 1 9.9.9.9
```

IPv4 source addresses:
192.168.61.89,10.14.30.61, 10.14.30.98, 10.14.30.100, 10.14.38.2, 176.126.38.32, 176.126.38.118

ΕΡΩΤΗΣΗ 6.16

IPv4 destination address: 192.168.61.44

ΕΡΩΤΗΣΗ 6.17

```
tcpdump -r data -nv icmp | grep "time exceeded"
```

IPv4 source addresses:
10.0.2.1, 10.14.30.61, 10.14.30.98, 10.14.30.100, 10.14.38.2, 176.126.38.32, 176.126.38.118

ΕΡΩΤΗΣΗ 6.18

IPv4 destination address: 10.0.2.15

ΕΡΩΤΗΣΗ 6.19

Όχι.

ΕΡΩΤΗΣΗ 6.20

Παρατηρούμε και time exceeded και έχουμε καλύτερη ορατότητα λόγω NAT Network.