

Όνοματεπώνυμο: Μοίρας Αλέξανδρος	Όνομα PC: LAPTOP-5A8R1JQR
Ομάδα: 3	Ημερομηνία: 30/3/2022

## 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 ifconfig em0 inet 192.168.1.2/24 και αντίστοιχα και για τις υπόλοιπες διεπαφές.

1.2 gateway\_enable="YES"

1.3 route add -net 192.168.2.0/24 192.168.1.1

1.4 U: Η διαδρομή είναι ενεργή.

G: Ο προορισμός είναι πύλη, που θα αποφασίσει πως θα προωθήσει τα πακέτα περαιτέρω.

S: Η διαδρομή έχει οριστεί στατικά.

192.168.2.0/24	192.168.1.1	UGS	em0
----------------	-------------	-----	-----

1.5 Ότι δε λαμβάνουμε απάντηση από το PC2.

1.6 Παράγονται μόνο ICMP Echo requests. Το PC1 έχει διαδρομή μέσω του router για το PC2 (για το υποδίκτυό του) οπότε στέλνει τα πακέτα του (requests) στον R1 ο οποίος τα προωθεί στο LAN2 οπότε φτάνουν στο PC2. Αλλά το PC2 εξετάζοντας τη διεύθυνση του PC1 ανιχνεύει ότι βρίσκεται σε διαφορετικό υποδίκτυο ωστόσο δεν έχει διαδρομή προς αυτό οπότε δε στέλνει απάντηση.

1.7 route add -net 192.168.1.0/24 192.168.2.1

1.8 Ναι τώρα επικοινωνούν κανονικά.

1.9 Γιατί έχει διεπαφή και στα δύο τοπικά δίκτυα και με ενεργοποιημένο το IP Forwarding ξέρει που να προωθήσει τα πακέτα όπως φαίνεται και στον πίνακα δρομολόγησης. Επίσης παρατηρούμε ότι εκτός από τα δίκτυα υπάρχουν εγγραφές και για τους δύο hosts.

Internet:				
Destination	Gateway	Flags	Netif	Expire
127.0.0.1	link#3	UH	lo0	
192.168.1.0/24	link#1	U	em0	
192.168.1.1	link#1	UHS	lo0	
192.168.2.0/24	link#2	U	em1	
192.168.2.1	link#2	UHS	lo0	

2

2.1 route del 192.168.2.0/24

2.2 ifconfig em0 inet 192.168.1.2/20

2.3 Από την προοπτική του PC1 βρίσκονται στο ίδιο δίκτυο.

2.4 Όχι δεν είναι.

2.5 Ναι το ping είναι επιτυχές γιατί το PC1 θεωρώντας ότι το PC2 βρίσκεται στο ίδιο υποδίκτυο στέλνει ARP Request για τη διεύθυνσή του στο οποίο απαντά ο R1, που έχει ενεργοποιημένη τη λειτουργία Proxy ARP, με τη δική του MAC και ύστερα προωθεί τα ICMP Echo requests που

λαμβάνει στο LAN2, τα λαμβάνει το PC2 που αναγνωρίζει ότι το PC1 βρίσκεται σε άλλο υποδίκτυο άλλα του έχουμε ορίσει διαδρομή στο Routing Table του οπότε στέλνει τις απαντήσεις στον R1 και από εκεί προωθούνται στο PC1.

2.6 Γιατί από την προοπτική του PC3 το PC1 βρίσκεται σε άλλο δίκτυο προς το οποίο δεν έχει οριστεί διαδρομή, οπότε οι απαντήσεις δε στέλνονται ποτέ στο PC1, ενώ δε στέλνονται καν ARP Requests για τη διεύθυνση του PC1 ώστε να λειτουργήσει το Proxy ARP.

2.7 route add -net 192.168.1.0/24 192.168.2.1

2.8 arp -ad

2.9 tcpdump -ei em0, tcpdump -ei em1, ping -c 1 192.168.2.3

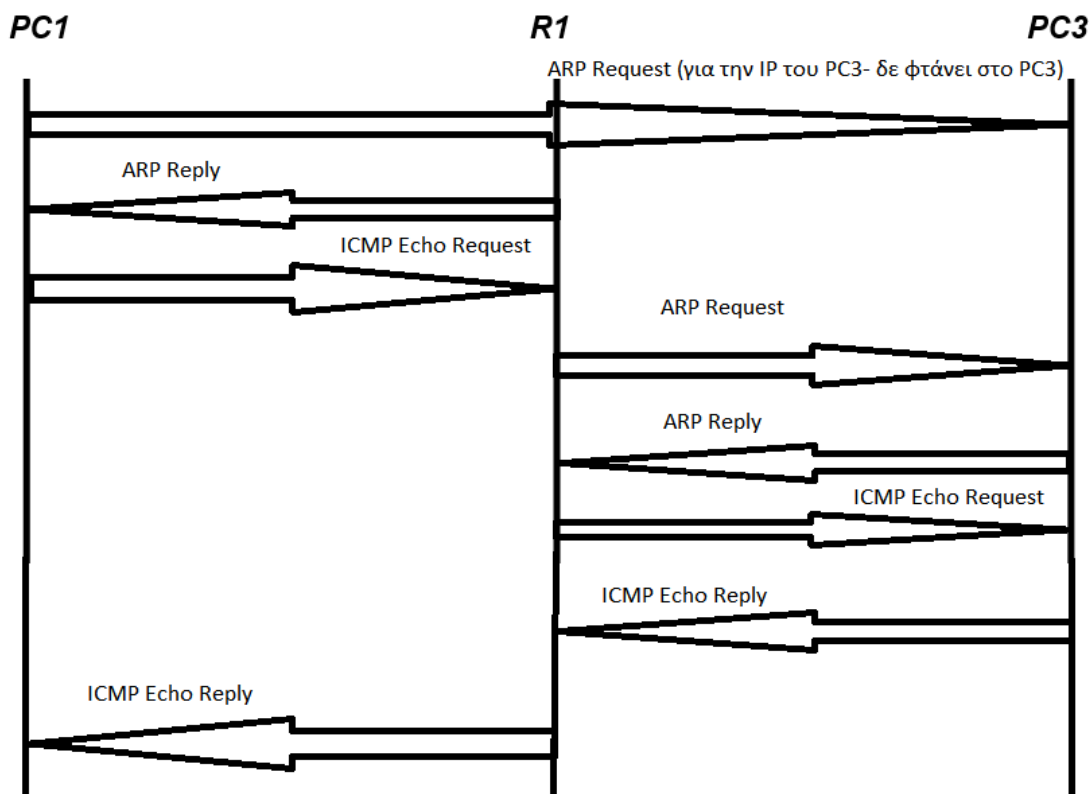
2.10 Ότι απαντά με τη δική του MAC (της διεπαφής του στο LAN1)

2.11 Προς τη MAC του R1.

2.12 Από τη MAC διεύθυνση του R1 και συγκεκριμένα της διεπαφής του στο LAN2.

2.13 ARP Request από το PC1 για τη διεύθυνση του PC3 Που θεωρεί ότι βρίσκεται στο ίδιο δίκτυο  
Arp Reply από τον R1 λόγω Proxy ARP

Στη συνέχεια ο PC1 «βλέπει» τον PC3 στον R1 και η επικοινωνία γίνεται με τον κλασσικό τρόπο (ICMP request στον R1 ARP request από R1 για PC3, Reply από PC3 στον R1 λόγω routing table και προώθηση προς PC1).



2.14 22 γιατί μετά το PC1 θα πάψει να θεωρεί ότι το PC3 βρίσκεται στο ίδιο τοπικό δίκτυο με αυτό.

2.15 ifconfig em0 inet 192.168.1.2/23

2.16 route add -net 192.168.2.0/24 -interface em0

2.17 Η MAC διεύθυνση της διεπαφής του PC1 στο LAN1.

192.168.2.0/24 08:00:27:32:93:02 US em0

2.18 Ναι είναι γιατί τώρα το PC1 έχει διαδρομή προς το PC3 που αναγνωρίζει πως βρίσκεται σε διαφορετικό υποδίκτυο (οπότε το Proxy ARP δε χρησιμεύει) οπότε στέλνει το πακέτο στον R1 και προωθείτε στον R3 (η υπόλοιπη επικοινωνία όπως πριν).

2.19 `sysctl net.link.ether.inet.proxyall=0`

2.20 `route change -net 192.168.2.0/24 192.168.1.1`

2.21 `ifconfig em0 inet 192.168.1.2/24`

2.22 Έχει διαγραφεί. `route add -net 192.168.2.0/24 192.168.1.1`

3

3.1 `ifconfig em0 192.168.1.1/24`

`ifconfig em1 172.17.17.1/30`

3.2 `ifconfig em0 172.17.17.2/30`

`ifconfig em1 192.168.2.1/24`

3.3 destination host unreachable μήνυμα από τον R1.

```
36 bytes from 192.168.1.1: Destination Host Unreachable
  Jr HL TOS  Len   ID Flg  off TTL Pro  cks      Src      Dst
   4   5   00 0054 7d5e   0 0000 40   01 78f6 192.168.1.2 192.168.2.2
```

3.4 Παράγονται μηνύματα ICMP Echo request από το PC1 και ICMP Destination Unreachable από τον R1. Αυτό συμβαίνει γιατί ο R1 δεν έχει εγγραφή στον πίνακα δρομολόγησής του που να ταιριάζει με τη διεύθυνση 192.168.2.2 οπότε δεν ξέρει που να προωθήσει το πακέτο.

3.5 Η ένδειξη λάθους !H σημαίνει Host Unreachable και επιστρέφεται από τον R1 στο δεύτερο βήμα δηλώνοντας ότι δεν υπάρχει διαδρομή από εκεί και πέρα προς το PC2.

3.6 `route add -net 192.168.2.0/24 172.17.17.2`

3.7 Όχι, δε λαμβάνουμε απάντηση.

3.8 ICMP Echo Requests που προωθούνται από τον R2 στο LAN2, ICMP Echo Replies που παράγονται ως απάντηση από το PC2 και στέλνονται στη διεπαφή με διεύθυνση 192.168.2.1 σύμφωνα με τον πίνακα δρομολόγησης και ICMP Destination Unreachable που παράγονται από τον R2 διότι δε γνωρίζει τη διαδρομή που πρέπει να ακολουθήσει το πακέτο που έχει να προωθήσει ώστε να φτάσει στο 192.168.1.2.

3.9 Δεν παρατηρούμε μηνύματα ICMP Echo Request. Παρατηρούμε δεδομενογράμματα UDP γιατί η traceroute χρησιμοποιεί δεδομενογράμματα UDP εκτός και αν τη ρυθμίσουμε διαφορετικά μέσω της παραμέτρου -I.

3.10 Παράγονται δεδομενογράμματα UDP και ICMP μηνύματα UDP Port Unreachable στην προσπάθεια του PC2 να στείλει Error message καθώς δεν ακούει σε αυτό το port

3.11 Δεν παρατηρούμε ICMP Host Unreachable στο LAN2 καθώς αυτά θα στέλνονταν ως απάντηση από τον R2 στο PC2 στην προσπάθειά του να προωθήσει τα ICMP Port Unreachable προς το PC1. Όμως τα ICMP Port Unreachable είναι μηνύματα λάθους ICMP και σύμφωνα με τη σύμβαση δεν παράγονται μηνύματα λάθους ICMP όπως το Host Unreachable ως απάντηση σε μηνύματα λάθους ICMP προκειμένου να αποφευχθούν loops από μηνύματα λάθους.

3.12 `route add -net 192.168.1.0/24 172.17.17.1`

3.13 Ναι μπορούμε. Παράγονται μηνύματα ICMP Time exceeded in transit Που οφείλονται στον

τρόπο λειτουργίας του traceroute που ξεκινά με μικρό TTL ώστε λαμβάνοντας αυτά τα πακέτα από τους ενδιάμεσους κόμβους να τους αναγνωρίζει και ICMP UDP Port Unreachable όταν τα μηνύματα φτάσουν στον τελικό κόμβο ο οποίος δεν ακούει σε αυτήν την port.

3.14 Η ping επιστρέφει no route to host.

3.15 route del 192.168.1.0/24

3.16 route add default 192.168.2.1

3.17 Τώρα το ping είναι επιτυχές

3.18 Πριν δεν υπήρχε διαδρομή προς τη διεύθυνση 172.17.17.1 στον πίνακα δρομολόγησης του PC2 δηλαδή καμία από τις εγγραφές δεν ταίριαζε με αυτή τη διεύθυνση. Τώρα ορίσαμε default διαδρομή στο PC2 προς τη διεπαφή του R2 στο LAN2 οπότε τα πακέτα του Ping φτάνουν στον R2 από όπου προωθούνται στον R1 οποίος απαντά γνωρίζοντας που βρίσκεται το PC2.

#### 4

4.1 ifconfig em0 up

ifconfig em0 192.168.2.3/24

4.2 route add -net 192.168.1.0/24 192.168.2.1

4.3 em0: LAN1, em1: WAN1, em2: WAN2

ifconfig em0 192.168.1.1/24

ifconfig em1 172.17.17.1/30

ifconfig em2 172.17.17.5/30

4.4 em0: WAN1, em1: WAN3, em2: LAN2

ifconfig em0 172.17.17.2/30

ifconfig em1 172.17.17.9/30

ifconfig em2 192.168.2.1/24

4.5 em0: WAN2, em1: WAN3

ifconfig em0 172.17.17.6/30

ifconfig em1 172.17.17.10/30

4.6 route add 192.168.2.0/24 172.17.17.2

4.7 route add 192.168.1.0/24 172.17.17.1

4.8 route add 192.168.1.0/24 172.17.17.5

route add 192.168.2.0/24 172.17.17.9

4.9 route add -host 192.168.2.3 172.17.17.6

Η σημαία H δηλώνει ότι πρόκειται για διαδρομή προς υπολογιστή.

4.10 Βλέπουμε 3 βήματα, ένα εκ των οποίων είναι το PC2 (το τελευταίο) επομένως δύο ενδιάμεσα βήματα μέχρι τον προορισμό.

```
traceroute to 192.168.2.2 (192.168.2.2), 64 hops max, 40 byte packets
 1  192.168.1.1 (192.168.1.1)  7.861 ms  0.395 ms  0.310 ms
 2  172.17.17.2 (172.17.17.2)  1.487 ms  0.926 ms  0.686 ms
 3  192.168.2.2 (192.168.2.2)  0.682 ms  0.396 ms  0.392 ms
```

4.11 Βλέπουμε 2 βήματα καθώς το TTL έχει μειωθεί κατά 2 (από 64 που ξεκίνησε έχει γίνει 62) μία φορά σε κάθε router από όπου πέρασε.

4.12 Βλέπουμε 4 βήματα, ένα εκ των οποίων είναι το PC3 (το τελευταίο) επομένως τρία ενδιάμεσα βήματα μέχρι τον προορισμό.

```
root@PC1:~ # traceroute 192.168.2.3
traceroute to 192.168.2.3 (192.168.2.3), 64 hops max, 40 byte packets
 1  192.168.1.1 (192.168.1.1)  0.326 ms  0.176 ms  0.202 ms
 2  172.17.17.6 (172.17.17.6)  0.348 ms  0.296 ms  0.299 ms
 3  172.17.17.2 (172.17.17.2)  0.450 ms  0.269 ms  0.344 ms
 4  192.168.2.3 (192.168.2.3)  0.752 ms  0.794 ms  0.668 ms
```

4.13 Βλέπουμε 2 βήματα (TTL 62) άρα η απάντηση πέρασε από δύο ενδιάμεσους κόμβους.

4.14 Το ICMP Echo Request ακολουθεί τη διαδρομή PC1=>R1=>R3=>R2=>PC3.

4.15 Το ICMP Echo Reply ακολουθεί τη διαδρομή PC3=>R2=>R1=>PC1.

Το ICMP Echo Request ακολουθεί τη διαδρομή μέσω του R3 διότι ορίσαμε στατικά στον R1 να δρομολογεί την κίνηση προς την IP της διεπαφής του PC3 μέσω του R3 οπότε όταν φτάσει το ICMP Echo Request από το PC1 στον R1 θα προωθηθεί στον R3 και από εκεί στον R2 και στο PC3.

Το ICMP Echo Reply ξεκινά από το PC3 που δρομολογεί κίνηση προς το 192.168.1.0/24 που ανήκει το PC1 μέσω του R2 που δρομολογεί κίνηση προς αυτό το δίκτυο μέσω του R1 και όχι του R3 με βάση τις στατικές εγγραφές που προσθέσαμε στα προηγούμενα ερωτήματα. Από τον R1 το πακέτο προωθείται απευθείας στο PC1.

4.16 tcpdump -i em2

4.17 Όχι δε φτάνουν ούτε παράγονται πακέτα UDP στο PC2.

4.18 Ναι φτάνουν και παράγονται πακέτα UDP στο PC3.

4.19 R1: route change -net 192.168.2.0/24 172.17.17.6

R2: route change -net 192.168.1.0/24 172.17.17.10

Μετά την αλλαγή υπάρχει επικοινωνία

4.20 Παρατηρούμε ότι στη διαδρομή προς το PC2 (192.168.2.2) ο προορισμός είναι δίκτυο (192.168.2.0) ενώ στη διαδρομή προς το PC3 (192.168.2.3) ο προορισμός είναι host (192.168.2.3).

```
root@PC:~ # route show 192.168.2.2
route to: 192.168.2.2
destination: 192.168.2.0
mask: 255.255.255.0
gateway: 172.17.17.6
fib: 0
interface: em2
flags: <UP,GATEWAY,DONE,STATIC>
rcvpipe sendpipe ssthresh rtt,msec mtu weight expire
0 0 0 0 1500 1 0
root@PC:~ # route show 192.168.2.3
route to: 192.168.2.3
destination: 192.168.2.3
gateway: 172.17.17.6
fib: 0
interface: em2
flags: <UP,GATEWAY,HOST,DONE,STATIC>
rcvpipe sendpipe ssthresh rtt,msec mtu weight expire
0 0 0 0 1500 1 0
```

4.21 Επιλέγεται η εγγραφή με προορισμό 192.168.2.3 (όπως παρατηρήσαμε και παραπάνω) και όχι αυτή με προορισμό 192.168.2.0/24 καθώς στην πρώτη έχουμε ταίριασμα μήκους 32 bit που είναι

μεγαλύτερο από το ταίριασμα μήκους 24 bit που έχουμε στη δεύτερη.

5

5.1 route change -net 192.168.2.0/24 172.17.17.5

5.2 Όχι δεν είναι επιτυχές

5.3 Από τη διεπαφή του R3 στο WAN2 (172.17.17.6)

```
root@PC1:~ # ping -c 1 192.168.2.2
PING 192.168.2.2 (192.168.2.2): 56 data bytes
36 bytes from 172.17.17.6: Time to live exceeded
  Jr HL TOS Len  ID Flg  off TTL Pro  cks      Src      Dst
   4  5  00 0054 7e53   0 0000  01  01 b701 192.168.1.2 192.168.2.2
```

5.4 Στον δρομολογητή R3 (ο οποίος στέλνει το μήνυμα λάθους) στο δίκτυο WAN2.

5.5 icmp[0]==8

5.6 Από το PC1 παρήχθη ένα ICMP Echo request ενώ στο WAN2 εμφανίστηκαν 63.

5.7 tcpdump -i em0 -w lab5\_5

5.8 Εμφανίζονται 64 βήματα. Η διαδρομή που καταγράφουμε είναι εναλλάξ οι διεπαφές με διευθύνσεις 192.168.1.1 και 172.17.17.6.

5.9 Στάλθηκαν 64 πακέτα ICMP Echo Request από το PC1 (tcpdump -r lab5\_5|grep request|wc -l)

5.10 Εμφανίστηκαν 2016 πακέτα ICMP Echo Request στο WAN2. Η traceroute σταδιακά αυξάνει το TTL των πακέτων που στέλνει (από 1 έως 64 αφού παρήχθησαν σύνολο 64 ICMP Echo requests από το PC1) ώστε μέσω των πακέτων σφάλματος ICMP Time to Live Exceeded να αναγνωρίζει τη διαδρομή του πακέτου. Όμως για TTL x, αυτό θα μειωθεί κατά 1 στο Hop από PC1 σε R1 και ύστερα θα μειώνεται επιπλέον κατά 1 σε κάθε hop μεταξύ R1 και R3. Επομένως συνολικά θα γίνουν x-1 hops μεταξύ R1 και R3 και θα παραχθούν ισάριθμα ICMP Echo Request πακέτα στο WAN2. Επομένως ο συνολικός αριθμός ICMP Echo Request που θα παραχθούν στο WAN2 θα είναι:

$$\sum_{i=1}^{64} (i - 1) = \frac{63 \cdot 64}{2} = 2016$$

5.11 Εμφανίστηκαν 32 πακέτα ICMP time exceeded στο WAN2. Αυτό συμβαίνει γιατί τα ICMP time exceeded μηνύματα στέλνονται προς το PC1 και θα σταλούν από τον κόμβο στον οποίο μηδενίστηκε το TTL δηλαδή είτε τον R1 είτε τον R3 (ένα πακέτο για κάθε μηδενισμό TTL σε πακέτο δηλαδή ένα για κάθε ICMP Echo Request που παρήχθη από το PC1), όμως τα ICMP time exceeded από τον R1 δε θα εμφανιστούν στο WAN2 αφού στέλνονται κατευθείαν στο PC1 μέσω του LAN1. Επομένως θα εμφανιστούν στο WAN2 τόσα ICMP time exceeded όσα τα πακέτα που το TTL έγινε 0 στον R2. Το PC1 στέλνει πακέτα με TTL από 1 έως 64 και από αυτά μόνο εκείνα με ζυγό αριθμό TTL θα εκπνέουν στον R3 ενώ αυτά με μονό στον R1 (είναι εμφανές με βάση την τοπολογία) επομένως τα μισά από τα αρχικά ICMP Echo Requests θα εκπνεύσουν στον R2 άρα θα παραχθούν 32 ICMP time exceeded στο WAN2.

5.12 Χρησιμοποιώντας φίλτρα ώστε να καταγράφουμε ένα είδος πακέτου κάθε φορά

icmp[0]==8 για να καταγράψουμε ICMP Echo

icmp[0]==11 για να καταγράψουμε ICMP Time Exceeded

5.13 Στο ότι τα πακέτα ICMP Echo Request που παράγονται από το εργαλείο Ping έχουν σταθερό TTL και ίσο με 64 (default για freebsd) ενώ αυτά που παράγονται με την traceroute έχουν μεταβαλλόμενο TTL που ξεκινά από 1 και μπορεί να φτάσει έως και 64.

5.14 Γιατί έχουν πεπερασμένο αριθμό time to live ο οποίος κάποια στιγμή μηδενίζεται και το πακέτο παύει να προωθείται

## 6

6.1 Για να υπάρχουν τουλάχιστον 120 υπολογιστές στο LAN1 χρειάζονται 7 bits για αριθμό Host άρα η διεύθυνση υποδικτύου του LAN1 θα είναι 172.17.17.0/25.

6.2 Για να υπάρχουν τουλάχιστον 60 υπολογιστές στο LAN2 χρειάζονται 6 bits για αριθμό Host άρα η διεύθυνση υποδικτύου του LAN2 θα είναι 172.17.17.192/26. (Διευθύνσεις που δε χρησιμοποιούνται από LAN1 αλλά ούτε και από τους Routers).

6.3 Για να υπάρχουν τουλάχιστον 30 υπολογιστές στο LAN3 χρειάζονται 5 bits για αριθμό Host άρα η διεύθυνση υποδικτύου του LAN1 θα είναι 172.17.17.160/27.

6.4 `ifconfig em0 172.17.17.1/25 (PC1)`

`ifconfig em0 172.17.17.126/25 (R1)`

6.5 `ifconfig em0 172.17.17.161/27 (PC4)`

`ifconfig em2 172.17.17.190/27 (R3)`

6.6 `ifconfig em2 172.17.17.193/26 (R2)`

`ifconfig em0 172.17.17.253/26 (PC2)`

`ifconfig em0 172.17.17.254/26 (PC3)`

6.7 `route add default 172.17.17.126 (PC1)`

`route add default 172.17.17.193 (PC2)`

`route add default 172.17.17.193 (PC3)`

`route add default 172.17.17.190 (PC4)`

6.8 `route add -net 172.17.17.192/26 172.17.17.130`

`route add -net 172.17.17.160/27 172.17.17.130`

6.9 `route add -net 172.17.17.0/25 172.17.17.137`

`route add -net 172.17.17.160/27 172.17.17.137`

6.10 `route add -net 172.17.17.0/25 172.17.17.133`

`route add -net 172.17.17.192/26 172.17.17.133`

6.11 `ping 172.17.17.253 (από PC1)`

`ping 172.17.17.161 (από PC2)`

`ping 172.17.17.1 (από PC3)`

Όλα τα Ping είναι επιτυχή άρα υπάρχει επικοινωνία ανάμεσα σε όλα τα LAN.

## 7

7.1 PC2: 08:00:27:ec:3d:57

PC3: 08:00:27:3b:cd:52

7.2 `ifconfig em0 172.17.17.254/26`

7.3 Ναι λάβαμε ένδειξη λάθους που δήλωνε ότι ένας άλλος Host (τον οποίο αναπαριστούσε με τη MAC διεύθυνσή του) χρησιμοποιεί τη «δική μου» IP address.

7.4 Ναι εμφανίστηκε αντίστοιχη ένδειξη λάθους.

7.5 Ναι έχει οριστεί η διεύθυνση στο PC2. Το νόημα των μηνυμάτων λάθους είναι να προειδοποιεί τον χρήστη ότι η IP που προσπαθεί να ορίσει χρησιμοποιείται ήδη και αυτό ενδέχεται να προκαλέσει προβλήματα στο δίκτυο.

7.6 Όχι διότι αλλάξαμε την IP διεύθυνση της διεπαφής του οπότε σβήνεται ο πίνακας δρομολόγησης που υπήρχε πριν.

7.7 `route add default 172.17.17.129`

7.8 `arp -ad`

7.9 `tcpdump -i em2 arp`

7.10 `tcpdump -n tcp`

7.11 `ssh lab@172.17.17.190`

Ναι εμφανίστηκε ένδειξη λάθους Connection reset by peer

7.12 Ναι τώρα ήταν επιτυχής.

7.13 Για το PC3:

172.17.17.254 at 08:00:27:3b:cd:52 on em2 expires in 1054 seconds [ethernet].

Για το PC1 δεν υπάρχει εγγραφή (έγινε overwrite).

7.14 Πρώτο απάντησε το PC2 και μετά το PC3.

7.15 Ανήκει στο PC3.

7.16 Συνδεθήκαμε στο PC3.

7.17 Εκτελώντας `who` στην κονσόλα του PC2 και του PC3 και βλέποντας σε ποιόν είναι συνδεδεμένο το PC1, ή στο PC1 στην κονσόλα που έχει συνδεθεί με το PC3 (Αν και εκεί ήδη φαίνεται στο prompt το όνομα του PC3). Εναλλακτικά, κοιτώντας την αντιστοίχιση στον πίνακα ARP του R2 για τη διεύθυνση στην οποία συνδεόμαστε ώστε να δούμε σε ποιο PC ανήκει η MAC, καταγράφοντας στον R2 πακέτα από τη διεπαφή του στο LAN2 εμφανίζοντας και το Ethernet Header ώστε να δούμε ποιος υπολογιστής του LAN2 αποστέλλει και λαμβάνει τεμάχια TCP, με καταγραφή και στο PC2 και στο PC3 για να δούμε ποιο απαντά. Για να παραχθούν τέτοια τεμάχια αρκεί να πληκτρολογήσουμε χαρακτήρες στην κονσόλα του PC1 που έχει συνδεθεί με τον remote υπολογιστή.

7.18 Γιατί όπως παρατηρούμε από τις καταγραφές το PC1 πρώτα στέλνει το SYN στο PC2 (καθώς αυτό απαντά πρώτο στο ARP request του R2) και αυτό στέλνει SYN, ACK πίσω στο PC1. Μέχρι όμως να απαντήσει με ACK το PC1, ο R2 έχει λάβει ARP Reply από το PC3 και θα στείλει εκεί το ACK του PC1. Όμως το PC3 δεν έχει εγκαταστήσει καμία σύνδεση με το PC1 οπότε θα απαντήσει με TCP τεμάχιο με ενεργοποιημένη τη σημαία Reset και θα ακυρώσει τη σύνδεση.