Ονοματεπώνυμο: Ιωάννης Γιαννούκος	**Όνομα PC:** John John
Ομάδα: 1	**Ημερομηνία:** 14/3/2023

Εργαστηριακή Άσκηση 2
Δικτύωση συστημάτων στο VirtualBox

Άσκηση 1

1.12) Το ιστορικό εντολών που έδωσα μέχρι αυτό το σημείο διαγράφεται με την εντολή "`history -c`".

Άσκηση 2

2.1) "`ifconfig`".

2.2) "`ifconfig em0 down`", "`ifconfig em0 up`", αντίστοιχα.

2.3) "`man tcpdump`", "`man pcap`", "`man pcap-filter`", αντίστοιχα.

2.4) "`tcpdump -i em0-n`".

2.5) Χρησιμοποιώ τις εξής εντολές για να συλλάβω όλα τα πλαίσια από την κάρτα δικτύου em0 και να εμφανίσω τα περιεχόμενά των σε:

-ASCII:

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

-Δεκαεξαδική μορφή:

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

2.6) "`tcpdump -e`".

2.7) "`tcpdump -s 68`" ή "`tcpdump -snapshot-length=68`".

2.8) "`tcpdump host 10.0.0.1 -v`"

2.9) "`tcpdump host (10.0.0.1 and 10.0.0.2) -i em0`"

2.10) "`tcpdump net 1.1 ip -x`"

2.11) `tcpdump not net 147.102.200.0 ip`

2.12) `tcpdump broadcast -n ip`

2.13) `tcpdump ip[2:2] > 576`

2.14) `tcpdump ip[8] < 5`

2.15) `tcpdump`

2.16) `tcpdump src 10.0.0.1 and icmp`

2.17) `tcpdump dst 10.00.0.2 and tcp`

2.18) `tcpdump dst port 53 and udp`

2.19) `tcpdump host 10.0.0.10 tcp ip`

2.20) `tcpdump host 10.0.0.10 and port 23 and -w sample_capture`

2.21) `tcpdump tcp[tcpflags] & tcp-syn != 0`

2.22) `tcpdump (tcp[tcpflags] & tcp-syn != 0) or (tcp[tcpflags] & (tcp-syn|tcp-ack) != 0)`

2.23) `tcpdump (tcp[tcpflags] & tcp-fin != 0) or (tcp[tcpflags] & tcp-fin|tcp-ack != 0)`

2.24) Η παράσταση αυτή ελέγχει αν τα 4 Most Significant Bits του byte12, δηλαδή το Data Offset, διαιρείται ακριβώς με το 4 χρησιμοποιώντας την πράξη '>> 2' (shift right logical 2 bits). Με αυτόν τον τρόπο μπορούμε να αποφανθούμε στο αν το TCP πακέτο φέρει Options ή όχι.
(Αν το Data Offset είναι μεγαλύτερο του 4, τότε το πακέτο φέρει Options, διαφορετικά όχι.

2.25) `tcpdump (tcp[12:1] & 0xf0 >> 2) > 5`

2.26) `tcpdump tcp port 80 -A`

2.27) `tcpdump udp port telnet and dst edu-dy.cn.ntua.gr`

2.28) `tcpdump ip6`

Άσκηση 3

3.1) Η διεύθυνση IPv4 του Host-only Ethernet adapter είναι 192.168.56.1.

3.2) Η διεύθυνση IPv4 του εξυπηρετητή DHCP για το δίκτυο Host-only είναι 192.168.56.100. Η περιοχή διευθύνσεων IPv4 που μπορεί να εκχωρήσει είναι από 192.168.56.101 έως 192.168.56.254.

3.3) Εκτελώντας την εντολή "`dhclient em0`" από κάθε εικονικό μηχάνημα αποδίδω διευθύνσεις IPv4 μέσω DHCP.

3.4) Οι διευθύνσεις IPv4 των 2 εικ. μηχανημάτων PC1, PC2 είναι 192.168.56.101 και 192.168.56.102, αντιστοίχως.

3.5) Για να διαπιστώσουμε ότι τα δύο μηχανήματα επικοινωνούν μεταξύ τους μπορούμε απλά να κάνουμε ping από το ένα στο άλλο. Παρατηρώ ότι το PC2 απαντά στο ping από το PC1.

3.6) Για να διαπιστώσουμε ότι τα δύο μηχανήματα επικοινωνούν με το φιλοξενούν μηχάνημα μπορούμε να κάνουμε ping από αυτό σε ένα εικ. μηχάνημα. Παρατηρώ ότι τα εικ. μηχανήματα απαντούν στα ping από το φιλοξενούν μηχάνημα.

3.7) Για να εμφανίσω την προεπιλεγμένη πύλη εκτελώ την εντολή "`netstat -r`".

3.8) Όχι, δεν υπάρχει προεπιλεγμένη πύλη στην περίπτωση Host-only, καθώς η επικοινωνία των PC1 και PC2 γίνεται μόνο μεταξύ αυτών και του φιλοξενούν μηχανήματος, και δεν υπάρχει επικοινωνία με εξωτερικά συστήματα.

3.9) Όχι, το φιλοξενούν μηχάνημα δεν απαντά στα pings των PC1, PC2. Αυτό συμβαίνει επειδή το φιλοξενούν μηχάνημα επικοινωνεί με μία ξεχωριστή εικονική διεπαφή για κάθε υποδίκτυο Host-only, δηλαδή η φυσική κάρτα δικτύου δεν είναι reachable από τα PC1, PC2. Ωστόσο, αν κάνουμε ping από τα φιλοξενούμενα μηχανήματα στην εικονική διεπαφή που ορίζουμε μέσω του Virtual-Box, βλέπουμε ότι το φιλοξενούν μηχάνημα απαντά.

3.10) Το όνομα των μηχανημάτων όπως το αντιλαμβάνονται τα ίδια είναι "PC.ntua.lab", το οποίο το βλέπουμε εκτελώντας την εντολή "`hostname`".

3.11) Αλλάζω τα ονόματα των εικονικών μηχανημάτων σε PC1 και PC2 με τις εντολές "`hostname PC1`" και "`hostname PC2`", αντίστοιχα.

3.12) Μπορώ να επιβεβαιώσω την αλλαγή του ονόματος από την προτροπή που εμφανίζεται πλέον (root@PC1) (root@PC2).

3.13) Όχι, το αρχείο /etc/rc.conf δεν περιέχει το νέο όνομα, επομένως όταν γίνει επανεκκίνηση του μηχανήματος θα δοθεί πάλι το παλιό όνομα.

3.14) Απλά αλλάζουμε το όνομα που αναφέρεται στο αρχείο /etc/rc.conf σε PC1 και PC2 για τα αντίστοιχα μηχανήματα.

3.15) Για να χρησιμοποιούμε τα ονόματα των μηχανημάτων έναντι των IPv4 διευθύνσεών τους προσθέτουμε στο αρχείο /etc/hosts την γραμμή [IPv4 address] [όνομα μηχανήματος]. Αναλυτικότερα:

- Στο PC1:
  192.168.56.102 PC2
- Στο PC2:
  192.168.56.101 PC1

3.16) Ένα παράδειγμα που χρησιμοποιούμε τα ονόματα αντί των διευθύνσεων είναι η εντολή "`ping PC1`" ή "`ping PC2`".

3.17) Από το PC2 μηχάνημα εκτελώ μία εκ των δύο παρακάτω εντολών, με την οποίες μπορώ να συλλαμβάνω πακέτα που προέρχονται από το PC1 και να τα εμφανίζω στην οθόνη καθώς και να τα καταγράφω σε αρχείο με όνομα test.

1ος τρόπος: `tcpdump host PC1 -l | tee test`
2ος τρόπος: `tcpdump host 192.168.56.101 -l | tee test`

3.18) Από τον φλοιό του PC1 βλέπουμε ότι το PC1 λαμβάνει πακέτα των 64 bytes με τιμή TTL = 64.

3.19) Κάνοντας ping από το μηχάνημα PC1, η απάντηση που λαμβάνει από το φιλοξενούν μηχάνημα έχει τιμή TTL = 128.

3.20) Για να λαμβάνω μόνο πακέτα ICMP και να τα εμφανίζω με όσο το δυνατόν περισσότερες λεπτομέρειες εκτελώ την εντολή:
`tcpdump icmp -vvv -l`

3.21) Το μήκος των πακέτων ICMP που στέλνει το φιλοξενούν μηχάνημα είναι 32 bytes. Αυτή η διαφορά είναι λογική, αφού κάθε λειτουργικό

σύστημα έχει διαφορετικές προκαθορισμένες τιμές για διαδικασίες όπως αυτή του pinging.

3.22) Η τιμή TTL των πακέτων ICMP είναι 64, τιμή που συμφωνεί με αυτήν της προηγούμενης περίπτωσης.

3.23) Όχι, δεν παρατηρούμε κάποια κίνηση από το μηχάνημα PC1.

3.24) Ναι, πλέον παρατηρούμε ότι το PC1 καταγράφει οποιαδήποτε κίνηση στο δίκτυο, ανεξαρτήτως της διεύθυνσης προορισμού των πακέτων.

Άσκηση 4

4.1) Για να ορίσω στατικές διευθύνσεις IPv4 στα PCi (i=1,2) χρησιμοποίησα τις εντολές: "`ifconfig em0 inet 192.168.56.10i`"

4.2) Το μήνυμα λάθους που εμφανίστηκε σήμανε την διακοπή της σύνδεσης των μηχανημάτων με τον DHCP server που υπήρχει προηγουμένως.

4.3) Ξεκινώ μια καταγραφή με εμφάνιση λεπτομερειών στο PC1 με την εντολή: "`tcpdump -vvv -l | tee log`".

4.4) Όχι, δεν είναι πλέον δυνατό να κάνουμε ping από το φιλοξενούν στο PC2 μηχάνημα.

4.5) Όχι, δεν παρατηρείται από το PC1 κίνηση σχετική με το ping στο PC2.

4.6) Όχι, δεν μπορώ να κάνω ping από το PC2 στο PC1.

4.7) Όχι, δεν παρατηρείται κίνηση σχετική με το ping του ερωτήματος (4.6).

4.8) Ναι, πλέον υπάρχει επικοινωνία μεταξύ των εικ. μηχανημάτων PCi.

4.9) Όχι, το φιλοξενούν μηχάνημα δεν μπορεί να επικοινωνήσει με κανένα από τα δύο εικ. μηχανήματα, καθώς αυτά βρίσκονται σε Internal Networking, στο οποίο όλα τα εικ. μηχανήματα έχουν δυνατότητα επικοινωνίας μόνο μεταξύ τους (τουλάχιστον αυτά που βρίσκονται στο ίδιο εσωτερικό δίκτυο).

4.10) Ξεκινώ μία νέα καταγραφή στο PC1 χωρίς επίλυση διευθύνσεων IPv4 σε ονόματα εκτελώντας την εντολή: "`tcpdump -n`".

4.11) Αδειάζω τον πίνακα arp του PC2 εκτελώ την εντολή "`arp -d -a`". Κάνω ping προς την IPv4 διεύθυνση της εικονικής κάρτας του φιλοξενούντος μηχανήματος εκτελώντας την εντολή:
"`ping 192.168.56.1`". Στην καταγραφή του PC1 παρατηρώ πακέτα ARP με τα οποία γίνεται εμφανές ότι το PC2 αναζητά το μηχάνημα που έχει την διεύθυνση 192.168.56.1.

4.12) Αφού δεν λαμβάνει οποιαδήποτε απάντηση στα προηγούμενα πακέτα ARP που έστειλε το PC2, θεωρεί πλέον ότι ο host δεν λειτουργεί αυτήν τη στιγμή, και έτσι, λογικώς, εμφανίζει το μήνυμα "host is down".

4.13) Για να αλλάξω τις διευθύνσεις IPv4 των εικ. μηχανημάτων στις τελευταίες 2 διευθύνσεις τους υποδικτύου 10.11.12.0/26 εκτελώ τις εντολές:

- PC1: `ifconfig em0 inet 10.11.12.62`
- PC2: `ifconfig em0 inet 10.11.12.63`

4.14) Ναι, τα δύο εικ. μηχανήματα τώρα επικοινωνούν με τις μόλις δοσμένες διευθύνσεις IPv4.

Άσκηση 5

5.1) Αποδίδω διευθύνσεις IPv4 σε κάθε μηχάνημα εκτελώντας την εντολή "`dhclient em0`" σε κάθε μηχάνημα.

5.2) Όλα τα εικ. μηχανήματα έχουν λάβει IPv4 διεύθυνση 10.0.2.15 από την 10.0.2.2, η οποία είναι η διεύθυνση της προκαθορισμένης πύλης.

5.3) Η προεπιλεγμένη πύλη έχει διεύθυνση IPv4 10.0.2.2.

5.4) Το περιεχόμενο του αρχείο /etc/resolv.conf είναι οι εξής 3 γραμμές:

```
# Generated by resolvconf
search home
nameserver 192.168.1.1
```

5.5) Η διεύθυνση IPv4 που αποδόθηκε μέσω HDCP και επιπλέον πληροφορίες που περιέχει το αρχείο resolv.conf έχουν αποθηκευτεί στο αρχείο /var/db/dhclient.leases.em0.

5.6) Ναι, το pinging από τα εικ. μηχανήματα είναι δυνατό προς την διεύθυνση της προκαθορισμένης πύλης.

5.7) Ναι, το νέο εικ. μηχάνημα PC3 έχει επικοινωνία με το Internet (κάνοντας ping στην διεύθυνση της σελίδας amazon.com το PC3 δέχεται απάντηση).

5.8) Απάντηση λαμβάνεται σε ping προς οποιαδήποτε διεύθυνση μεταξύ των 10.0.2.2, 10.0.2.3, 10.0.2.4, και δεν λαμβάνεται απάντηση από την 10.0.2.1 (διεύθυνση που δεν αποδίδεται by default κάπου).
Οι διευθύνσεις αυτές αντιστοιχίζονται με ορισμένους servers, όπως φαίνεται παρακάτω:

- 10.0.2.2 : προκαθορισμένη πύλη (default gateway)
- 10.0.2.3 : Proxy DNS server
- 10.0.2.4 : TFTP Server

5.9) Όχι, το νέο εικ. μηχάνημα PC3 δεν επικοινωνεί με τα 2 άλλα PC1, PC2 (τουλάχιστον προς το παρόν). Σε δικτύωση NAT κάθε εικ. μηχάνημα έχει την εντύπωση ότι βρίσκεται σε δικό του ξεχωριστό δίκτυο. (Εάν θέλουμε να επιτρέψουμε στα εικ. μηχανήματα PC1, PC2, PC3 την επικοινωνία μεταξύ τους, θα χρειαστεί να χρησιμοποιήσουμε Port Forwarding κ.ά., πράγμα που θα περιπλέξει πολύ την διαδικασία).

5.10) Για να ξεκινήσω καταγραφή των ICMP πακέτων που διέρχονται από την διεπαφή em0 του PC3 εκτελώ την εντολή:
“`tcpdump -n -i em0 -w data icmp`”.
Οι επιλογή -I εισάχθηκε για χρήση ICMP πακέτων (αντί για δεδομενογράμματα UDP), η επιλογή -n εισάχθηκε για εκτύπωση των αποτελεσμάτων (αριθμητικά και όχι «συμβολικά») και η επιλογή -q 1 επιλέχθηκε για να χρησιμοποιηθεί 1 probe ανά βήμα.

5.11) Στην καταγραφή που έγινε από την εντολή `tcpdump` φαίνεται ότι η διεύθυνση προορισμού είναι 10.0.2.15 και ο τύπος πακέτων ICMP είναι ICMP echo request.

5.12) Στην καταγραφή που έγινε από το Wireshark φαίνεται ότι η διεύθυνση προορισμού είναι 192.168.1.3 (η διεύθυνση IPv4 του υπολογιστή μου στο οικιακό μου δίκτυο).

5.13) Οι διευθύνσεις IPv4 πηγής των μηνυμάτων ICMP τύπου TTL exceeded in transit από την καταγραφή του Wireshark φαίνεται να είναι (με χρονική σειρά):

192.168.1.1,
80.106.125.100,
79.128.226.161,
79.128.226.98,
79.128.227.227,
176.128.38.5.

5.14) Η διεύθυνση IPv4 προορισμού όλων των παραπάνω (5.13) μηνυμάτων είναι η 192.168.1.3 (η διεύθυνση IPv4 του υπολογιστή μου στο οικιακό μου δίκτυο).

5.15) Οι διευθύνσεις IPv4 πηγής των μηνυμάτων ICMP τύπου TTL exceeded in transit από την καταγραφή του `tcpdump` φαίνεται να είναι (με χρονική σειρά):

10.0.2.2
H1600V7.home
80.106.125.100
79.128.226.161
98.226.128.79
79.128.227.227
5.38.126.176

5.16) Η διεύθυνση IPv4 προορισμού όλων των παραπάνω (5.15) μηνυμάτων είναι 10.0.2.15 (η διεύθυνση IPv4 του εικ. μηχανήματος PC3).

5.17) Ναι, φαίνεται να υπάρχουν αντιστοιχίες σε μεγάλο βαθμό στις διευθύνσεις αυτές, με εξαίρεση την πρώτη διεύθυνση και λίγες ακόμα στη συνέχεια.

5.18) Το πλήθος των αναπηδήσεων (hops) που θα προκύψει από την εντολή `tracert -d 1.1.1.1` από το φιλοξενούν μηχάνημά μου θα είναι πάντα μεγαλύτερο κατά ένα από αυτό που θα προκύψει από την traceroute στο εικ. μηχάνημα. Αυτό είναι πολύ λογικό, επειδή το εικ. μηχάνημα θα βρίσκεται πάντα 1 hop μακριά από το φιλοξενούν, και κάθε επικοινωνία του εικ. μηχανήματος θα γίνεται πάντα μέσω του φιλοξενούντος.

Άσκηση 6

6.1) Το υποδίκτυο NAT που έχει οριστεί στο VirtualBox έχει διεύθυνση 10.0.2.0/24.

6.2) Διαγράφω τις διευθύνσεις IPv4 από τις κάρτες δικτύου των PC1, PC2 καθώς και το αρχείο /var/dbdhclient.leases.em0 στα 2 εικ. μηχανήματα με την εντολή: "`ifconfig em0 delete`".

6.3) Αποδίδω διευθύνσεις IPv4 μέσω DHCP στα PC1, PC2 με την εντολή "`dhclient em0`".

6.4) Στο PC1 αποδόθηκε η διεύθυνση 10.0.2.15, δηλαδή η διεύθυνσή του δεν άλλαξε. Στο PC2 αποδόθηκε η διεύθυνση 10.0.2.4, επομένως η διεύθυνσή του άλλαξε.

6.5) Η διεύθυνση IPv4 του DHCP Server είναι 10.0.2.3.

6.6) Το περιεχόμενο του αρχείο /etc/resolv.conf είναι οι εξής 3 γραμμές:

```
# Generated by resolvconf
search home
nameserver 192.168.1.1
```

Στο αρχείο αυτό θα αποθηκεύονται οι DNS αντιστοιχίες.

6.7) Η προεπιλεγμένη πύλη στον πίνακα δρομολόγησης έχει διεύθυνση 10.0.2.1.

6.8) Ναι, μπορώ να κάνω ping από τα εικ. μηχανήματα PC1, PC2 στην προεπιλεγμένη πύλη.

6.9) Ναι, μπορώ να κάνω ping από τα εικ. μηχανήματα PC1, PC2 στον εξυπηρετητή DHCP.

6.10) Ναι, μπορώ να κάνω ping από τα PC1, PC2 στη διεύθυνση 10.0.2.2. Το μηχάνημα που απαντά είναι το φιλοξενούν (έχει διεύθυνση 10.0.2.2, όπως και 10.0.2.1).

6.11) Ναι, τα εικ. μηχανήματα έχουν επικοινωνία με το Internet, μέσω φυσικά του φιλοξενούντος μηχανήματος. Αυτό μπορεί να διαπιστωθεί αν κάνουμε ping από εικ. μηχάνημα σε εξωτερική διεύθυνση IP, πράγμα που θα επιτύχει.

6.12) Ναι, τα εικ. μηχανήματα PC1, PC2 επικοινωνούν μεταξύ τους στην Δικτύωση NAT Network. Αυτό μπορεί να διαπιστωθεί αν κάνουμε ping από ένα εικ. μηχάνημα στο άλλο, πράγμα που θα επιτύχει.

6.13) Όχι, δεν μπορώ να κάνω ping από το PC3 στα PC1, PC2. Αυτό συμβαίνει επειδή το PC3 βρίσκεται σε δικτύωση NAT, η οποία δίνει την αίσθηση ότι το PC3 βρίσκεται σε ξεχωριστό δικό του δίκτυο. Επομένως, παρόλο που τα PC1, PC2 δεν βρίσκονται σε NAT δικτύωση, εξακολουθεί η επικοινωνία μεταξύ τους να μην είναι δυνατή.

6.14) Ναι, απάντηση σε κάποιο από τα προηγούμενα ping θα προέρχεται από το αντίστοιχο PC, καθώς σε δικτύωση NAT Network κάθε εικ. μηχάνημα έχει ξεχωριστή IP διεύθυνση.