Ονοματεπώνυμο: Μάρκος Δεληγιάννης	Όνομα PC: Lenovo-Laptop
Ομάδα: 1	Ημερομηνία: 28 / 3 / 2023

Εργαστηριακή Άσκηση 5
Στατική δρομολόγηση

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

1

1.1 Εντολές: **ifconfig em0 [IPv4 addr/24]** σε PC1, PC2 και R1 – LAN1
ifconfig em1 [IPv4 addr/24] σε R1 – LAN2

1.2 **gateway_enable="YES"**

1.3 Εντολή: **route add -net 192.168.2.0/24 192.168.1.1**

1.4 Εντολή: **netstat -4r**. Έχουμε τις σημαίες **U = up / ενεργή, G = gateway / πύλη, S = static / στατική**

1.5 Το ping **αποτυγχάνει**, καθώς δεν λαμβάνουμε **καμία απάντηση**, ούτε κάποιο μήνυμα στο terminal. Εντολή: **ping 192.168.2.2**

1.6 Παρατηρούμε **μόνο πακέτα ICMP echo request και στα δύο LAN**. Αυτό συμβαίνει διότι ο PC2 δεν έχει κατάλληλη εγγραφή στο routing table του για τον PC1. Έτσι, τα πακέτα ICMP echo request προωθούνται από τον PC1 στον R1 (χάρη στην εγγραφή του 1.3) και έπειτα στο LAN2 (χάρη στην εγγραφή του 1.2), αλλά ο PC2 δεν γνωρίζει πώς να προωθήσει τα ICMP echo reply στον PC1. Εντολές: **tcpdump -i emX icmp** (X = {0,1})

1.7 Εντολή: **route add -net 192.168.1.0/24 192.168.2.1**

1.8 **Ναι**, υπάρχει επικοινωνία.

1.9 Ο R1 έχει **ήδη εγγραφές για τα LAN1/2 στο routing table** του, οι οποίες **δημιουργήθηκαν όταν αποδώσαμε IPv4 διευθύνσεις** στις διεπαφές του. Έτσι, γνωρίζει πώς να προωθήσει πακέτα IPv4 με διεύθυνση προορισμού που ανήκει σε αυτά τα LAN.

2

2.1 Εντολή: **route del 192.168.2.0/24**

2.2 Εντολή: **ifconfig em0 192.168.1.2/20**

2.3 Βρίσκονται **στο ίδιο υποδίκτυο IP**, το 192.168.0.0/20.

2.4 Τα ping **αποτυγχάνουν** (αρχικά καμία απάντηση και έπειτα "host is down"). Αυτό συμβαίνει καθώς τα PC1 και PC2,3 δεν βρίσκονται στο ίδιο φυσικό μέσο εκπομπής, οπότε μόνο ο R1 "ακούει" τα ARP request του PC1, τα οποία φυσικά αγνοεί. Εντολή: **ping 192.168.2.2**

2.5 Το ping **επιτυγχάνει**, καθώς τώρα ο R1 λειτουργεί ως proxy για τα μηχανήματα των LAN1,2, απαντώντας ο ίδιος στα ARP request των μηχανημάτων ενός LAN για τα μηχανήματα του άλλου και προωθώντας τα πλαίσια κατάλληλα. Εντολή: **ping -c 1 192.168.2.2**

2.6 Το ping αποτυγχάνει (καμία απάντηση) καθώς τα πλαίσια του PC1 προωθούνται μεν στο PC3, αλλά αυτό **δεν θεωρεί ότι το PC1 είναι στο ίδιο LAN** (έχει πρόθεμα δικτύου 24), οπότε δεν γνωρίζει πώς να προωθήσει τα ICMP echo reply στο PC1. Εντολή: **ping -c 1 192.168.2.2**

2.7 Εντολή: **route add -net 192.168.1.0/24 192.168.2.1**

2.8 Εντολή: **arp -da**

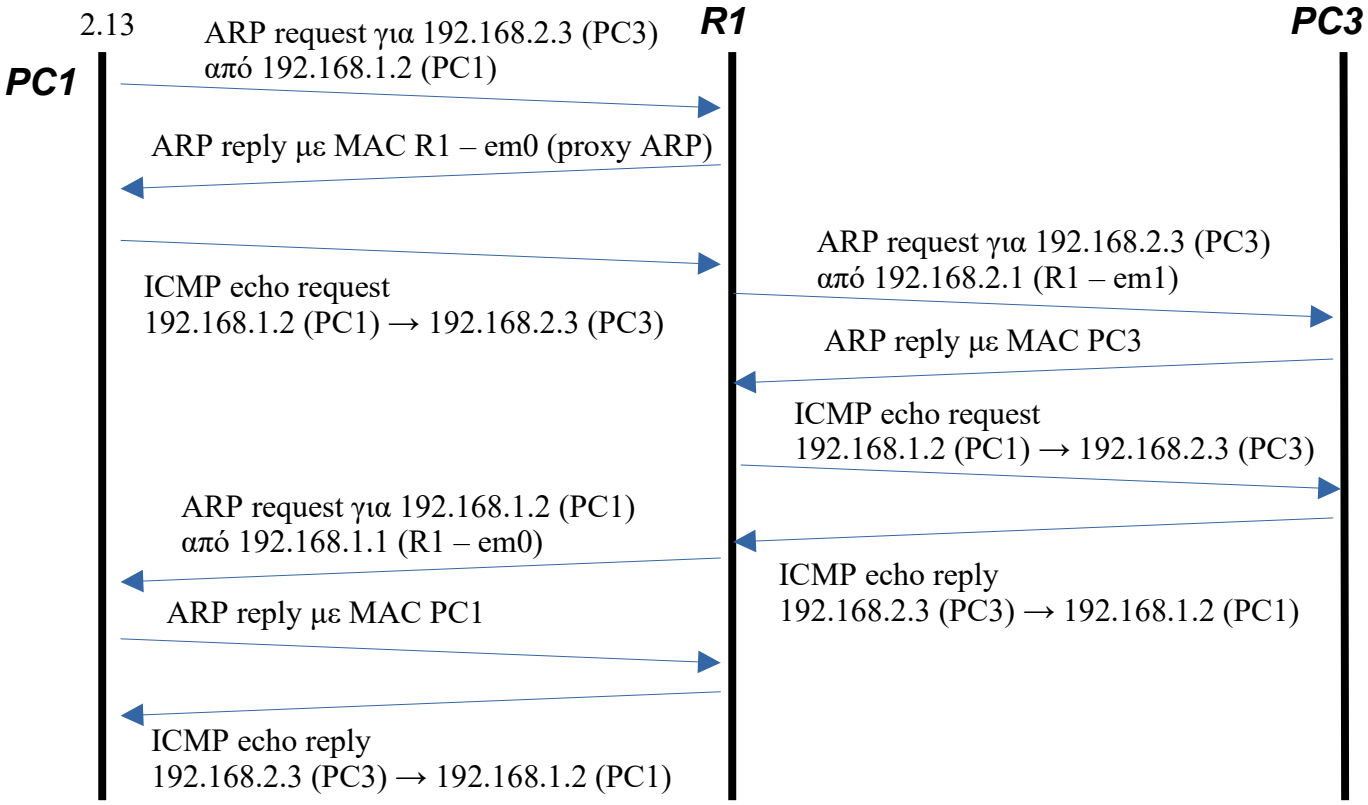
2.9 Εντολές: 1) **tcpdump -ei em0** 2) **tcpdump -ei em1** 3) **ping -c 1 192.168.2.3**

2.10 Παρατηρούμε ότι ο **R1 απαντά εκ μέρους του PC3** με ARP reply, δίνοντας την **δική του διεύθυνση MAC (em0)**.

2.11 Προς τη διεύθυνση MAC της **em0 του R1**, όπως είναι αναμενόμενο από το 2.10.

2.12 Από τη διεύθυνση MAC της **em1 του R1**.

2.13



2.14 Η συμπεριφορά των R1/PC3 δεν επηρεάζεται από το μήκος προθέματος που θέτουμε στο PC1. Άρα για να λειτουργεί το ping πρέπει και αρκεί το PC1 να θεωρεί ότι οι **192.168.1.1** και **192.168.2.3** ανήκουν στο υποδίκτυό του. Άρα το μέγιστο μήκος προθέματος είναι **22**.

2.15 Εντολή: **ifconfig em0 192.168.1.2/23**

2.16 Εντολή: **route add 192.168.2.0/24 -interface em0**

2.17 Εμφανίζεται η διεύθυνση MAC της **em0 του PC1**. Εντολή: **netstat -4r**

2.18 **Ναι**, καθώς τώρα υπάρχει εγγραφή στο routing table του PC1 για το δίκτυο του PC3.

2.19 Εντολή: **sysctl net.link.ether.inet.proxyall=0**

2.20 Εντολή: **route change 192.168.2.0/24 192.168.1.1**

2.21 Εντολή: **ifconfig em0 192.168.1.2/24**

2.22 Έχει **διαγραφεί** λόγω της εντολής 2.21.

2.23 Εντολή: **route add 192.168.2.0/24 192.168.1.1**

3

3.1 Εντολές: 1) **ifconfig em0 192.168.1.1/24** 2) **ifconfig em1 172.17.17.1/30**

3.2 Εντολές: 1) **ifconfig em0 172.17.17.2/30** 2) **ifconfig em1 192.168.2.1/24**

3.3 Παρατηρούμε μηνύματα **Destination Host Unreachable**.

3.4 Στο LAN1 παράγονται μηνύματα **ICMP echo request** και **ICMP host unreachable**, ενώ στο WAN1 **δεν παράγονται** μηνύματα ICMP. Ο λόγος είναι ότι το R1 δεν έχει την κατάλληλη εγγραφή στο routing table του για το PC2. Συνεπώς λαμβάνει το ICMP echo request, δεν το προωθεί στο WAN1 και απαντά στο PC1 με ICMP host unreachable. Εντολές: **tcpdump -i emX icmp** από το R1 (X = {0,1})

3.5 Παρατηρούμε ότι στη θέση του 2ου κόμβου έχουμε πάλι την IP 192.168.1.1 του R1 με την **ένδειξη λάθους "!H"**, η οποία σημαίνει **Host Unreachable**. Εντολή: **traceroute 192.168.2.2**

3.6 Εντολή: **route add 192.168.2.0/24 172.17.17.2**

3.7 **Όχι**, δεν μπορούμε. **Δεν λαμβάνουμε καμία απάντηση**.

3.8 1) **ICMP echo request PC1 → PC2** οφείλεται στο ping
2) **ICMP echo reply PC2 → PC1** οφείλεται στο ping
3) **ICMP host unreachable R2 → PC2** αφού το R2 δεν έχει εγγραφή στο routing table για το PC1

3.9 **Όχι**, παρατηρούμε UDP datagrams στο WAN1, όπως είναι λογικό, καθώς τώρα ο R1 γνωρίζει ότι πρέπει να προωθήσει τα πακέτα αυτά στον R2 για να φτάσουν το PC2. Τα UDP datagrams είναι η προεπιλογή της traceroute αντί για ICMP echo request.

3.10 1) **UDP datagram PC1 → PC2** οφείλεται στο traceroute (αντί του ICMP echo request)
2) **ICMP UDP port unreachable PC2 → PC1** οφείλεται στο traceroute

3.11 Ο R2 δεν μπορεί να προωθήσει στο PC1 το μήνυμα ICMP UDP port unreachable. Εντούτοις, αυτό είναι μήνυμα λάθους, οπότε **δεν επιτρέπεται να παραχθεί ICMP μήνυμα λάθους** ως απάντηση σε αυτό. Αυτός είναι ο λόγος για τον οποίον δεν παρατηρείται τέτοιο μήνυμα στο LAN2.

3.12 Εντολή: **route add 192.168.1.0/24 172.17.17.1**

3.13 **Ναι**, τώρα μπορούμε. Τα μηνύματα ICMP που παράγονται στο WAN1 είναι τα εξής:
1) **ICMP time exceeded in-transit R2 (em0) → PC1** τριάδα αποτυχημένων ping με στόχο τον R2
2) **ICMP UDP port unreachable PC2 → PC1** τριάδα επιτυχών ping με στόχο το PC2

3.14 Το ping **αποτυγχάνει**, με μήνυμα **No route to host**. Εντολή: **ping 172.17.17.1**

3.15 Εντολή: **route del 192.168.1.0/24**

3.16 Εντολή: **route add default 192.168.2.1**

3.17 Το ping τώρα **επιτυγχάνει**.

3.18 Στην πρώτη περίπτωση **δεν υπήρχε εγγραφή** στο routing table του PC2 που να ταιριάζει με την IP 172.17.17.1, με αποτέλεσμα το μήνυμα **No route to host**. Το ping μεταξύ PC1 – PC2 δούλευε γιατί υπήρχαν εγγραφές για τα υποδίκτυα LAN1,2 σε αμφότερα τα PC1,2. Όταν προσθέσαμε default gateway στο PC2 τα ICMP echo request άρχισαν να προωθούνται στον R2, οδηγώντας στην **επιτυχία των ping**.

4

4.1 Ρυθμίσεις PC3 → Network → Adapter 1 → **Enable Network Adapter & Attached to: Internal Network & Name: LAN2 & Advanced → Cable Connected**.
Έπειτα εκτελούμε την εντολή: **ifconfig em0 192.168.2.3/24**

4.2 Εντολή: **route add 192.168.1.0/24 192.168.2.1**

4.3 Οι em0,1,2 του R1 πρέπει να βρίσκονται στα LAN1, WAN1 και WAN2 αντίστοιχα. Οι εντολές είναι:
1) **ifconfig em0 192.168.1.1/24** 2) **ifconfig em1 172.17.17.1/30** 3) **ifconfig em2 172.17.17.5/30**

4.4 Οι em0,1,2 του R2 πρέπει να βρίσκονται στα WAN1, LAN2 και WAN3 αντίστοιχα. Οι εντολές είναι:
1) **ifconfig em0 172.17.17.2/30** 2) **ifconfig em1 192.168.2.1/24** 3) **ifconfig em2 172.17.17.9/30**

4.5 Οι em0,1 του R3 πρέπει να βρίσκονται στα WAN2 και WAN3 αντίστοιχα. Οι εντολές είναι:
1) **ifconfig em0 172.17.17.6/30** 2) **ifconfig em1 172.17.17.10/30**

4.6 Εντολή: **route add 192.168.2.0/24 172.17.17.2**

4.7 Εντολή: **route add 192.168.1.0/24 172.17.17.1**

4.8 Εντολές: 1) **route add 192.168.1.0/24 172.17.17.5**
2) **route add 192.168.2.0/24 172.17.17.9**

4.9 Εντολή: **route add 192.168.2.3 172.17.17.6**
Η σημαία **H** στον πίνακα δρομολόγησης δηλώνει ότι πρόκειται για διαδρομή προς υπολογιστή (Host)

4.10 Βλέπουμε **3 βήματα**, την **192.168.1.1** (R1 – em0), την **172.17.17.2** (R2 – em0) και την **192.168.2.2** (PC2) Εντολή: **traceroute -I 192.168.2.2**

4.11 Έχουμε TTL = 62 (με αρχικό TTL = 64), οπότε έχουμε πάλι 64 – (62 – 1) = **3 βήματα**.
Εντολή: **ping 192.168.2.2**

4.12 Βλέπουμε **4 βήματα**, την **192.168.1.1** (R1 – em0), την **172.17.17.6** (R3 – em0), την **172.17.17.2** (R2 – em0) και τέλος την **192.168.2.3** (PC3) Εντολή: **traceroute -I 192.168.2.3**

4.13 Βλέπουμε TTL = 62, δηλαδή **3 βήματα**, σε αντίθεση με πριν. Εντολή: **ping 192.168.2.2**

4.14 **Το ICMP echo request ακολουθεί την διαδρομή της traceroute**, διότι κάθε βήμα αυτής αντιστοιχεί σε έναν κόμβο από τον οποίον το ICMP echo request περνάει και δεν μπορεί να προχωρήσει λόγω Time limit exceeded (με εξαίρεση φυσικά τον κόμβο-προορισμό του ping). Να σημειωθεί βέβαια ότι οι IP που βλέπουμε είναι οι IP πηγής των ICMP time exceeded, οπότε δεν υποδεικνύουν πάντα τη διεπαφή του κόμβου όπου φτάνει το echo request, όπως στην περίπτωση του R2 στο ping PC1 → PC3.

4.15 **Το ICMP echo reply ακολουθεί την διαδρομή του ping**, διότι το TTL που βλέπουμε στο terminal και χρησιμοποιούμε για τον υπολογισμό των βημάτων είναι το TTL του πακέτου IP που φέρει το ICMP echo reply.

4.16 Εντολή: **tcpdump -i em1**

4.17 **Όχι**, δεν παρατηρούμε πακέτα UDP στο LAN2. Εντολή: **traceroute 192.168.2.2**

4.18 **Ναι**, **φτάνουν πακέτα UDP** στο PC3 και **παράγονται ICMP UDP port unreachable** από αυτό.
Εντολή: **traceroute 192.168.2.3**

4.19 R1: **route change 192.168.2.0/24 172.17.17.6** R2: **route change 192.168.1.0/24 172.17.17.10**
Επιβεβαιώνουμε με **traceroute 192.168.2.2** από το PC1

4.20 PC2: **route get 192.168.2.2** PC3: **route get 192.168.2.3**
Για τον PC2 έχουμε destination **192.168.2.0** και netmask **255.255.255.0**, που αντιστοιχούν σε εγγραφή στο routing table για το LAN2. Αντιθέτως, για το PC3 το destination είναι το **192.168.2.3** και **δεν εμφανίζεται netmask**, το οποίο υποδεικνύει εγγραφή στο routing table συγκεκριμένα για το PC3 (μάλιστα υπάρχει και σημαία "HOST"). Τα παραπάνω βρίσκονται σε συμφωνία με τα **4.9** και **4.19**.

4.21 Επιλέγεται η διαδρομή που παρατηρήσαμε στο 4.20 για τον PC3, που όπως προαναφέραμε αντιστοιχεί σε **εγγραφή στο routing table του R1 συγκεκριμένα για τον PC3**.

5

5.1 Εντολή: **route change 192.168.2.0/24 172.17.17.5**

5.2 Το ping **αποτυγχάνει**. Εντολή: **ping 192.168.2.2**

5.3 Λαμβάνουμε πολλά μηνύματα **ICMP Redirect Host** από τις 192.168.1.1 (R1 – em0) και 172.17.17.6 (R3 – em0) και στο τέλος ένα μήνυμα **ICMP TTL exceeded** από την 172.17.17.6 (R3 – em0).

5.4 Εντολές: **tcpdump -i em0 > tcpdump_LAN1** (R1) και **tcpdump -i em0 > tcpdump_WAN2** (R3)

5.5 LAN1: Καταγράφηκαν **64 μηνύματα ICMP**, εκ των οποίων **1** ήταν **echo request**, **1** ήταν **time exceeded in-transit** και **62** ήταν **redirect**.
WAN2: Καταγράφηκαν **95 μηνύματα ICMP**, εκ των οποίων **63** ήταν **echo request**, **1** ήταν **time exceeded in-transit** και **31** ήταν **redirect**.
Εντολές: **grep Y tcpdump_X | wc -l**
(με X = {LAN1, WAN2} και Y = {ICMP, "echo request", "time exceeded", redirect})

5.6 Εντολή: **tcpdump -evi em0 'icmp[icmptype] == icmp-echo'**

5.7 Εμφανίστηκαν **63 μηνύματα ICMP Echo request** στο WAN2 ("63 packets captured"). Παρατηρούμε ότι οι MAC πηγής εναλλάσσονται μεταξύ του R1 και του R3, με τον R1 να εμφανίζεται στο πρώτο και το τελευταίο πλαίσιο, οπότε συμπεραίνουμε ότι τα **32 πλαίσια έχουν ως πηγή τον R1 και τα 31 τον R3**. Η εναλλαγή των R1 και R3 είναι λογική, καθώς ο R1 ξεκινά προωθώντας το πακέτο στον R3, εκείνος το προωθεί πίσω στον R1 και η διαδικασία επαναλαμβάνεται, μέχρι να μηδενιστεί το TTL.

5.8 Εντολές: **tcpdump -evi em0 'icmp[icmptype] == 5'** σε R1 και R3

5.9 Στο WAN2 εμφανίζονται **31 μηνύματα ICMP redirect**. Ο R3 στέλνει ICMP redirect κάθε φορά που λαμβάνει το echo request στο WAN2 από τον R1, με εξαίρεση την τελευταία φορά που δεν προωθεί το echo request λόγω της λήξης του TTL. Συνεπώς **είναι αναμενόμενο ο αριθμός των ICMP redirect** που στέλνονται από τον R3 **να ταυτίζεται με τον αριθμό των echo request** που στέλνει στο WAN2, το οποίο πράγματι συμβαίνει.

5.10 Στο LAN1 εμφανίζονται **62 μηνύματα ICMP redirect**. Τα 31 από αυτά προέρχονται από τον R3, όπως προαναφέραμε, και τα υπόλοιπα 31 προέρχονται από τον R1. Αυτό βρίσκεται σε συμφωνία με το 5.7, καθώς ο R1 στέλνει ένα ICMP redirect **κάθε φορά που λαμβάνει echo request από το WAN2**, δηλαδή κάθε φορά που στέλνει echo request ο R3.

5.11 Εμφανίζονται **64 βήματα** μέχρι την ολοκλήρωση της εντολής, τα οποία είναι **εναλλάξ ο R1 και ο R3** (192.168.1.1 και 172.17.17.6). Αυτό είναι λογικό, καθώς αναφέρεται ότι έχουμε "64 hops max", δηλαδή η διαδικασία τερματίζεται μετά από 64 βήματα. Εντολή: **traceroute -I -q 1 192.168.2.2**

5.12 Στάλθηκαν **64 μηνύματα ICMP echo request από τον PC1**. Αυτό είναι λογικό, καθώς έχουμε **64 βήματα της traceroute**, που αντιστοιχούν ένα προς ένα σε μηνύματα echo request του PC1. Επιβεβαιώνουμε με την εντολή **grep "echo request" tcpdump_LAN1 | wc -l** από τον R1. Εμφανίζονται **2016 μηνύματα ICMP echo request στο WAN2**, καθώς **για το ν-οστό βήμα** της traceroute έχουμε TTL = n, και άρα το echo request θα σταλεί **n-1 φορές στο WAN2**. Έτσι, έχουμε συνολικά 0 + 1 + … + 63 = 63*64/2 = **2016 μηνύματα ICMP στο WAN2**.
Εντολή: **grep "echo request" tcpdump_WAN2 | wc -l** από τον R3

5.13 Εμφανίστηκαν **32 μηνύματα ICMP** time exceeded στο WAN2. Αυτό είναι λογικό, καθώς από τα 64 βήματα της traceroute, **32** οδήγησαν σε μήνυμα **time exceeded από τον R1**, το οποίο δεν εμφανίζεται στο WAN2 (πηγαίνει απευθείας μέσω του LAN1) και **τα υπόλοιπα 32 εστάλησαν από τον R3, μέσω του WAN2**.

5.14 Εκτελούμε την εντολή **tcpdump -i em0 'icmp[0] == X'**, με X = 8 για echo request και 11 για time exceeded. Έπειτα σταματάμε την καταγραφή και εστιάζουμε στο **"Y packets captured"**.

6

6.1 Είναι η **172.17.17.0/25** (χωρητικότητα 2^7 – 2 = 126 υπολογιστές)

6.2 Είναι η **172.17.17.192/26** (χωρητικότητα 2^6 – 2 = 62 υπολογιστές)

6.3 Είναι η **172.17.17.160/27** (χωρητικότητα 2^5 – 2 = 30 υπολογιστές)

6.4 Εντολές: **ifconfig em0 172.17.17.1/25** PC1
ifconfig em0 172.17.17.126/25 R1

6.5 Εντολές: **ifconfig em0 172.17.17.161/27** PC4
ifconfig em2 172.17.17.190/27 R3

6.6 Εντολές: **ifconfig em1 172.17.17.193/26** R2
ifconfig em0 172.17.17.253/26 PC2
ifconfig em0 172.17.17.254/26 PC3

6.7 Εντολές: **route add default 172.17.17.126** PC1 **route add default 172.17.17.190** PC4
route add default 172.17.17.193 PC2,3

6.8 Εντολές: 1) **route add 172.17.17.192/26 172.17.17.130**
2) **route add 172.17.17.160/27 172.17.17.130**

6.9 Εντολές: 1) **route add 172.17.17.0/25 172.17.17.137**
2) **route add 172.17.17.160/27 172.17.17.137**

6.10 Εντολές: 1) **route add 172.17.17.0/25 172.17.17.133**
2) **route add 172.17.17.192/26 172.17.17.133**

6.11 PC1: **ping 172.17.17.253** PC2: **ping 172.17.17.161** PC3: **ping 172.17.17.1**
Τα παραπάνω ping είναι **όλα επιτυχή**.

7

7.1 PC2: **08:00:27:ad:5d:60**
PC3: **08:00:27:23:2f:4f** Εντολή: **ifconfig em0 | grep ether**

7.2 Εντολή: **ifconfig em0 172.17.17.254/26**

7.3 **Ναι**, λάβαμε μήνυμα λάθους "arp: 08:00:27:23:2f:4f is using my IP address 172.17.17.254 on em0!"

7.4 **Ναι**, λάβαμε μήνυμα λάθους "arp: 08:00:27:ad:5d:60 is using my IP address 172.17.17.254 on em0!"

7.5 **Ναι**, έχει οριστεί η νέα IP. Τα μηνύματα λάθους απλώς μας προειδοποιούν ότι αυτή η δικτυακή ρύθμιση ενδέχεται να έχει ανεπιθύμητα αποτελέσματα, στην περίπτωση που η ανάθεση έγινε εκ παραδρομής.

7.6 **Όχι**, καθώς αλλάξαμε την IP της em0 με χρήση της ifconfig.

7.7 Εντολή: **route add default 172.17.17.193**

7.8 Εντολή: **arp -da**

7.9 Εντολή: **tcpdump -ni em1 arp**

7.10 Εντολή: **tcpdump -ni em0 tcp**

7.11 Εμφανίζεται error **"Fssh_kex_exchange_identification: read: Connection reset by peer**
Connection reset by 172.17.17.254 port 22" Εντολή: **ssh lab@172.17.17.254**

7.12 **Ναι**, το SSH τώρα **επιτυγχάνει**.

7.13 Ο πίνακας ARP του R2 μπορεί να έχει μόνο μία εγγραφή για τους PC2,3, αφού και οι δύο έχουν την ίδια διεύθυνση IP. Εκτελώντας **arp 172.17.17.254** λαμβάνουμε τη MAC **08:00:27:ad:5d:60**.

7.14 Στο ARP request του R2 απάντησε **πρώτο το PC3 και δεύτερο το PC2**.

7.15 Στο **PC2**.

7.16 Στο **PC2**. Εντολή: **ifconfig em0 | grep ether** από το SSH

7.17 1) **netstat -4n** και στα δύο μηχανήματα και επιλέγουμε αυτό στο οποίο εμφανίζεται το PC1.
2) **who** και στα δύο μηχανήματα και επιλέγουμε αυτό στο οποίο εμφανίζεται το PC1.

7.18 Την πρώτη φορά δεν δούλεψε το SSH διότι ο R2 έλαβε το ARP reply από το PC3 και έστειλε το πρώτο πακέτο της τριπλής χειραψίας σε αυτό. Στη συνέχεια όμως έφτασε και το ARP reply του PC2, οπότε τα τεμάχια TCP άρχισαν να στέλνονται σε αυτόν, οδηγώντας στην κατάρρευση της σύνδεσης. Εντούτοις, τη δεύτερη φορά υπήρχε στο ARP table του R2 καταχώρηση με τη MAC του PC2, με αποτέλεσμα η σύνδεση να δουλεύει κανονικά.