Ονοματεπώνυμο: Χαράλαμπος Καμπουγέρης **Όνομα PC/ΛΣ:** DESKTOP-N90CRE0

Ομάδα: 1, Τρίτη 10:45-13:30, Αιθ.Α4 **Ημερομηνία:** 28/02/2024

Εργαστηριακή Άσκηση 2
Δικτύωση συστημάτων στο VirtualBox

Άσκηση 1

1.1) – 1.15) Ακολουθούμε τα βήματα. Συγκεκριμένα έχουμε:

1.7

```
Username    : lab
Password    : *****
Full Name   :
Uid         : 1001
Class       :
Groups      : wheel
Home        : /home/lab
Home Mode   :
Shell       : /bin/csh
Locked      : no
```

1.10

```
root@PC:~ # ps aux | grep sshd
root  736   0.0  3.2 12420 7368  -  Is   07:53   0:00.00 sshd: /usr/sbin/sshd [
root  769   0.0  0.1   420  212 v0  R+   07:54   0:00.00 grep sshd
```

1.11 rm /etc/resolv.conf
rm /var/db/dhclient.leases.*

1.12 history -c

Άσκηση 2

2.1 Με την εντολή “ifconfig”

2.2 Εκτελώντας διαδοχικά την εντολή “ifconfig em0 down” για απενεργοποίηση και στη συνέχεια την εντολή “ifconfig em0 up” για ενεργοποίηση

2.3 Με τις εντολές “man tcpdump”, “man pcap” και “man pcap-filter”

2.4 Με την εντολή “tcpdump -i em0 -n”. Καθώς το σύστημα μας έχει μόνο μια κάρτα δικτύου η εντολή αυτή μπορεί να παραλέιπεται

2.5 Με την εντολή “tcpdump -X”. Εμφανίζει στην οθόνη τα περιεχόμενα (πλην της επικεφαλίδας στρώματος ζεύξης δεδομένων) του πακέτου σε δεκαεξαδική και ASCII μορφή.

2.6 Θέλουμε να τυπώσουμε επιπλέον την επικεφαλίδα ethernet, άρα με την εντολή “tcpdump -e”.

2.7 Με την εντολή “tcpdump -s 68”

2.8 Με την εντολή “tcpdump ip host 10.0.0.1 -v ”

2.9 Με την εντολή “tcpdump host 10.0.0.1 and 10.0.0.2”

2.10 Με την εντολή “tcpdump net 1.1.0.0/16”

2.11 Με την εντολή “tcpdump not net 192.168.1.0/24 -e”

2.12 Με την εντολή “tcpdump ip ‘broadcast or multicast’c ”

2.13 Με την εντολή “tcpdump ip and greater 576”

2.14 Με την εντολή “tcpdump ‘ip[8] < 5’”

2.15 Με την εντολή “tcpdump (ip[0] & 0x0f) > 5”. Στο πρώτο byte της επικεφαλίδας IP έχουμε τα πρώτα 4 bits για το Version και άλλα 4 για το Header Length, το οποίο by default είναι 5 εκτός και αν έχουμε options. Επομένως, εκτελούμε bitwise and με το 1111, ώστε να πάρουμε τα τελευταία 4 bits και τα συγκρίνουμε με το 5.

2.16 Με την εντολή “tcpdump icmp and src host 10.0.0.1”

2.17 Με την εντολή “tcpdump tcp and dst host 10.0.0.2”

2.18 Με την εντολή “tcpdump udp and dst port 53”

2.19 Με την εντολή “tcpdump tcp and host 10.0.0.10”

2.20 Με την εντολή “tcpdump tcp and host 10.0.0.10 and port 23 -w “sample_capture””

2.21 Με την εντολή “tcpdump tcp[tcpflags] & (tcp-syn) != 0“

2.22 Με την εντολή “tcpdump ‘tcp[tcpflags] & ((tcp-syn) | (tcp-syn & tcp-ack)) != 0’”

2.23 Με την εντολή “tcpdump tcp[tcpflags] & (tcp-fin|tcp-rst) != 0 “

2.24 Η παράσταση tcp[12:1] μας δίνει τα 8 bits του 13ου Byte μιας TCP επικεφαλίδας.

Η έκφραση tcp[12:1] & 0xf0 μας δίνει τις τιμές των τεσσάρων αριστερότερων bits, τα οποία και εκφράζουν την τιμή του πεδίου Data Offset (Header Length σε 32bites λέξεις).
Με την τελική παράσταση που μας δίνεται (>>2), διαιρούμε ουσιαστικά το Data Offset ακέραια με το 4. Αυτό που προκύπτει τελικά είναι το πραγματικό μέγεθος της επικεφαλίδας σε bytes. Π.χ. αν είχαμε αρχικά ως 13ο byte το 01110001, τότε, από τα 4 αριστερότερα bits συμπεραίνουμε ότι το μήκος της επικεφαλίδας είναι 0111 = 7_{10} * 4bytes = 28 bytes, ενώ αν εφαρμόσουμε το φίλτρο τότε το byte αυτό μετατρέπεται σε 00011100 = 28_{10}

2.25 Με την εντολή "tcpdump (tcp[12] & 0xf0) > 5 "
Το πεδίο Data Offset καθορίζει το μήκος της κεφαλίδας TCP σε λέξεις 4 byte, επομένως μια τιμή μεγαλύτερη από 5 υποδηλώνει την παρουσία επιλογών (καθώς το ελάχιστο μήκος κεφαλίδας χωρίς επιλογές είναι 20 byte ή 5 μονάδες).

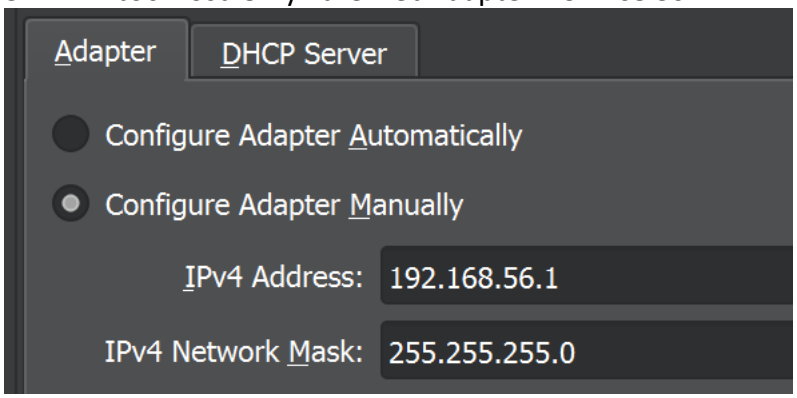
2.26 Με την εντολή "tcpdump -A port 80"

2.27 Με την εντολή "tcpdump dst edu-dy.cn.ntua.gr and port 23 "

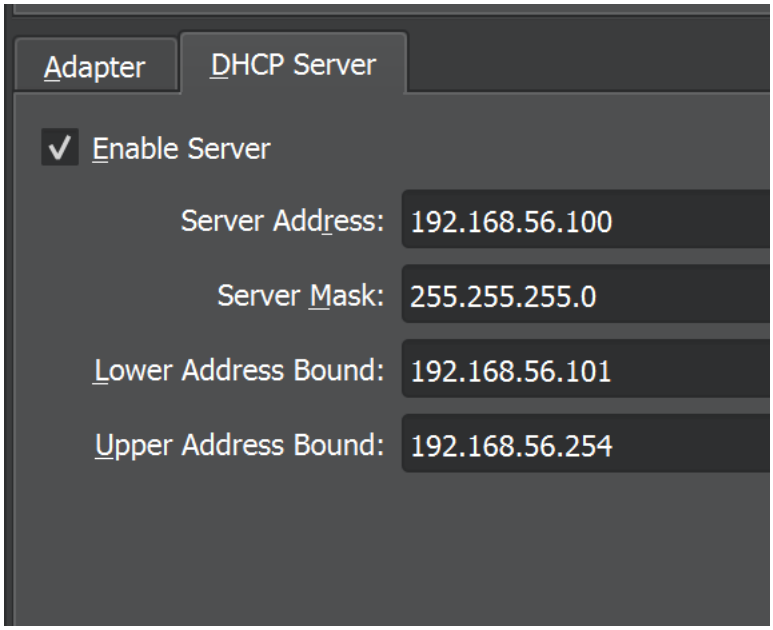
2.28 Με την εντολή "tcpdump ip6"

Άσκηση 3

3.1 IPv4 του Host-Only Ethernet Adapter: 192.168.56.1



3.2 IPv4 του DHCP Server: 192.168.56.100 και περιοχή εκχώρησης διευθύνσεων: 192.168.56.101 έως 192.168.56.254



3.3 Εκτελούμε την εντολή “dhclient” σε κάθε μηχάνημα.

3.4 Αποδίδεται η 192.168.56.104 στο PC1 και η 192.168.56.105 στο PC2.

3.5 Κάνουμε ping από το 1 μηχάνημα στο άλλο και λαμβάνουμε απάντηση (π.χ. ping 192.168.56.105 από το PC1).

3.6 Κάνοντας ping από το terminal του υπολογιστή μας σε κάθε μία από τις IPv4 διευθύνσεις που αποδόθηκαν παραπάνω

3.7 netstat -r

3.8 Με την εντολή netstat -r παίρνουμε τον ακόλουθο πίνακα:

```
root@PC:~ # netstat -r
Routing tables

Internet:
Destination        Gateway            Flags     Netif Expire
localhost          link#2             UH          lo0
192.168.56.0/24    link#1             U           em0
192.168.56.105     link#1             UHS         lo0

Internet6:
Destination        Gateway            Flags     Netif Expire
::/96              localhost          URS         lo0
localhost          link#2             UHS         lo0
::ffff:0.0.0.0/96  localhost          URS         lo0
fe80::/10          localhost          URS         lo0
fe80::%lo0/64      link#2             U           lo0
fe80::1%lo0        link#2             UHS         lo0
ff02::/16          localhost          URS         lo0
```

Όπως περιμέναμε, δεν υπάρχει gateway καθώς στη Host-Only δικτύωση δεν επιτρέπεται σύνδεση με συσκευές εκτός του Host-Only δικτύου.

3.9 Δεν μπορούμε να κάνουμε ping στην IPv4 διεύθυνση της φυσικής κάρτας δικτύου του host machine, στην δικτύωση Host-Only των VMs ανήκει σε διαφορετικό δίκτυο. Όταν ο host θέλει να επικοινωνήσει με τα VMs χρησιμοποιεί τη Virtual κάρτα δικτύου (με IP 192.168.56.1)

3.10 Με την εντολή hostname βλέπουμε ότι τα μηχανήματα έχουν όνομα **PC.ntua.lab**

```
root@PC:~ # hostname
PC.ntua.lab
```

3.11 hostname PC1 και hostname PC2 στα μηχανήματα PC1 και PC2 αντίστοιχα

3.12

```
root@PC1:~ #
```

3.13 Όχι, δε το περιέχει, αντ' αυτού περιέχει το "PC.ntua.lab", επομένως σε ενδεχόμενη επανεκκίνηση θα χρησιμοποιηθεί πάλι το παλιό.

3.14 Διορθώνουμε την τιμή του πεδίου "hostname=" σε PC1 και PC2 αντίστοιχα με χρήση του vi ("vi /etc/rc.conf").

3.15 Όπως διαβάζουμε από το manpage της hosts (“man hosts”), θα πρέπει για κάθε IPv4 διεύθυνση που επιθυμούμε να χρησιμοποιούμε όνομα αντί αυτής να προσθέσουμε μια γραμμή με τα παρακάτω:

- Internet Address
- official host name
- Aliases

Επομένως, προσθέτουμε στο /etc/hosts του PC1 τη γραμμή “192.168.56.105 PC2 PC2.local”, ενώ στου PC2 τη γραμμή “192.168.56.104 PC1 PC1.local”.

3.16 ping localhost, το οποίο αντιστοιχη στην ip 127.0.0.1 και έχει οριστεί στο αρχείο /etc/hosts ως «127.0.0.1 localhost localhost.my.domain

3.17

```
root@PC1:~ # ping -c 2  192.168.56.100
PING 192.168.56.100 (192.168.56.100): 56 data bytes
64 bytes from 192.168.56.100: icmp_seq=0 ttl=255 time=0.677 ms
64 bytes from 192.168.56.100: icmp_seq=1 ttl=255 time=0.719 ms

--- 192.168.56.100 ping statistics ---
2 packets transmitted, 2 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.677/0.698/0.719/0.021 ms
```

```
root@PC1:~ # ping -c 2 192.168.56.1
PING 192.168.56.1 (192.168.56.1): 56 data bytes
64 bytes from 192.168.56.1: icmp_seq=0 ttl=128 time=0.471 ms
64 bytes from 192.168.56.1: icmp_seq=1 ttl=128 time=1.620 ms

--- 192.168.56.1 ping statistics ---
2 packets transmitted, 2 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.471/1.046/1.620/0.574 ms
```

```
root@PC1:~ # ping -c 2 PC2
PING PC2 (192.168.56.105): 56 data bytes
64 bytes from 192.168.56.105: icmp_seq=0 ttl=64 time=0.832 ms
64 bytes from 192.168.56.105: icmp_seq=1 ttl=64 time=1.080 ms

--- PC2 ping statistics ---
2 packets transmitted, 2 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.832/0.956/1.080/0.124 ms
```

3.18 tcpdump -n host PC1

3.19 Length: 64 bytes, TTL: 64 bytes

3.20 tcpdump icmp -vvv

3.21 Το φιλοξενούν μηχάνημα αναφέρει πως παράγει 32bytes, τα οποία, ωστόσο αφορούν καθαρά το ICMP Payload, επομένως, το συνολικό ICMP μήνυμα εάν συμπεριλάβουμε την ICMP επικεφαλίδα είναι 40 bytes. Η διαφορά αυτή έγκειται στα λειτουργικά συστήματα των 2 μηχανημάτων, καθώς τα Windows στέλνουν μηνύματα μήκους 40 bytes, ενώ τα unix* μηχανήματα 64 bytes

3.22 TTL:64 bytes, ταυτίζεται με τις τιμές που βρήκα προηγουμένως

3.23 Είτε με την εντολή "tcpdump icmp and host PC1 -l | tee capture" είτε με την εντολή "tcpdump icmp and host PC1 -l > capture & tail -f capture".

3.24 Δεν παρατηρείται κίνηση

3.25 Παρατηρούμε ARP request που αφορά την MAC του PC2

3.26 Βλέπουμε ότι καταγράφει όλη την κίνηση του υποδικτύου και όχι μόνο αυτή που έχει προορισμό το PC1

Άσκηση 4

4.1 PC1: "ifconfig em0 192.168.56.104/24", PC2: "ifconfig em0 192.168.56.105/24"

4.2 Σταματάει η σύνδεση με τον dhclient που υπήρχε

```
root@PC2:~ # Feb 27 20:02:16 PC2 dhclient[1366]: My address (192.168.56.105) was
 deleted, dhclient exiting
Feb 27 20:02:16 PC2 dhclient[1366]: connection closed
Feb 27 20:02:16 PC2 dhclient[1366]: exiting.
```

4.3 tcpdump -vvv

4.4 Όχι, δεν μπορούμε

4.5 Όχι, δεν παρατηρούμε

4.6 Όχι, δεν μπορούμε

4.7 Όχι, δεν παρατηρούμε

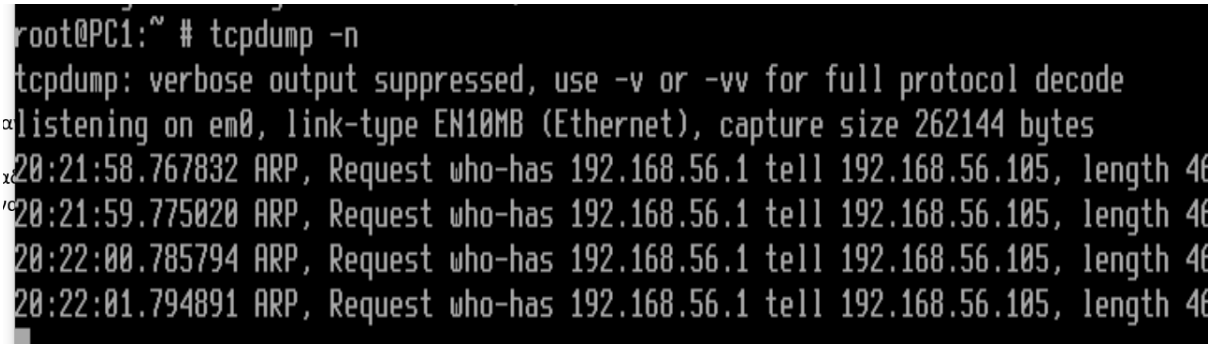
4.8 Ναι, τώρα επικοινωνούν κανονικά

4.9 Το φιλοξενούν μηχάνημα αδυνατεί να επικοινωνήσει με οποιοδήποτε από τα μηχανήματα όπως και ήταν αναμενόμενο. Ο λόγος που αυτό συμβαίνει, είναι πως με τη

δικτύωση Internal Network στην πραγματικότητα δημιουργούμε ένα εικονικό ιδιωτικό LAN δίκτυο για τα VMs μας, χωρίς να υπάρχει δυνατότητα επικοινωνίας με τον host, αφού η εικονική διεπαφή που διαθέτει ο host δεν είναι στο δίκτυο αυτό.

4.10 Εκτελούμε “tcpdump -n” στο PC1

4.11 Αδειάζουμε τον πίνακα arp του PC2 με την εντολή “arp -ad”. Παράγονται τα εξής μηνύματα τύπου ARP request, δηλαδή ο PC2 ψάχνει την MAC address της διεύθυνσης 192.168.56.1:



4.12 Το μήνυμα “host is down” υποδεικνύει πως δε γνωρίζουμε τη διαδρομή για τη διεύθυνση που κάναμε ping και κανένα μηχάνημα δεν απαντάει στα ARP request του PC2

4.13 Το υποδίκτυο "10.11.12.0/26" έχει συνολικά 64 διευθύνσεις IP, οι οποίες περιλαμβάνουν τη network address (10.11.12.0), τη broadcast address(10.11.12.63) και 62 χρησιμοποιήσιμες διευθύνσεις κεντρικού υπολογιστή (που κυμαίνονται από 10.11.12.1 έως 10.11 .12.62). Οι τελευταίες διαθέσιμες διευθύνσεις IP του υποδικτύου είναι οι 10.11.12.61 και 10.11.12.62. Επομένως, εισάγουμε τις εντολές:
PC1: ifconfig em0 10.11.12.61/26
PC2: ifconfig em0 10.11.12.62/26

4.14 Τα μηχανήματα επικοινωνούν κανονικά

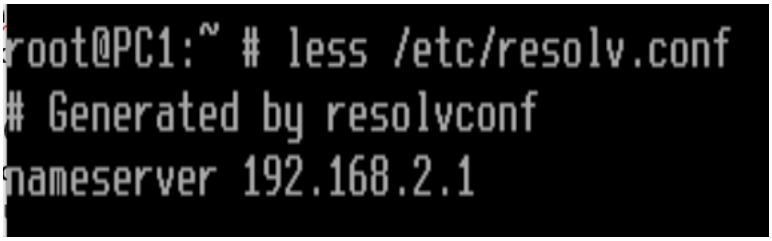
Άσκηση 5

5.1 Εκτελούμε σε κάθε μηχάνημα “dhclient em0”.

5.2 Αποδόθηκε στο καθένα από αυτά η IP 10.0.2.15 από τη διεύθυνση 10.0.2.2

5.3 Εκτελώντας την εντολή **netstat -r** παρατηρούμε ότι η προεπιλεγμένη πύλη είναι η 10.0.2.2

5.4 Το περιεχόμενο του αρχείο /etc/resolv.conf είναι το εξής:



5.5 Στο αρχείο /var/db/dhclient.leases.em0

5.6 Ναι, μπορούμε να κάνουμε “ping 10.0.2.2”.

5.7 Το νέο εικονικό μηχάνημα επικοινωνεί κανονικά με το internet, μιας και διατίθεται για αυτό προκαθορισμένη πύλη(gateway), στην οποία και θα αποσταλούν τα όποια πακέτα έχουν προορισμό σε εξωτερικό δίκτυο για να δρομολογηθούν. Εκτελώντας “ping www.amazon.com” λαμβάνουμε κανονικά απάντηση.

5.8 Παρατηρήσαμε τα εξής:
• 10.0.2.1 (δε λαμβάνουμε απάντηση)
• 10.0.2.2 (λαμβάνουμε απάντηση – default gateway)
• 10.0.2.3 (λαμβάνουμε απάντηση – proxy DNS server)
• 10.0.2.4 (λαμβάνουμε απάντηση – TFTP Server)

5.9 Το κάθε VM βλέπει τον εαυτό του σαν μοναδικό στο δίκτυό του και επικοινωνεί με το δικό του gateway router, το οποίο με τη σειρά του επικοινωνεί με τη φυσική κάρτα δικτύου του host. Επομένως, δεν υπάρχει τρόπος να δρομολογηθεί ένα πακέτο από το PC3 στο PC1 ή στο PC2, διότι θα έχει ως αποδέκτη την IP διεύθυνση 10.0.2.15, επομένως θα στέλνει στην πραγματικότητα πακέτα στον εαυτό του.

5.10
• -I: Επιβάλει χρήση ICMP Echo μηνυμάτων αντί για UDP datagrams
• -n: Εμφανίζει μόνο τις διευθύνσεις από τις οποίες περνάνε τα πακέτα χωρίς να κάνει resolve σε ονόματα.
• -q: Καθορίζει το πόσα πακέτα θα σταλούν ανά request (το default είναι 3, εμείς στέλνουμε 1
• 9.9.9.9: Η τελική διεύθυνση των πακέτων μας

5.11 “tcpdump icmp and host PC1 -l | tee capture”
Διεύθυνση IPv4 πηγής: 10.0.2.15 Τύπος μηνυμάτων που παράγει η traceroute: ICMP Echo request.

5.12 Από το Wireshark ως διεύθυνση πηγής εμφανίζεται η 192.168.2.9 , δηλαδή αυτή του υπολογιστή μας (host).

5.13 192.168.2.1 -> 62.38.0.170 -> 176.126.38.118

5.14 192.168.2.9 , δηλαδή αυτή του υπολογιστή μας

5.15 Οι ίδιες με το ερώτημα 5.13 αλλά υπάρχει και η Default Gateway: 10.0.2.2

5.16 Η IP του εικονικού μηχανήματος 10.0.2.15

5.17 Αντιστοιχούν όλα εκτός του πρώτου

5.18

```
PS C:\Users\xarri> tracert -d 9.9.9.9

Tracing route to 9.9.9.9 over a maximum of 30 hops

  1     2 ms     2 ms     3 ms  192.168.2.1
  2    16 ms    15 ms    15 ms  62.38.0.170
  3     *        *       15 ms  176.126.38.32
  4    20 ms    16 ms    18 ms  176.126.38.118
  5    21 ms    16 ms    22 ms  9.9.9.9

Trace complete.
```

```
root@PC:~ # traceroute -I -n -q 1 9.9.9.9
traceroute to 9.9.9.9 (9.9.9.9), 64 hops max, 48 byte packets
 1  10.0.2.2  0.692 ms
 2  192.168.2.1  7.880 ms
 3  62.38.0.170  15.654 ms
 4  *
 5  176.126.38.118  19.092 ms
 6  9.9.9.9  17.372 ms
```

Από το φιλοξενούν μηχάνημα έχουμε ένα λιγότερο hop καθώς το εικονικό μηχάνημα βρίσκεται σε ακόμα ένα υποδίκτυο μέσα στο host

Άσκηση 6

6.1 Έχει ορισθεί η 10.0.2.0/24.

6.2 Σε καθένα από τα μηχανήματα εκτελούμε την εντολή “ifconfig em0 delete” και “rm /var/db/dhclient.leases.em0”

6.3 Εκτελούμε “dhclient em0”

6.4 Αποδόθηκαν στο PC1 και PC2 οι 10.0.2.15 και 10.0.2.4 αντίστοιχα

6.5 DHCP IPv4: 10.0.2.3.

6.6 Και για τα δύο μηχανήματα το περιεχόμενο είναι:

```
root@PC2:~ # cat /etc/resolv.conf
# Generated by resolvconf
nameserver 192.168.2.1
```

6.7 Η προκαθορισμένη πύλη είναι η 10.0.2.1

```
root@PC1:~ # netstat -r
Routing tables

Internet:
Destination        Gateway            Flags     Netif Expire
default            10.0.2.1           UGS        em0
```

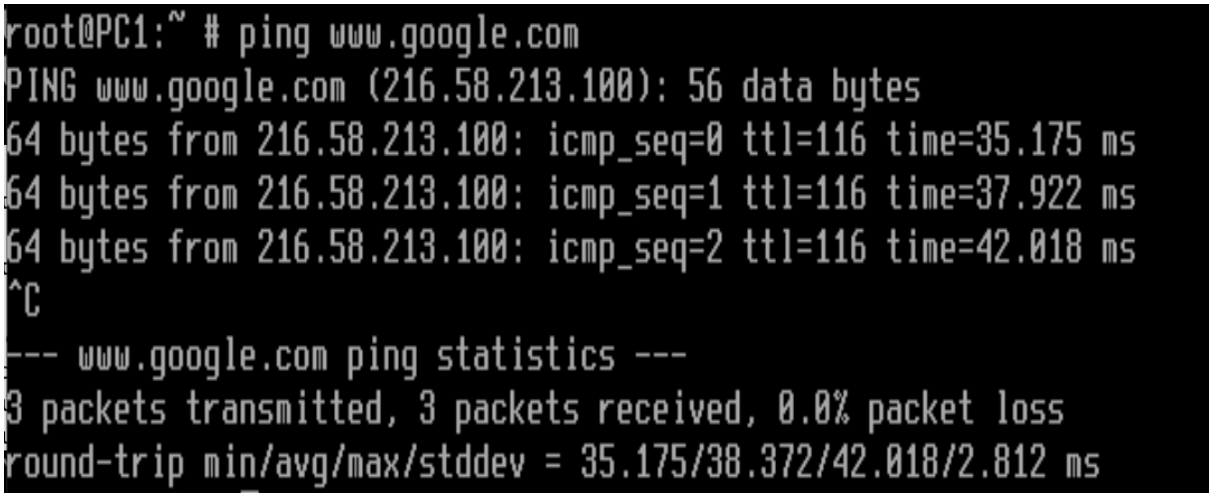
6.8 Ναι, μπορούμε

6.9 Ναι, μπορούμε

6.10 Μπορούμε να κάνουμε κανονικά ping στην “10.0.2.2”. Μάλιστα, παρατηρούμε πως πρόκειται στην πραγματικότητα για την “συσκευή” που αποτελεί την προκαθορισμένη πύλη, αφού από τον πίνακα arp βλέπουμε πως η 10.0.2.1 και 10.0.2.2 έχουν ίδιες MAC διευθύνσεις.

```
root@PC1:~ # arp -a
10.0.2.15 (10.0.2.15) at 08:00:27:32:89:85 on em0 permanent [ethernet]
10.0.2.1 (10.0.2.1) at 52:54:00:12:35:00 on em0 expires in 1059 seconds [etherne
t]
10.0.2.2 (10.0.2.2) at 52:54:00:12:35:00 on em0 expires in 1191 seconds [etherne
t]
```

6.11 Τα μηχανήματα επικοινωνούν κανονικά με το Internet (π.χ. ping www.google.com), αναμενόμενο αφού έχουν gateway router για να κάνει τις απαραίτητες δρομολογήσεις.



6.12 Ναι, επικοινωνούν

6.13 Δοκιμάζοντας να κάνουμε ping στο PC2, φαίνεται πως λαμβάνουμε κανονικά απάντηση. Το PC1 εν προκειμένω έχει ίδια IPv4 με το PC3 επομένως δε μπορούμε να το εξετάσουμε

6.14 Βλέποντας τη MAC που είναι αποθηκευμένη στον ARP πίνακα για τη διεύθυνση 10.0.2.4 (PC2), παρατηρούμε πως είναι διαφορετική από αυτή που πραγματικά έχει το PC2, δε μπορούμε από το PC3 να κάνουμε ping στο PC2, ούτε και στο PC1