Ονοματεπώνυμο: Μάρκος Δεληγιάννης	Όνομα PC: Lenovo-Laptop
Ομάδα: 1	Ημερομηνία: 7 / 3 / 2023

Εργαστηριακή Άσκηση 2
Δικτύωση συστημάτων στο VirtualBox

Απαντήστε στα ερωτήματα στον χώρο που σας δίνεται παρακάτω και στην πίσω σελίδα εάν δεν επαρκεί. Το φυλλάδιο αυτό θα παραδοθεί στον επιβλέποντα.

2

2.1 Εντολή: **ifconfig**

2.2 Εντολές: 1) **ifconfig em0 down** 2) **ifconfig em0 up**

2.3 Εντολές: 1) **man tcpdump** 2) **man pcap** **3**) **man pcap-filter**

2.4 Εντολή: **tcpdump -i em0 -n**

2.5 Εντολή: **tcpdump -i em0 -XX**

2.6 Εντολή: **tcpdump -e**

2.7 Εντολή: **tcpdump -i em0 -s 68 -e**

2.8 Εντολή: **tcpdump -v 'host 10.0.0.1'**

2.9 Εντολή: **tcpdump -i em0 'host 10.0.0.1 and 10.0.0.2'**

2.10 Εντολή: **tcpdump -X 'dst net 1.1.0.0/16'**

2.11 Εντολή: **tcpdump -e 'ip and not net 192.168.1.0/24'**

2.12 Εντολή: **tcpdump 'ip and broadcast'**

2.13 Εντολή: **tcpdump 'ip and len > 576'** (Μετρώντας και τις Ethernet επικεφαλίδες)

2.14 Εντολή: **tcpdump 'ip[8] < 5'**

2.15 Εντολή: **tcpdump 'ip[0] & 0xf > 5'**

2.16 Εντολή: **tcpdump 'icmp and src 10.0.0.1'**

2.17 Εντολή: **tcpdump 'tcp and dst 10.0.0.2'**

2.18 Εντολή: **tcpdump 'udp and dst port 53'**

2.19 Εντολή: **tcpdump 'tcp and host 10.0.0.10'**

2.20 Εντολή: **tcpdump -w "sample_capture" 'tcp and host 10.0.0.10 and dst port 23'**

2.21 Εντολή: **tcpdump 'tcp[tcpflags] == tcp-syn'**

2.22 Εντολή: **tcpdump 'tcp[tcpflags] & tcp-syn != 0'**

2.23 Εντολή: **tcpdump 'tcp[tcpflags] & tcp-fin != 0'**

2.24 Λαμβάνει τα 4MSBits του byte #12 (data offset) του TCP segment και τα ολισθαίνει 2 bits προς τα δεξιά. Αυτό ισοδυναμεί με πολλαπλασιασμό του data offset επί 4, το οποίο ισούται με το μήκος της επικεφαλίδας TCP σε byte (αφού το data offset μετρά 32bit λέξεις).

2.25 Εντολή: **tcpdump '((tcp[12] & 0xf0) >> 4) > 5'**

2.26 Εντολή: **tcpdump -A 'tcp port 80'**

2.27 Εντολή: **tcpdump 'tcp port 23 and dst host edu-dy.cn.ntua.gr'**

2.28 Εντολή: **tcpdump 'ip6'**

3

3.1 **192.168.56.1** (με ctrl+h)

3.2 IPv4 διεύθυνση DHCP: **192.168.56.100**
Περιοχή διευθύνσεων: **192.168.56.101 – 192.168.56.254**

3.3 Εντολή: **dhclient em0**

3.4 Διεύθυνση **192.168.56.103** στο **PC1** και **192.168.56.104** στο **PC2**. Η πληροφορία αυτή εμφανίζεται στο terminal με την εκτέλεση της εντολής **dhclient em0**.

3.5 Συνδεόμαστε στο PC2 από το PC1 με χρήση ssh. Στην κονσόλα του PC2 εμφανίζεται σχετική πληροφορία, επιβεβαιώνοντας ότι αυτό είναι το μηχάνημα στο οποίο συνδεθήκαμε. Εντολή: **ssh lab@192.168.56.104**

3.6 Πλήρως αντίστοιχα με το 3.5. Εντολές: **ssh lab@192.168.56.103** και **ssh lab@192.168.56.104**.

3.7 Εντολή: **netstat -4r** και αναζήτηση της σημαίας G (αντιστοιχεί σε gateway).

3.8 Δεν βρίσκουμε καταχώρηση με τη σημαία G, οπότε **δεν υπάρχει**. Αυτό είναι αναμενόμενο, καθώς στην δικτύωση Host-only το δίκτυο δεν επικοινωνεί με εξωτερικά μηχανήματα και συνεπώς δεν υπάρχει ανάγκη για default gateway.

3.9 **Όχι**, δεν μπορούμε, καθώς όπως προαναφέραμε το δίκτυο δεν επικοινωνεί με εξωτερικά μηχανήματα, οπότε δεν υπάρχει default gateway. Συνεπώς, τα εικονικά μηχανήματα δεν γνωρίζουν πώς να προωθήσουν τα πακέτα στην φυσική κάρτα δικτύου του φιλοξενούντος μηχανήματος.

3.10 **PC.ntua.lab**. Εντολή: **hostname**

3.11 Εντολή: **hostname PC1** (και PC2 αντίστοιχα)

3.12 Το prompt πλέον είναι **root@PC1** και **root@PC2 αντίστοιχα**.

3.13 **Όχι**, δεν το περιέχει, αλλά περιέχει το παλιό όνομα **PC.ntua.lab** (hostname="PC.ntua.lab"). Συνεπώς κατά την επανεκίνηση το όνομα του PC1 θα ξαναγίνει PC.ntua.lab.

3.14 Εντολές: 1) **vi /etc/rc.conf** 2) **:%s /PC.ntua.lab/PC1.ntua.lab/ g** (αντ. για PC2) 3) **:wq**

3.15 Προσθέτουμε και στα δύο μηχανήματα κάτω από τις καταχωρήσεις για το localhost τις εξής γραμμές: 1) **192.168.56.103 PC1** και 2) **192.168.56.104 PC2**

3.16 Εντολή: **ssh lab@PC2**

3.17 1ος τρόπος: **tcpdump -l 'host PC1' | tee tcpdump_res**
2ος τρόπος: **tcpdump -l 'host PC1' > tcpdump_res & tail -f tcpdump_res**

3.18 Το μήκος των μηνυμάτων ICMP echo reply είναι **64 bytes** και η τιμή του TTL είναι **64**.

3.19 Το TTL έχει τιμή **128**.

3.20 Εντολή: **tcpdump -vvvX 'icmp'**

3.21 Το μήκος των μηνυμάτων ICMP που παράγει το φιλοξενούν μηχάνημα είναι 40. Η διαφορά οφείλεται στο ότι η ping εκτελέστηκε από διαφορετικό ΛΣ (w11), το οποίο έχει διαφορετικές προεπιλογές.

3.22 Το TTL έχει τιμή **128** για τα μηνύματα ICMP echo request και τιμή **64** για τα μηνύματα ICMP echo reply. Αυτά βρίσκονται σε συμφωνία με τα προηγούμενα, καθώς τα μηνύματα ICMP που στέλνουν τα w11 έχουν TTL 128, ενώ τα μηνύματα που προέρχονται από freeBSD έχουν TTL 64.

3.23 **Όχι**, δεν παρατηρούμε σχετική κίνηση, θα μπορούσαμε όμως να παρατηρήσουμε ARP request από το φιλοξενούν για τη MAC του PC2, τα οποία είναι broadcast.

3.24 Σε αντίθεση με το 3.23 τώρα **μπορούμε να δούμε όλα τα ανταλλασσόμενα μηνύματα** μεταξύ του PC2 και του φιλοξενούντος μηχανήματος. Αυτό είναι λογικό, καθώς προηγουμένως τα Ethernet πλαίσια (που δεν προορίζονται για τον PC1) απορρίπτονταν, ενώ τώρα όχι, αφού έχουμε ενεργοποιήσει το promiscuous mode.

4

4.1 Εντολές: **ifconfig em0 192.168.56.103/24** για το PC1
ifconfig em0 192.168.56.104/24 για το PC2

4.2 Μήνυμα λάθους: **My address ([addr]) was deleted, dhclient exiting**. Αυτό σημαίνει ότι αναθέσαμε στατικά διεύθυνση σε διεπαφή που είχε ήδη λάβει αύτοματα διεύθυνση μέσω DHCP, με αποτέλεσμα να μην έχει νόημα η περαιτέρω χρήση του DHCP και άρα ο client να τερματίσει.

4.3 Εντολή: **tcpdump -vvvX**

4.4 **Όχι**, δεν μπορούμε.

4.5 **Ναι**, παρατηρούμε πακέτα ARP που αφορούν την IPv4 του PC2. Εντολή: **ping 192.168.56.104**

4.6 **Όχι**, δεν μπορούμε. Εντολή: **ping PC1**

4.7 **Όχι**, δεν παρατηρούμε.

4.8 **Ναι**, τώρα τα δύο μηχανήματα επικοινωνούν.

4.9 **Όχι**, δεν μπορούμε. Αυτό είναι αναμενόμενο, καθώς η τοπολογία “internal network” απομονώνει τα εικονικά μηχανήματα από το φιλοξενούν.

4.10 Εντολή: **tcpdump -n**

4.11 Εντολές: 1) **arp -da** 2) **ping 192.168.56.1**
Στην καταγραφή του PC1 παρατηρούμε μηνύματα **ARP request** από το PC2.

4.12 Η ping επιστρέφει μήνυμα *host is down* επειδή δεν ελήφθη απάντηση στα μηνύματα ARP request του PC2, οπότε δεν είναι γνωστή η MAC διεύθυνση στην οποία πρέπει να προωθηθούν τα μηνύματα ICMP.

4.13 Εντολές: **ifconfig em0 10.11.12.61/26** (PC1)
ifconfig em0 10.11.12.62/26 (PC2)

4.14 Αν χρησιμοποιήσουμε τις εντολές **ping PC1** και **ping PC2** προφανώς τα μηχανήματα δεν μπορούν να επικοινωνήσουν, αφού δεν έχουμε ενημερώσει τα αρχεία /etc/hosts. Οι ακόλουθες όμως εντολές **λειτουργούν**:
ping 10.11.12.61 και **ping 10.11.12.62**.

5

5.1 Εντολή: **dhclient em0**

5.2 Όλα έλαβαν τη διεύθυνση **10.0.2.15** από τον DHCP server **10.0.2.2**.

5.3 Η προεπιλεγμένη πύλη είναι ο **10.0.2.2**. Εντολή: **netstat -r** και αναζήτηση της σημαίας G.

5.4 Περιεχόμενο: **nameserver 192.168.1.254**

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

5.6 **Ναι**, μπορούμε.

5.7 **Ναι**, επικοινωνεί. Εκτελούμε την εντολή: **ping 1.1.1.1** και λαμβάνουμε απάντηση. Αυτό είναι αναμενόμενο από τη θεωρία για την τοπολογία NAT.

5.8 Λαμβάνουμε απάντηση από την 10.0.2.4, η οποία αντιστοιχεί στον εξυπηρετητή tftp του VirtualBox, και όχι από την 10.0.2.1, η οποία δεν αντιστοιχεί σε κάτι.

5.9 **Όχι**, δεν επικοινωνεί. Γνωρίζουμε από θεωρία ότι στην τοπολογία NAT τα εικονικά μηχανήματα δεν επικοινωνούν μεταξύ τους (χωρίς port forwarding). Αυτό επιβεβαιώνεται από το γεγονός ότι σε όλα έχει αποδοθεί η ίδια διεύθυνση IPv4, οπότε δεν υπάρχει καν διεύθυνση που να μπορούμε να θέσουμε στην εντολή ping.

5.10 **-I**: χρήση μηνυμάτων ICMP echo request αντί για UDP datagrams.
-n: εμφανίζονται μόνο οι IP διευθύνσεις των ενδιάμεσων διεπαφών, χωρίς να γίνεται αναζήτηση των ονομάτων τους
-q 1: γίνεται 1 probe ανά hop, αντί για 3, που είναι το default.

5.11 IPv4 διεύθυνση πηγής: **10.0.2.15** Τύπος μηνυμάτων ICMP: **ICMP echo request**

5.12 Η διεύθυνση IPv4 πηγής είναι τώρα η **192.168.1.13**, δηλαδή η διεύθυνση της φυσικής κάρτας δικτύου. Αυτό οφείλεται στο NAT.

5.13 1) 192.168.1.254 2) 62.169.255.59 3) 62.169.252.250 4) 176.126.38.5

5.14 **192.168.1.13**, δηλαδή η διεύθυνση IPv4 της φυσικής κάρτας δικτύου του υπολογιστή μας.

5.15 1) 10.0.2.2 2) 192.168.1.254 3) 62.169.255.59 4) 62.169.252.250 5) 176.126.38.5

5.16 Η διεύθυνση προορισμού είναι η **10.0.2.15**, δηλαδή η διεύθυνση της εικονικής διεπαφής του VM.

5.17 Τα μηνύματα TTL exceeded in transit είναι 4 ως προς το φιλοξενούν μηχάνημα και 5 ως προς το εικονικό. Εντούτοις, τα μηνύματα #2-#5 του εικονικού μηχανήματος αντιστοιχούν ένα προς ένα στα μηνύματα του φιλοξενούντος, με μόνη ουσιαστική διαφορά την IP διεύθυνση προορισμού, η οποία οφείλεται στο NAT. Το πρώτο μήνυμα που παρατηρούμε στην καταγραφή του tcpdump προέρχεται από το VirtualBox, για αυτό και δεν εντοπίζεται στην καταγραφή του wireshark.

5.18 Αναμένουμε να προκύψει πλήθος hops κατά ένα μικρότερο από αυτό της traceroute, καθώς τα πακέτα από το VM περνάνε από το φιλοξενούν μηχάνημα ως ενδιάμεσο κόμβο και έπειτα, λόγω του NAT, δεν διαφέρουν σε τίποτα από τα πακέτα τα οποία παράγονται από αυτό. Πράγματι εκτελώντας την εντολή τα παραπάνω επιβεβαιώνονται.

6

6.1 Διεύθυνση δικτύου: **10.0.2.0/24**

6.2 Εντολές: 1) **ifconfig em0 delete** 2) **rm /var/db/dhclient.leases.em0**

6.3 Εντολή: **dhclient em0**

6.4 PC1: **10.0.2.15** PC2: **10.0.2.4** Διαφέρουν με αυτές που είχαν προηγουμένως.

6.5 Διεύθυνση εξυπηρετητή DHCP: **10.0.2.3**

6.6 Περιεχόμενο: **nameserver 192.168.1.254**

6.7 Default gateway: **10.0.2.1** Εντολή: **netstat -4r** (εστιάζουμε στην καταχώρηση με τη σημαία G)

6.8 **Ναι**, μπορούμε. Εντολή: **ping 10.0.2.1**

6.9 **Ναι**, μπορούμε. Εντολή: **ping 10.0.2.3**

6.10 **Ναι**, μπορούμε. Εντολή: **ping 10.0.2.2**
Από τον πίνακα arp φαίνεται ότι το μηχάνημα που απαντά ταυτίζεται με τον default gateway (έχουν την ίδια MAC address), δηλαδή το φιλοξενούν. Εντολή: **arp -a**

6.11 **Ναι**, επικοινωνούν. Εντολή: **ping 1.1.1.1** (λαμβάνουμε απάντηση)

6.12 **Ναι**, επικοινωνούν. Εντολή: **ssh lab@10.0.2.15** (από το PC2, αντίστοιχα από το PC1)

6.13 **Όχι**, δεν μπορούμε. Αυτό είναι αναμενόμενο, καθώς το PC3 βρίσκεται σε διαφορετικό δίκτυο από τα PC1 και PC2, και δεν έχουμε κάνει port forwarding στο δίκτυο των PC1 και PC2.

6.14 **Όχι**, δεν είναι. Στο υποδίκτυο των PC1 και PC2 τυχαίνει το PC1 να έχει τη διεύθυνση 10.0.2.15, η οποία είναι αυτή που αποδίδεται πάντα στα μηχανήματα στην τοπολογία NAT. Έτσι, αν εκτελέσουμε **ping 10.0.2.15** από το PC3 ουσιαστικά θα κάνουμε ping στο ίδιο το PC3. Μπορούμε να επαληθεύσουμε τα παραπάνω εκτελώντας **tcpdump 'icmp'** στο PC1 όσο το PC3 εκτελεί την ping **με επιτυχία** και να παρατηρήσουμε ότι η tcpdump δεν ανιχνεύει κανένα μήνυμα ICMP. Αντίστοιχες παρατηρήσεις ισχύουν για το 10.0.2.4, το οποίο (ως προς τον PC3) είναι ο tftp server του VirtualBox.