



ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

Εργαστήριο Δικτύων Υπολογιστών

Αναφορά 2ης Εργαστηριακής Άσκησης

Ραπτόπουλος Πέτρος (ει19145)

Άσκηση 2: Ανάλυση δικτυακών πρωτοκόλλων με το TCPDUMP

2.1) Με ποια εντολή φλοιού μπορείτε να δείτε ποιες κάρτες δικτύου διαθέτει το εικονικό μηχάνημα καθώς και την κατάστασή τους;

```
root@PC:~ # ifconfig
em0: flags=8802<BROADCAST,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=81009b<RXCSUM,TXCSUM,ULAN_MTU,ULAN_HWTAGGING,ULAN_HWCSUM,ULAN_HW
FILTER>
        ether 08:00:27:d1:96:68
        media: Ethernet autoselect (1000baseT <full-duplex>)
        status: active
        nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> metric 0 mtu 16384
        options=680003<RXCSUM,TXCSUM,LINKSTATE,RXCSUM_IPv6,TXCSUM_IPv6>
        inet6 ::1 prefixlen 128
        inet6 fe80::1%lo0 prefixlen 64 scopeid 0x2
        inet 127.0.0.1 netmask 0xff000000
        groups: 1o
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
```

2.2) Με ποιες εντολές μπορείτε να απενεργοποιήσετε: **root@PC:~ # ifconfig em0 down**

και στη συνέχεια ενεργοποιήσετε την κάρτα δικτύου em0: **root@PC:~ # ifconfig em0 up**

2.3) Με ποιες εντολές φλοιού μπορείτε να βρείτε περισσότερες πληροφορίες για τα tcpdump, pcap και pcap-filter; **man tcpdump**, **man pcap**, **man pcap-filter**

2.4) Ποια είναι η σύνταξη της εντολής tcpdump που θα σας επιτρέψει να συλλάβετε όλα τα πλαίσια από την κάρτα δικτύου em0 χωρίς επίλυση διευθύνσεων IP; **tcpdump -i em0 -n**

2.5) Ποια είναι η σύνταξη της εντολής tcpdump που θα σας επιτρέψει να συλλάβετε όλα τα πλαίσια από την κάρτα δικτύου em0 και να εμφανίσετε τα περιεχόμενα των σε ASCII: **tcpdump -i em0 -A**
και δεκαεξαδική μορφή: **tcpdump -i em0 -x**

2.6) Ποια είναι η σύνταξη της εντολής tcpdump που θα σας επιτρέψει να βλέπετε και τις διευθύνσεις MAC πηγής, προορισμού των πλαισίων που συλλάβατε; **tcpdump -e**

2.7) Ποια είναι η σύνταξη της εντολής tcpdump που θα σας επιτρέψει να συλλάβετε από την κάρτα δικτύου em0 τα πρώτα 68 byte όλων των πλαισίων; **tcpdump -s 68**

2.8) Ποια είναι η σύνταξη της εντολής tcpdump που θα σας επιτρέψει να συλλάβετε πακέτα IPv4 με διεύθυνση 10.0.0.1 και να δείτε τις λεπτομέρειες της επικεφαλίδας τους; **tcpdump -v host 10.0.0.1**

2.9) Ποια είναι η σύνταξη της εντολής tcpdump που θα σας επιτρέψει να συλλάβετε στην κάρτα δικτύου em0 πακέτα της επικοινωνίας μεταξύ δύο μηχανημάτων με διευθύνσεις 10.0.0.1 και 10.0.0.2;
tcpdump -v host 10.0.0.1 and 10.0.0.2 -i em0

2.10) Ποια είναι η σύνταξη της εντολής tcpdump που θα σας επιτρέψει να συλλάβετε πακέτα IPv4 για το δίκτυο 1.1.0.0/16 και να εμφανίσετε στην οθόνη το περιεχόμενό τους; **tcpdump -x net 1.1.0.0/16 and ip**

2.11) Ποια είναι η σύνταξη της εντολής tcpdump που θα σας επιτρέψει να συλλάβετε πακέτα IPv4 που δεν ανήκουν (και δεν έπρεπε ποτέ να έχουν φτάσει) στο τοπικό σας δίκτυο, ας πούμε το 192.168.1.0/24, και να τυπώσετε στην οθόνη το περιεχόμενό τους περιλαμβανομένων των επικεφαλίδων Ethernet; **tcpdump -x -e not net 192.168.1.0/24 and ip**

2.12) Ποια είναι η σύνταξη της εντολής tcpdump που θα σας επιτρέψει να συλλάβετε IPv4 πακέτα εκπομπής; **tcpdump -i em0 -n 'broadcast' and ip**

2.13) Ποια είναι η σύνταξη της εντολής που θα σας επιτρέψει να συλλάβετε πακέτα IPv4 μήκους μεγαλύτερου των 576B; **tcpdump -i em0 ip[2:2] > 576**

2.14) Ποια είναι η σύνταξη της εντολής που θα σας επιτρέψει να συλλάβετε πακέτα IPv4 με τιμές TTL μικρότερες του 5; **tcpdump -i em0 ip[8:1] < 5**

2.15) Ποια είναι η σύνταξη της εντολής που θα σας επιτρέψει να συλλάβετε πακέτα IPv4 με προαιρετικές επικεφαλίδες; **tcpdump -i em0 'ip[0] & ox0f > 5'**

2.16) Ποια είναι η σύνταξη της εντολής tcpdump που θα σας επιτρέψει να συλλάβετε πακέτα ICMP με αποστολέα την IP διεύθυνση 10.0.0.1; **tcpdump -i em0 'src 10.0.0.1 and icmp'**

2.17) Ποια είναι η σύνταξη της εντολής που θα σας επιτρέψει να συλλάβετε τεμάχια TCP με παραλήπτη την IP 10.0.0.2; **tcpdump -i em0 'dst 10.0.0.2 and tcp'**

- 2.18) Ποια είναι η σύνταξη εντολής ώστε να συλλάβετε δεδομενογράμματα UDP με θύρα προορισμού 53; **tcpdump -i em0 'dst port 53 and udp'****
- 2.19) Ποια είναι η σύνταξη εντολής ώστε να συλλάβετε τεμάχια TCP με διεύθυνση αποστολέα ή παραλήπτη 10.0.0.10; **tcpdump 'host 10.0.0.10 and tcp'****
- 2.20) Τροποποιήστε την εντολή της παραπάνω ερώτησης, ώστε να εμφανίζονται μόνο όσα τεμάχια εξ αυτών προορίζονται για την TCP θύρα 23 και τα αποτελέσματα να αποθηκεύονται στο αρχείο "sample_capture". **tcpdump 'host 10.0.0.10 and port 23 and tcp' -w sample_capture****
- 2.21) Ποια είναι η σύνταξη της εντολής tcpdump που θα σας επιτρέψει να συλλάβετε τεμάχια TCP που περιέχουν μόνο τη σημαία SYN; **tcpdump -i em0 'tcp[tcpflags] & tcp-syn != 0'****
- 2.22) Ποια είναι η σύνταξη της εντολής tcpdump που θα σας επιτρέψει να συλλάβετε τα πρώτα δύο τεμάχια της τριμερούς χειραψίας TCP; **tcpdump -i em0 '(tcp[tcpflags]&tcp-syn!=0 and tcp[tcpflags]&tcp-ack==0) or (tcp[tcpflags]&tcp-syn!=0 and tcp[tcpflags]&tcp-ack!=0)'****
- 2.23) Ποια είναι η σύνταξη της εντολής tcpdump που θα σας επιτρέψει να συλλάβετε τα σχετικά με την απόλυτη μιας σύνδεσης TCP τεμάχια; **tcpdump -i em0 'tcp[tcpflags]&tcp-fin!=0'****
- 2.24) Τι ακριβώς υπολογίζει η παράσταση ((tcp[12:1] & 0xfo) >> 2) χρησιμοποιούμενη ως στοιχείο φίλτρου για τη σύλληψη τεμαχίων TCP; **Υπολογίζει το μήκος της επικεφαλίδας TCP σε bytes.****
- 2.25) Ποια είναι η σύνταξη της εντολής tcpdump που θα σας επιτρέψει να συλλάβετε τεμάχια TCP που περιλαμβάνουν προαιρετικές επικεφαλίδες (options); **tcpdump -i em0 '(tcp[12:1] & 0xfo) >> 2) > 20'****
- 2.26) Ποια είναι η σύνταξη της εντολής tcpdump που θα σας επιτρέψει να συλλάβετε μηνύματα HTTP και να δείτε το περιεχόμενο ως χαρακτήρες ASCII; **tcpdump -i em0 'tcp port 80' -A****
- 2.27) Ποια είναι η σύνταξη της εντολής tcpdump που θα σας επιτρέψει να συλλάβετε μηνύματα telnet προς το edu-dy.cn.ntua.gr; **tcpdump udp port telnet and dst edu-dy.cn.ntua.gr****
- 2.28) Ποια είναι η σύνταξη της εντολής tcpdump που θα σας επιτρέψει να συλλάβετε πακέτα IPv6; **tcpdump ip6****

Άσκηση 3: Δικτύωση Host-only

- 3.1) Από το μενού του VirtualBox βρείτε τη διεύθυνση IPv4 του Host-only Ethernet adapter. **192.168.56.1****
- 3.2) Παρομοίως βρείτε τη διεύθυνση IPv4 του εξυπηρετητή DHCP για το δίκτυο Host-only: **192.168.56.100** καθώς και την περιοχή διευθύνσεων IPv4 που αυτός μπορεί να εκχωρήσει: **Από 192.168.56.101 έως 192.168.56.254****
- 3.3) Αποδώστε μέσω DHCP διευθύνσεις IPv4 στα εικονικά μηχανήματα.**

| | |
|---|---|
| <pre>root@PC:~ # dhclient em0 DHCPDISCOVER on em0 to 255.255.255.255 port 67 interval 7 Mar 4 22:16:12 PC dhclient[1115]: send_packet: Network is down DHCPDISCOVER on em0 to 255.255.255.255 port 67 interval 8 DHCPOFFER from 192.168.56.100 DHCPREQUEST on em0 to 255.255.255.255 port 67 DHCPACK from 192.168.56.100 bound to 192.168.56.102 -- renewal in 300 seconds.</pre> | <pre>root@PC:~ # dhclient em0 DHCPDISCOVER on em0 to 255.255.255.255 port 67 interval 3 Mar 4 22:17:30 PC dhclient[1100]: send_packet: Network is down DHCPDISCOVER on em0 to 255.255.255.255 port 67 interval 4 DHCPOFFER from 192.168.56.100 DHCPREQUEST on em0 to 255.255.255.255 port 67 DHCPACK from 192.168.56.100 bound to 192.168.56.103 -- renewal in 300 seconds.</pre> |
|---|---|

- 3.4) Ποιες είναι οι διευθύνσεις IPv4 που έχει αποδώσει το VirtualBox στα μηχανήματα;**

PC1: 192.168.56.102, PC2: 192.168.56.103

- 3.5) Πώς θα καταλάβετε αν τα δύο μηχανήματα επικοινωνούν μεταξύ τους;**

Κάνουμε ping από το ένα μηχάνημα στο άλλο και παρατηρούμε ότι τα πακέτα μεταδίδονται επιτυχώς.

| | |
|--|--|
| <pre>root@PC:~ # ping 192.168.56.103 PING 192.168.56.103 (192.168.56.103): 56 data bytes 64 bytes from 192.168.56.103: icmp_seq=0 ttl=64 time=1.351 ms 64 bytes from 192.168.56.103: icmp_seq=1 ttl=64 time=0.792 ms 64 bytes from 192.168.56.103: icmp_seq=2 ttl=64 time=1.171 ms ^C --- 192.168.56.103 ping statistics --- 3 packets transmitted, 3 packets received, 0.0% packet loss round-trip min/avg/max/stdev = 0.792/1.105/1.351/0.233 ms</pre> | <pre>root@PC:~ # ping 192.168.56.102 PING 192.168.56.102 (192.168.56.102): 56 data bytes 64 bytes from 192.168.56.102: icmp_seq=0 ttl=64 time=0.795 ms 64 bytes from 192.168.56.102: icmp_seq=1 ttl=64 time=0.836 ms 64 bytes from 192.168.56.102: icmp_seq=2 ttl=64 time=0.993 ms ^C --- 192.168.56.102 ping statistics --- 3 packets transmitted, 3 packets received, 0.0% packet loss round-trip min/avg/max/stdev = 0.795/0.874/0.993/0.085 ms</pre> |
|--|--|

- 3.6) Πώς θα καταλάβετε αν το φιλοξενούν μηχάνημα επικοινωνεί με τα δύο μηχανήματα;**

Κάνουμε ping από το host μηχάνημα και στα δύο guest και παρατηρούμε ότι τα πακέτα μεταδίδονται επιτυχώς.

```
petrosrapt0@petrosrapt0Assistant:~$ ping 192.168.56.102
PING 192.168.56.102 (192.168.56.102) 56(84) bytes of data.
64 bytes from 192.168.56.102: icmp_seq=1 ttl=64 time=1.12 ms
64 bytes from 192.168.56.102: icmp_seq=2 ttl=64 time=0.514 ms
64 bytes from 192.168.56.102: icmp_seq=3 ttl=64 time=0.557 ms
^C
--- 192.168.56.102 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 0.514/0.729/1.117/0.274 ms
```

```
petrosrapt0@petrosrapt0Assistant:~$ ping 192.168.56.103
PING 192.168.56.103 (192.168.56.103) 56(84) bytes of data.
64 bytes from 192.168.56.103: icmp_seq=1 ttl=64 time=0.524 ms
64 bytes from 192.168.56.103: icmp_seq=2 ttl=64 time=0.329 ms
64 bytes from 192.168.56.103: icmp_seq=3 ttl=64 time=0.646 ms
^C
--- 192.168.56.103 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2035ms
rtt min/avg/max/mdev = 0.329/0.499/0.646/0.130 ms
```

3.7) Ποια είναι η σύνταξη της εντολής που θα σας δείξει την προεπιλεγμένη πύλη;

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

Internet:
Destination      Gateway          Flags   Netif Expire
localhost        link#2           UH     lo0
192.168.0.0/24    link#1           U       em0
192.168.56.103   link#1           UHS    lo0

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

3.8) Υπάρχει προεπιλεγμένη πύλη στη συγκεκριμένη κατάσταση δικτύωσης; Τεκμηριώστε την απάντησή σας.

Παρατηρούμε ότι δεν υπάρχει προεπιλεγμένη πύλη για τη συγκεκριμένη κατάσταση δικτύωσης καθώς στους πίνακες δρομολόγησης απουσιάζουν rows με flag 'G' που υποδεικνύει default gateway.

Στον τρόπο δικτύωσης 'Host-Only' οι εικονικές μηχανές επικοινωνούν μεταξύ τους και με το φιλοξενούν μηχάνημα.

Ωστόσο το δίκτυο είναι απομονωμένο από άλλα εξωτερικά δίκτυα. Συνεπώς δεν έχει νόημα η ύπαρξη def. gateway.

3.9) Από τα εικονικά μηχανήματα μπορείτε να κάνετε ping στην IPv4 διεύθυνση της φυσικής κάρτας δικτύου του φιλοξενούντος μηχανήματος; 'Όχι δεν μπορούμε ("No route to host").

```
root@PC:~ # ping 192.168.1.138
PING 192.168.1.138 (192.168.1.138): 56 data bytes
ping: sendto: No route to host
ping: sendto: No route to host
ping: sendto: No route to host
^C
--- 192.168.1.138 ping statistics ---
3 packets transmitted, 0 packets received, 100.0% packet loss
```

Τεκμηριώστε την απάντησή σας. Με τη δικτύωση host-only η κίνηση από τα εικονικά μηχανήματα παραμένει εσωτερικά στο φιλοξενούν μηχάνημα και είναι ορατή μόνο στα άλλα εικονικά μηχανήματα του ίδιου εσωτερικού δικτύου (και στο φιλοξενούν). Δεν υπάρχει επικοινωνία με το διαδίκτυο. Συνεπώς η φυσική κάρτα δικτύου του φιλοξενούν μηχανήματος δεν είναι προσβάσιμη από τα εικονικά μηχανήματα, καθώς δεν ανήκει στο εσωτερικό δίκτυο.

3.10) Ποιο είναι το όνομα των μηχανημάτων όπως το αντιλαμβάνεται το λειτουργικό τους σύστημα; Ποια εντολή φλοιού χρησιμοποιήσατε; **root@PC:~ # hostname**

```
PC.ntua.lab
```

3.11) Αλλάξετε τα ονόματα, όπως τα αντιλαμβάνεται το λειτουργικό τους σύστημα, των δύο εικονικών συστημάτων ώστε να ταυτιστούν με τα ονόματα PC1 και PC2, αντίστοιχα, που έχουν στο VirtualBox.

```
root@PC:~ # hostname PC1
root@PC:~ # hostname
PC1
```

```
root@PC:~ # hostname PC2
root@PC:~ # hostname
PC2
```

3.12) Χωρίς χρήση κάποιας εντολής, επιβεβαιώστε ότι το όνομα άλλαξε. Που εμφανίζεται αυτό στον φλοιό; **root@PC1:~ #**
Παρατηρούμε ότι εμφανίζεται στον φλοιό κατά την προτροπή για εισαγωγή εντολής. ("@PC1").

3.13) Περιέχει το αρχείο παραμετροποίησης /etc/rc.conf στο PC1 το νέο όνομα; 'Όχι δεν το περιέχει'.
Σε ενδεχόμενη επανεκκίνηση του PC1 ποιο θα είναι το όνομά του; Θα παραμείνει "PC.ntua.lab"

```
root@PC1:~ # cat /etc/rc.conf
sshd_enable="YES" # to enable the ssh daemon
hostname="PC.ntua.lab" # to assign the host name
syslogd_flags="-scc" # to disable compression of repeated messages
```

3.14) Διορθώστε, ώστε στην επόμενη επανεκκίνηση τα μηχανήματα να έχουν τα νέα ονόματα:

```
root@PC1:~ # cat /etc/rc.conf
sshd_enable="YES" # to enable the ssh daemon
hostname="PC1" # to assign the host name
syslogd_flags="-scc" # to disable compression of repeated messages
```

3.15) Τι πρέπει να προσθέσετε για να μπορείτε να χρησιμοποιείτε σε αμφότερα τα μηχανήματα τα ονόματα αντί των IPv4 διευθύνσεών τους στις διάφορες δικτυακές εντολές;

Πρέπει σε κάθε μηχάνημα να προσθέσουμε στο αρχείο /etc/hosts την γραμμή <ip_address><hostname> όπου ip_address, hostname τα στοιχεία του άλλου εικονικού μηχανήματος. Για παράδειγμα στο μηχάνημα PC1:

```
# Host Database
#
# This file should contain the addresses and aliases for local hosts that
# share this file. Replace 'my.domain' below with the domainname of your
# machine.
#
# In the presence of the domain name service or NIS, this file may
# not be consulted at all; see /etc/nsswitch.conf for the resolution order.
#
#
::1           localhost localhost.my.domain
127.0.0.1     localhost localhost.my.domain
#
# Imaginary network.
#10.0.0.2      myname.my.domain myname
#10.0.0.3      myfriend.my.domain myfriend
192.168.56.103 PC2
#
# According to RFC 1918, you can use the following IP networks for
# private nets which will never be connected to the Internet:
#
#      10.0.0.0      -      10.255.255.255
/etc/hosts: 32 lines, 1117 characters.
```

3.16) Γράψτε ένα παράδειγμα σύνταξης κάποιας εντολής, στην οποία χρησιμοποιείται η λειτουργία που προσφέρει το αρχείο hosts, ώστε να μη χρειάζεται να ορίσουμε διεύθυνση IPv4.

Πριν να αλλάξουμε το αρχείο /etc/hosts:

```
root@PC1:~ # ping PC2
ping: cannot resolve PC2: Host name lookup failure
```

Μετά την αλλαγή στο αρχείο /etc/hosts:

```
root@PC1:~ # ping PC2
PING PC2 (192.168.56.103): 56 data bytes
64 bytes from 192.168.56.103: icmp_seq=0 ttl=64 time=0.988 ms
64 bytes from 192.168.56.103: icmp_seq=1 ttl=64 time=0.879 ms
^C
--- PC2 ping statistics ---
2 packets transmitted, 2 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.879/0.933/0.988/0.055 ms
```

3.17) Καταγράψτε δύο τρόπους με τους οποίους μπορείτε να χρησιμοποιήσετε την εντολή tcpdump ώστε να καταγράφετε την κίνηση σε αρχείο ενώ παράλληλα την παρατηρείτε στην οθόνη.

```
root@PC1:~ # ping -c 4 PC2
PING PC2 (192.168.56.103): 56 data bytes
64 bytes from 192.168.56.103: icmp_seq=0 ttl=64 time=0.559 ms
64 bytes from 192.168.56.103: icmp_seq=1 ttl=64 time=0.528 ms
64 bytes from 192.168.56.103: icmp_seq=2 ttl=64 time=1.275 ms
64 bytes from 192.168.56.103: icmp_seq=3 ttl=64 time=0.959 ms

--- PC2 ping statistics ---
4 packets transmitted, 4 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.528/0.830/1.275/0.308 ms
```

Α' Τρόπος:

```
root@PC2:~ # tcpdump -i em0 host PC1 -l | tee test
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on em0, link-type EN10MB (Ethernet), capture size 262144 bytes
23:40:39.275468 IP PC1 > 192.168.56.103: ICMP echo request, id 30981, seq 0, length 64
23:40:39.275489 IP 192.168.56.103 > PC1: ICMP echo reply, id 30981, seq 0, length 64
23:40:40.280096 IP PC1 > 192.168.56.103: ICMP echo request, id 30981, seq 1, length 64
23:40:40.280115 IP 192.168.56.103 > PC1: ICMP echo reply, id 30981, seq 1, length 64
23:40:41.290976 IP PC1 > 192.168.56.103: ICMP echo request, id 30981, seq 2, length 64
23:40:41.290996 IP 192.168.56.103 > PC1: ICMP echo reply, id 30981, seq 2, length 64
23:40:42.300839 IP PC1 > 192.168.56.103: ICMP echo request, id 30981, seq 3, length 64
23:40:42.300859 IP 192.168.56.103 > PC1: ICMP echo reply, id 30981, seq 3, length 64
```

Β' Τρόπος:

```
root@PC2:~ # tcpdump -w - -U | tee test | tcpdump -r -
tcpdump: listening on em0, link-type EN10MB (Ethernet), capture size 262144 bytes
reading from file -, link-type EN10MB (Ethernet)
23:43:06.017097 IP PC1 > 192.168.56.103: ICMP echo request, id 34053, seq 0, length 64
23:43:06.017132 IP 192.168.56.103 > PC1: ICMP echo reply, id 34053, seq 0, length 64
23:43:07.019968 IP PC1 > 192.168.56.103: ICMP echo request, id 34053, seq 1, length 64
23:43:07.020003 IP 192.168.56.103 > PC1: ICMP echo reply, id 34053, seq 1, length 64
23:43:08.029101 IP PC1 > 192.168.56.103: ICMP echo request, id 34053, seq 2, length 64
23:43:08.029136 IP 192.168.56.103 > PC1: ICMP echo reply, id 34053, seq 2, length 64
23:43:09.039999 IP PC1 > 192.168.56.103: ICMP echo request, id 34053, seq 3, length 64
23:43:09.040138 IP 192.168.56.103 > PC1: ICMP echo reply, id 34053, seq 3, length 64
```

3.18) Ποιο είναι το μήκος των μηνυμάτων ICMP της απάντησης που λαμβάνει το PC1: **64 bytes**

και ποια είναι η τιμή του πεδίου TTL των αντίστοιχων πακέτων IPv4; **64**

3.19) Κάντε τώρα ping από το PC1 στη διεύθυνση IPv4 της εικονικής κάρτας (Host-only adapter) του φιλοξενούντος μηχανήματος. Ποια είναι η τιμή του πεδίου TTL της απάντησης; **64**

```
root@PC1:~ # ping 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=64 time=1.073 ms
64 bytes from 192.168.56.1: icmp_seq=1 ttl=64 time=0.633 ms
64 bytes from 192.168.56.1: icmp_seq=2 ttl=64 time=0.356 ms
^C
--- 192.168.56.1 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.356/0.688/1.073/0.295 ms
```

3.20) Ποια είναι η σύνταξη της εντολής tcpdump που χρησιμοποιήσατε; **root@PC2:~ # tcpdump -i em0 icmp -vvv**

3.21) Ποιο είναι το μήκος των μηνυμάτων ICMP που παράγει το φιλοξενούν μηχάνημα; **841B μήκος πακέτου (56B data)**

```
petrosrapto@petrosraptoAssistant:~$ ping 192.168.56.103
PING 192.168.56.103 (192.168.56.103) 56(84) bytes of data.
64 bytes from 192.168.56.103: icmp_seq=1 ttl=64 time=0.442 ms
^C
--- 192.168.56.103 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.442/0.442/0.442/0.000 ms
```

```
root@PC2:~ # tcpdump -i em0 icmp -vvv
tcpdump: listening on em0, link-type EN10MB (Ethernet), capture size 262144 bytes
01:30:05.114063 IP (tos 0x0, ttl 64, id 17980, offset 0, flags [DF], proto ICMP (1), length 84)
    192.168.56.1 > 192.168.56.103: ICMP echo request, id 5, seq 1, length 64
01:30:05.114105 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto ICMP (1), length 84)
    192.168.56.103 > 192.168.56.1: ICMP echo reply, id 5, seq 1, length 64
```

Γιατί διαφέρει από το μήκος που παρατηρήσατε πριν; Οφείλεται στα διαφορετικά λειτουργικά συστήματα.

3.22) Ποια είναι η τιμή του πεδίου TTL των πακέτων που ανταλλάσσονταν τα δύο μηχανήματα; Συμφωνεί με τις τιμές που βρήκατε προηγουμένως; **Είναι 64 και ναι συμφωνεί.**

3.23) Ξεκινήστε μια νέα καταγραφή στο PC1 και από το παράθυρο εντολών στο φιλοξενούν μηχάνημα κάντε πάλι ping στη διεύθυνση IP του PC2. Παρατηρήσατε στην καταγραφή στο PC1 κάποια σχετική με το ping κίνηση. Εάν ναι, τι αφορούσε; **Δεν παρατηρούμε καταγραφή στο PC1.**

3.24) Από το μενού Advanced στις ρυθμίσεις της κάρτας δικτύου του PC1, αφού σταματήσετε την καταγραφή, αλλάξτε το promiscuous mode σε Allow VMs και επαναλάβετε τη διαδικασία της προηγούμενης ερώτησης. Τι διαφορετικό παρατηρείτε τώρα; Καταγράφεται η κίνηση icmp μεταξύ φιλοξενούντος μηχανήματος και PC2.

```
root@PC1:~ # tcpdump -i em0 icmp -vvv
tcpdump: listening on em0, link-type EN10MB (Ethernet), capture size 262144 bytes
01:39:57.376033 IP (tos 0x0, ttl 64, id 1511, offset 0, flags [DF], proto ICMP (1), length 84)
    192.168.56.1 > PC2: ICMP echo request, id 7, seq 1, length 64
01:39:57.376261 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto ICMP (1), length 84)
    PC2 > 192.168.56.1: ICMP echo reply, id 7, seq 1, length 64
01:39:58.403024 IP (tos 0x0, ttl 64, id 1711, offset 0, flags [DF], proto ICMP (1), length 84)
```

Άσκηση 4: Δικτύωση Internal

4.1) Ποια είναι σύνταξη εντολής που χρησιμοποιήσατε για να ορίσετε τις στατικές διευθύνσεις IPv4 στα μηχανήματα;

```
root@PC1:~ # ifconfig em0 192.168.56.102
```

```
root@PC2:~ # ifconfig em0 192.168.56.103
```

4.2) Τι σημαίνει το μήνυμα λάθους που εμφανίσθηκε όταν ορίσατε στατικές διευθύνσεις;

Απόλυτη σύνδεσης με τον DHCP server.

4.3) Ξεκινήστε μια καταγραφή με εμφάνιση λεπτομερειών στο PC1 αφήστε την να τρέχει. **tcpdump -i em0 -vvv**

4.4) Από το φιλοξενούν μηχάνημα μπορείτε να κάνετε ping στο PC2;

```
petrosrapto@petrosraptoAssistant:~$ ping 192.168.56.103
PING 192.168.56.103 (192.168.56.103) 56(84) bytes of data.
From 192.168.56.1 icmp_seq=10 Destination Host Unreachable
From 192.168.56.1 icmp_seq=11 Destination Host Unreachable
From 192.168.56.1 icmp_seq=12 Destination Host Unreachable
^C
--- 192.168.56.103 ping statistics ---
14 packets transmitted, 0 received, +3 errors, 100% packet loss, time 13292ms
pipe 4
```

4.5) Παρατηρείτε στην καταγραφή κίνηση σχετική με το ping προς το PC2;

```
02:05:51.738551 ARP, Ethernet (len 6), IPv4 (len 4), Request who-has PC2 tell 19
2.168.56.1, length 46
02:05:52.762672 ARP, Ethernet (len 6), IPv4 (len 4), Request who-has PC2 tell 19
2.168.56.1, length 46
02:05:53.786999 ARP, Ethernet (len 6), IPv4 (len 4), Request who-has PC2 tell 19
2.168.56.1, length 46
02:05:54.810581 ARP, Ethernet (len 6), IPv4 (len 4), Request who-has PC2 tell 19
2.168.56.1, length 46
02:05:55.834205 ARP, Ethernet (len 6), IPv4 (len 4), Request who-has PC2 tell 19
2.168.56.1, length 46
```

4.6) Από το PC2 μπορείτε να κάνετε ping στο PC1;

```
root@PC2:~ # ping 192.168.56.102
PING 192.168.56.102 (192.168.56.102): 56 data bytes
ping: sendto: Host is down
ping: sendto: Host is down
ping: sendto: Host is down
^C
--- 192.168.56.102 ping statistics ---
8 packets transmitted, 0 packets received, 100.0% packet loss
```

4.7) Παρατηρείτε στην καταγραφή κίνηση σχετική με το ping προς το PC1; **Όχι**

4.8) Αφού σταματήσετε την καταγραφή, αλλάξτε τις ρυθμίσεις δικτύου του PC1 αντίστοιχα με το PC2. Επικοινωνούν τώρα τα δύο εικονικά μηχανήματα; **Ναι**

```
root@PC2:~ # ping 192.168.56.102
PING 192.168.56.102 (192.168.56.102): 56 data bytes
64 bytes from 192.168.56.102: icmp_seq=0 ttl=64 time=0.970 ms
64 bytes from 192.168.56.102: icmp_seq=1 ttl=64 time=0.623 ms
^C
--- 192.168.56.102 ping statistics ---
2 packets transmitted, 2 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.623/0.796/0.970/0.174 ms
```

4.9) Από το φιλοξενούν μηχάνημα μπορείτε να επικοινωνήσετε με κάποιο από τα δύο εικονικά μηχανήματα; Τεκμηριώστε την απάντησή σας.

```
petrosrapto@petrosraptoAssistant:~$ ping 192.168.56.103
PING 192.168.56.103 (192.168.56.103) 56(84) bytes of data.
From 192.168.56.1 icmp_seq=1 Destination Host Unreachable
From 192.168.56.1 icmp_seq=2 Destination Host Unreachable
From 192.168.56.1 icmp_seq=3 Destination Host Unreachable
^C
--- 192.168.56.103 ping statistics ---
4 packets transmitted, 0 received, +3 errors, 100% packet loss, time 3074ms
pipe 4
petrosrapto@petrosraptoAssistant:~$ ping 192.168.56.102
PING 192.168.56.102 (192.168.56.102) 56(84) bytes of data.
From 192.168.56.1 icmp_seq=9 Destination Host Unreachable
From 192.168.56.1 icmp_seq=10 Destination Host Unreachable
From 192.168.56.1 icmp_seq=11 Destination Host Unreachable
^C
--- 192.168.56.102 ping statistics ---
12 packets transmitted, 0 received, +3 errors, 100% packet loss, time 11261ms
pipe 4
```

Δεν μπορούμε να επικοινωνήσουμε από το φιλοξενούν μηχάνημα με κάποιο από τα δύο μηχανήματα καθώς στην δικτύωση "Internal Network" το φιλοξενούν μηχάνημα δεν είναι μέρος του δικτύου.

4.10) Αφού επαναφέρετε το promiscuous mode στην προκαθορισμένη τιμή Deny ξεκινήστε μια νέα καταγραφή στο PC1 χωρίς επίλυση διευθύνσεων IPv4 σε ονόματα

```
root@PC1:~ # tcpdump -i em0 -n
```

4.11) Στη συνέχεια στο PC2, αφού αδειάσετε τον πίνακα arp (δείτε σχετική σελίδα man), κάντε ping στη διεύθυνση IPv4 της εικονικής κάρτας του φιλοξενούντος μηχανήματος. Στην καταγραφή στο PC1, τι είδους μηνύματα παρατηρείτε ότι παράγει το PC2;

Arp requests ψάχνοντας για την MAC διεύθυνση που αντιστοιχεί στην διεύθυνση IPv4 του φιλοξενούντος

```
root@PC2:~ # arp -d -a  
192.168.56.102 (192.168.56.102) deleted  
root@PC2:~ # ping 192.168.56.1  
PING 192.168.56.1 (192.168.56.1): 56 data bytes  
^C  
--- 192.168.56.1 ping statistics ---  
5 packets transmitted, 0 packets received, 100.0% packet loss  
root@PC2:~ #
```

```
root@PC1:~ # tcpdump -i em0 -n  
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode  
listening on em0, link-type EN10MB (Ethernet), capture size 262144 bytes  
02:23:37.951370 ARP, Request who-has 192.168.56.1 tell 192.168.56.103, length 46  
02:23:38.955661 ARP, Request who-has 192.168.56.1 tell 192.168.56.103, length 46  
02:23:39.963531 ARP, Request who-has 192.168.56.1 tell 192.168.56.103, length 46
```

4.12) Πώς εξηγείτε το μήνυμα host is down που επιστρέφει το ping;

```
root@PC2:~ # ping 192.168.56.1  
PING 192.168.56.1 (192.168.56.1): 56 data bytes  
ping: sendto: Host is down  
ping: sendto: Host is down  
^C  
--- 192.168.56.1 ping statistics ---  
7 packets transmitted, 0 packets received, 100.0% packet loss  
root@PC2:~ #
```

To ping επιστρέφει εν τέλει το μήνυμα “host is down” αφού δεν λαμβάνουμε ARP reply στο ARP request που στείλαμε.

4.13) Αλλάξτε τη διεύθυνση IPv4 των δύο συστημάτων χρησιμοποιώντας τις τελευταίες 2 διαθέσιμες διεύθυνσεις IP από το υποδίκτυο 10.11.12.0/26. **PC1: 10.11.12.61 (bin(61): 00111101) PC2: 10.11.12.62 (bin(62): 00111110)**

Τα πρώτα 26 bit αποτελούν το netmask. Η διεύθυνση 10.11.12.63 (bin(63): 00111111) είναι broadcast.

```
root@PC1:~ # ifconfig em0 10.11.12.61 root@PC2:~ # ifconfig em0 10.11.12.62
```

4.14) Επικοινωνούν τώρα τα δύο εικονικά μηχανήματα μεταξύ τους χρησιμοποιώντας τις διεύθυνσεις IPv4 που ορίσατε προηγουμένως; Ναι

```
root@PC1:~ # ping 10.11.12.62  
PING 10.11.12.62 (10.11.12.62): 56 data bytes  
64 bytes from 10.11.12.62: icmp_seq=0 ttl=64 time=0.739 ms  
64 bytes from 10.11.12.62: icmp_seq=1 ttl=64 time=0.685 ms  
^C  
--- 10.11.12.62 ping statistics ---  
2 packets transmitted, 2 packets received, 0.0% packet loss  
round-trip min/avg/max/stddev = 0.685/0.712/0.739/0.027 ms
```

```
root@PC2:~ # ping 10.11.12.61  
PING 10.11.12.61 (10.11.12.61): 56 data bytes  
64 bytes from 10.11.12.61: icmp_seq=0 ttl=64 time=0.919 ms  
64 bytes from 10.11.12.61: icmp_seq=1 ttl=64 time=0.783 ms  
^C  
--- 10.11.12.61 ping statistics ---  
2 packets transmitted, 2 packets received, 0.0% packet loss  
round-trip min/avg/max/stddev = 0.783/0.851/0.919/0.068 ms
```

Άσκηση 5: Δικτύωση NAT

5.1) Αποδώστε με DHCP διεύθυνση IPv4 στη διεπαφή em0 των εικονικών μηχανημάτων.

```
root@PC1:~ # dhclient em0  
DHCPDISCOVER on em0 to 255.255.255.255 port 67 interval 6  
DHCPOFFER from 10.0.2.2  
DHCPREQUEST on em0 to 255.255.255.255 port 67  
DHCPACK from 10.0.2.2  
bound to 10.0.2.15 -- renewal in 43200 seconds.
```

```
root@PC2:~ # dhclient em0  
DHCPDISCOVER on em0 to 255.255.255.255 port 67 interval 5  
DHCPOFFER from 10.0.2.2  
DHCPREQUEST on em0 to 255.255.255.255 port 67  
DHCPACK from 10.0.2.2  
bound to 10.0.2.15 -- renewal in 43200 seconds.
```

```
root@PC:~ # dhclient em0  
DHCPDISCOVER on em0 to 255.255.255.255 port 67 interval 3  
Mar 6 18:52:38 PC dhclient[766]: send_packet: Network is down  
DHCPDISCOVER on em0 to 255.255.255.255 port 67 interval 3  
DHCPOFFER from 10.0.2.2  
DHCPREQUEST on em0 to 255.255.255.255 port 67  
DHCPACK from 10.0.2.2  
bound to 10.0.2.15 -- renewal in 43200 seconds.
```

5.2) Ποια διεύθυνση IPv4 έχουν λάβει: **10.0.2.15** και από πού (διεύθυνση IP) αποδόθηκε; **10.0.2.2**

5.3) Ποια είναι η προεπιλεγμένη πύλη στον πίνακα δρομολόγησης; **10.0.2.2**

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

Internet:
Destination      Gateway        Flags     Netif   Expire
default          10.0.2.2      UGS      em0
10.0.0.0/8       link#1        U         em0
10.0.2.0/24      link#1        U         em0
10.0.2.15        link#1        UHS      lo0
10.11.12.61      link#1        UHS      lo0
localhost        link#2        UH       lo0

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

5.4) Ποιο είναι το περιεχόμενο του αρχείου /etc/resolv.conf;

```
root@PC1:~ # cat /etc/resolv.conf
# Generated by resolvconf
search lan
nameserver 10.0.2.3
```

5.5) Σε ποιο αρχείο των εικονικού μηχανήματος έχει καταγραφεί η διεύθυνση IPv4 που αποδόθηκε προηγουμένως μέσω DHCP καθώς και οι πληροφορίες που περιέχει το resolv.conf; **Στο αρχείο "/var/db/dhclient.leases.em0"**

5.6) Από τα εικονικά μηχανήματα μπορείτε να κάνετε ping στη διεύθυνση IPv4 της προεπιλεγμένης πύλης; **Ναι**

```
root@PC1:~ # ping 10.0.2.2
PING 10.0.2.2 (10.0.2.2): 56 data bytes
64 bytes from 10.0.2.2: icmp_seq=0 ttl=64 time=1.184 ms
64 bytes from 10.0.2.2: icmp_seq=1 ttl=64 time=0.622 ms
^C
--- 10.0.2.2 ping statistics ---
2 packets transmitted, 2 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.622/0.903/1.184/0.281 ms
```

5.7) Επικοινωνεί το νέο εικονικό μηχάνημα με το Internet; **Ναι**

Τεκμηριώστε την απάντησή σας.

Στη δικτύωση NAT του VirtualBox,

όταν το φιλοξενούμενο μηχάνημα στέλνει κίνηση μέσω της πύλης προς το διαδίκτυο, οι διευθύνσεις IPv4 των πακέτων μεταφράζονται ώστε να φαίνεται ότι αυτά ξεκινούν από το φιλοξενούν μηχάνημα και όχι από το φιλοξενούμενο, τα δε πακέτα που προκύπτουν σε απάντηση επιστρέφονται στο φιλοξενούμενο μηχάνημα ως εάν προέρχονταν από το διαδίκτυο. Συνεπώς τα εικονικά μηχανήματα επικοινωνούν με το Internet.

5.8) Σε ποιες από τις διευθύνσεις 10.0.2.1 έως 10.0.2.4 λαμβάνετε απάντηση εάν κάνετε ping; Τι παριστάνουν αυτές;

```
root@PC1:~ # ping 10.0.2.1
PING 10.0.2.1 (10.0.2.1): 56 data bytes
ping: sendto: Host is down
^C
--- 10.0.2.1 ping statistics ---
6 packets transmitted, 0 packets received, 100.0% packet loss
root@PC1:~ # ping 10.0.2.2
PING 10.0.2.2 (10.0.2.2): 56 data bytes
64 bytes from 10.0.2.2: icmp_seq=0 ttl=64 time=4.065 ms
64 bytes from 10.0.2.2: icmp_seq=1 ttl=64 time=0.369 ms
^C
--- 10.0.2.2 ping statistics ---
2 packets transmitted, 2 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.369/2.217/4.065/1.848 ms
```

```
root@PC1:~ # ping 10.0.2.3
PING 10.0.2.3 (10.0.2.3): 56 data bytes
64 bytes from 10.0.2.3: icmp_seq=0 ttl=64 time=0.378 ms
64 bytes from 10.0.2.3: icmp_seq=1 ttl=64 time=0.595 ms
^C
--- 10.0.2.3 ping statistics ---
2 packets transmitted, 2 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.378/0.487/0.595/0.109 ms
root@PC1:~ # ping 10.0.2.4
PING 10.0.2.4 (10.0.2.4): 56 data bytes
64 bytes from 10.0.2.4: icmp_seq=0 ttl=64 time=1.197 ms
64 bytes from 10.0.2.4: icmp_seq=1 ttl=64 time=0.744 ms
^C
--- 10.0.2.4 ping statistics ---
2 packets transmitted, 2 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.744/0.970/1.197/0.227 ms
```

10.0.2.1: Δεν έχει αποδοθεί, 10.0.2.2: Default Gateway (DHCP server), 10.0.2.3: name server, 10.0.2.4: TFTP server

5.9) Επικοινωνεί το νέο εικονικό μηχάνημα με τα άλλα δύο εικονικά μηχανήματα; Τεκμηριώστε την απάντησή σας. By default, στην δικτύωση "NAT" δεν υποστηρίζεται άμεση επικοινωνία μεταξύ δύο εικονικών μηχανών.

Ουστόσο με χρήση "port-forwarding" μπορούμε να διαχρίνουμε τις εικονικές μηχανές με βάση τη θύρα, παρόλο που έχουν ίδια IPv4.

5.10) Ποια η σημασία των παραμέτρων στην εντολή traceroute;

-I: Χρήση ICMP Echo Request αντί για δεδομενογράμματα UDP.

-n: Μη αντιστοίχιση των διευθύνσεων IPv4 σε hostnames.

-q: Αριθμός πακέτων για κάθε άλμα (hop).

5.11) Ποια είναι η διεύθυνση IPv4 πηγής: 10.0.2.15 και ποιος ο τύπος των μηνυμάτων ICMP που παράγει η traceroute, όπως αυτά εμφανίζονται στην καταγραφή του tcpdump;: ICMP Echo Request

```
21:42:09.450740 IP 10.0.2.15 > 1.1.1.1: ICMP echo request, id 33841, seq 1, ttl 28
```

5.12) Ποια είναι η διεύθυνση IPv4 πηγής των αντίστοιχων μηνυμάτων ICMP, όπως αυτά εμφανίζονται στην καταγραφή του Wireshark;: 192.168.1.138

| | | | | |
|-----------------------------|---------|------|------------------------|---------------------------------|
| 1 0.000000000 192.168.1.138 | 1.1.1.1 | ICMP | 62 Echo (ping) request | id=0x840c, seq=2/512, ttl=1 (no |
|-----------------------------|---------|------|------------------------|---------------------------------|

5.13) Ποιες είναι οι διευθύνσεις IPv4 πηγής των μηνυμάτων ICMP τύπου TTL exceeded in transit της καταγραφής στο Wireshark.: 192.168.1.254, 62.169.255.69, 62.169.252.250, 176.126.38.5

5.14) Ποια είναι η διεύθυνση IPv4 προορισμού των μηνυμάτων αυτών; 192.168.1.138

5.15) Ποιες είναι οι διευθύνσεις IPv4 πηγής των μηνυμάτων ICMP τύπου TTL exceeded in transit που εμφανίζονται στην καταγραφή του tcpdump; 10.0.2.2, 192.168.1.254, 62.169.255.59, 62.169.252.250, 176.126.38.5

5.16) Ποια είναι η διεύθυνση IPv4 προορισμού των μηνυμάτων αυτών; 10.0.2.15

5.17) Αντιστοιχούν ένα προς ένα τα μηνύματα TTL exceeded in transit των δύο καταγραφών;

Παρατηρούμε ότι τα μηνύματα “exceeded in transit” της καταγραφής του wireshark εμφανίζονται και στην καταγραφή του tcpdump. Ωστόσο παρατηρούμε ένα ακόμα μήνυμα “exceeded in transit” 10.0.2.2 > 10.0.2.15 που δεν υπάρχει στην καταγραφή του wireshark.

5.18) Αν εκτελέσετε την εντολή tracert -d 1.1.1.1 από το φιλοξενούν μηχάνημα, ποιο θα είναι το πλήθος των αναπηδήσεων (hops) που θα προκύψει, σε σχέση με αυτό που εμφάνισε η traceroute στο εικονικό μηχάνημα; Αιτιολογήστε. Παρατηρούμε ότι για το εικονικό μηχάνημα έχουμε ένα ακόμα hop. Αυτό το hop οφείλεται στην

```
root@PC:~ # traceroute -I -n -q 1 1.1.1.1
traceroute to 1.1.1.1 (1.1.1.1), 64 hops max, 48 byte packets
 1  10.0.2.2  0.634 ms
 2  192.168.1.254  5.049 ms
 3  62.169.255.59  22.983 ms
 4  *
 5  62.169.252.250  60.686 ms
 6  176.126.38.5  28.162 ms
 7  1.1.1.1  31.012 ms
```

μετάδοση του πακέτου από το default gateway στο εικονικό μηχάνημα μέσω των εικονικών καρτών δικτύου.

```
petrosrapto@petrosraptoAssistant:~$ traceroute -I -n -q 1 1.1.1.1
traceroute to 1.1.1.1 (1.1.1.1), 30 hops max, 60 byte packets
 1  192.168.1.254  7.932 ms
 2  62.169.255.59  25.121 ms
 3  *
 4  62.169.252.250  31.122 ms
 5  176.126.38.5  33.536 ms
 6  1.1.1.1  33.522 ms
```

Άσκηση 6: Δικτύωση NAT Network

6.1) Ποια είναι η διεύθυνση του δικτύου NAT που έχει οριστεί στο VirtualBox; 10.0.2.0/24

6.2) Στα PC1, PC2 διαγράψτε τη διεύθυνση IPv4 από την κάρτα δικτύου καθώς και το αρχείο /var/db/dhclient.leases.em0 με τα δάνεια που έχουν εκχωρηθεί.

```
root@PC1:~ # rm /var/db/dhclient.leases.em0
root@PC1:~ # ifconfig em0 delete
```

```
root@PC2:~ # ifconfig em0 delete
root@PC2:~ # rm /var/db/dhclient.leases.em0
```

6.3) Αποδώστε μέσω DHCP διευθύνσεις IPv4 στα εικονικά μηχανήματα PC1, PC2.

```
root@PC1:~ # dhclient em0
DHCPDISCOVER on em0 to 255.255.255.255 port 67 interval 6
DHCPoffer from 10.0.2.3
DHCPREQUEST on em0 to 255.255.255.255 port 67
DHCPACK from 10.0.2.3
bound to 10.0.2.15 -- renewal in 300 seconds.
```

```
root@PC2:~ # dhclient em0
DHCPDISCOVER on em0 to 255.255.255.255 port 67 interval 7
DHCPoffer from 10.0.2.3
DHCPREQUEST on em0 to 255.255.255.255 port 67
DHCPACK from 10.0.2.3
bound to 10.0.2.4 -- renewal in 300 seconds.
```

6.4) Ποιες διευθύνσεις αποδόθηκαν; Διαφέρουν από αυτές που είχαν τα PC1, PC2 προηγουμένως;

PC1: 10.0.2.15 (Ιδια με προηγουμένως), PC2: 10.0.2.4 (Όχι ίδια με προηγουμένως)

6.5) Ποια η διεύθυνση IPv4 του εξυπηρετητή DHCP; 10.0.2.3

6.6) Ποιο είναι το περιεχόμενο του αρχείου /etc/resolv.conf;

```
root@PC2:~ # cat /etc/resolv.conf
# Generated by resolvconf
search lan
nameserver 10.0.2.1
```

6.7) Ποια είναι η προεπιλεγμένη πύλη στον πίνακα δρομολόγησης; 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) Από τα εικονικά μηχανήματα PC1, PC2 μπορείτε να κάνετε ping στην IPv4 διεύθ. της προεπιλεγμένης πύλης; Ναι

```
root@PC1:~ # ping 10.0.2.1
PING 10.0.2.1 (10.0.2.1): 56 data bytes
64 bytes from 10.0.2.1: icmp_seq=0 ttl=255 time=0.374 ms
64 bytes from 10.0.2.1: icmp_seq=1 ttl=255 time=0.412 ms
64 bytes from 10.0.2.1: icmp_seq=2 ttl=255 time=0.798 ms
^C
--- 10.0.2.1 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.374/0.528/0.798/0.192 ms
```

```
root@PC2:~ # ping 10.0.2.1
PING 10.0.2.1 (10.0.2.1): 56 data bytes
64 bytes from 10.0.2.1: icmp_seq=0 ttl=255 time=0.622 ms
64 bytes from 10.0.2.1: icmp_seq=1 ttl=255 time=0.410 ms
^C
--- 10.0.2.1 ping statistics ---
2 packets transmitted, 2 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.410/0.516/0.622/0.106 ms
```

6.9) Από τα PC1, PC2 μπορείτε να κάνετε ping στην IPv4 διεύθυνση του εξυπηρετητή DHCP; Ναι

```
root@PC1:~ # ping 10.0.2.3
PING 10.0.2.3 (10.0.2.3): 56 data bytes
64 bytes from 10.0.2.3: icmp_seq=0 ttl=255 time=0.352 ms
64 bytes from 10.0.2.3: icmp_seq=1 ttl=255 time=0.375 ms
^C
--- 10.0.2.3 ping statistics ---
2 packets transmitted, 2 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.352/0.363/0.375/0.011 ms
```

```
root@PC2:~ # ping 10.0.2.3
PING 10.0.2.3 (10.0.2.3): 56 data bytes
64 bytes from 10.0.2.3: icmp_seq=0 ttl=255 time=0.856 ms
64 bytes from 10.0.2.3: icmp_seq=1 ttl=255 time=0.447 ms
^C
--- 10.0.2.3 ping statistics ---
2 packets transmitted, 2 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.447/0.651/0.856/0.204 ms
```

6.10) Από τα PC1, PC2 μπορείτε να κάνετε ping στη διεύθυνση 10.0.2.2; Ναι Ποιο μηχάνημα απαντά;

```
root@PC1:~ # ping 10.0.2.2
PING 10.0.2.2 (10.0.2.2): 56 data bytes
64 bytes from 10.0.2.2: icmp_seq=0 ttl=64 time=0.800 ms
64 bytes from 10.0.2.2: icmp_seq=1 ttl=64 time=0.574 ms
^C
--- 10.0.2.2 ping statistics ---
2 packets transmitted, 2 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.574/0.687/0.800/0.113 ms
root@PC1:~ # arp -a
? (10.0.2.15) at 08:00:27:d1:96:68 on em0 permanent [ethernet]
? (10.0.2.1) at 52:54:00:12:35:00 on em0 expires in 866 seconds [ethernet]
? (10.0.2.2) at 52:54:00:12:35:00 on em0 expires in 1196 seconds [ethernet]
? (10.0.2.3) at 08:00:27:82:56:fc on em0 expires in 579 seconds [ethernet]
```

Απαντά η προεπιλεγμένη πύλη.

6.11) Επικοινωνούν τα εικονικά μηχάνημα με το Internet; Τεκμηριώστε την απάντησή σας.

Τα μηχανήματα επικοινωνούν με το Internet καθώς έχουν με δικτύωση “NAT Network”.

```
root@PC1:~ # ping amazon.com
PING amazon.com (205.251.242.103): 56 data bytes
64 bytes from 205.251.242.103: icmp_seq=0 ttl=228 time=151.334 ms
64 bytes from 205.251.242.103: icmp_seq=1 ttl=228 time=150.729 ms
^C
--- amazon.com ping statistics ---
2 packets transmitted, 2 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 150.729/151.031/151.334/0.302 ms
```

6.12) Επικοινωνούν τα PC1, PC2 μεταξύ τους; Ναι αφού βρίσκονται στο ίδιο υποδίκτυνο.

```
root@PC2:~ # ping 10.0.2.15
PING 10.0.2.15 (10.0.2.15): 56 data bytes
64 bytes from 10.0.2.15: icmp_seq=0 ttl=64 time=0.866 ms
64 bytes from 10.0.2.15: icmp_seq=1 ttl=64 time=1.023 ms
^C
--- 10.0.2.15 ping statistics ---
2 packets transmitted, 2 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.866/0.944/1.023/0.079 ms
```

```
root@PC1:~ # ping 10.0.2.4
PING 10.0.2.4 (10.0.2.4): 56 data bytes
64 bytes from 10.0.2.4: icmp_seq=0 ttl=64 time=1.524 ms
64 bytes from 10.0.2.4: icmp_seq=1 ttl=64 time=0.701 ms
^C
--- 10.0.2.4 ping statistics ---
2 packets transmitted, 2 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.701/1.112/1.524/0.411 ms
```

6.13) Μπορείτε από το PC3 να κάνετε ping στα PC1, PC2; Όχι, δεν απαντάν τα PC1, PC2 (φαίνεται αν tcpdump στο PC1)

```
root@PC:~ # ping 10.0.2.15
PING 10.0.2.15 (10.0.2.15): 56 data bytes
64 bytes from 10.0.2.15: icmp_seq=0 ttl=64 time=0.055 ms
64 bytes from 10.0.2.15: icmp_seq=1 ttl=64 time=0.099 ms
^C
--- 10.0.2.15 ping statistics ---
2 packets transmitted, 2 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.055/0.077/0.099/0.022 ms
```

```
root@PC:~ # ping 10.0.2.4
PING 10.0.2.4 (10.0.2.4): 56 data bytes
64 bytes from 10.0.2.4: icmp_seq=0 ttl=64 time=0.579 ms
64 bytes from 10.0.2.4: icmp_seq=1 ttl=64 time=0.550 ms
^C
--- 10.0.2.4 ping statistics ---
2 packets transmitted, 2 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.550/0.565/0.579/0.014 ms
```

6.14) Εάν σε κάποιο από τα προηγούμενα ping λάβετε απάντηση είναι το αντίστοιχο PC που απαντά; Γιατί; Πώς μπορείτε να το διαπιστώσετε; Απαντά το PC3 στον εαυτό του και ο TFTP server (φαίνεται αν tcpdump στο PC1, PC2).