ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

Εργαστήριο Δικτύων Υπολογιστών

Αναφορά 5ης Εργαστηριακής Άσκησης

Ραπτόπουλος Πέτρος (el19145)

Ημερομηνία: 28/3/2023

Άσκηση 1: Δρομολόγηση σε ένα βήμα

1.1) Με ποιες εντολές φλοιού ορίσατε διευθύνσεις IPv4 στα εικονικά μηχανήματα;

```
root@PC1:~ # ifconfig em0 192.168.1.2/24
```

```
root@PC2:~ # ifconfig em0 192.168.2.2/24
```

```
root@PC:~ # ifconfig em0 192.168.1.1/24
root@PC:~ # ifconfig em1 192.168.2.1/24
```

1.2) Ποια γραμμή προσθέσατε στο /etc/rc.conf του R1 ώστε να ενεργοποιηθεί η λειτουργία προώθησης πακέτων IPv4;

```
gateway_enable="YES"
```

1.3) Προσθέστε στο PC1 στατική εγγραφή για το δίκτυο 192.168.2.0/24 που βρίσκεται ο υπολογιστής PC2.

```
root@PC1:~ # route add -net 192.168.2.0/24 192.168.1.1
add net 192.168.2.0: gateway 192.168.1.1
```

1.4) Εξετάστε τον πίνακα δρομολόγησης του PC1. Τι σημαίνουν οι σημαίες (flags) που παρατηρείτε για τη διαδρομή προς το 192.168.2.0/24; **Παρατηρούμε τις σημαίες UGS. Η σημαία U σημαίνει ότι η διαδρομή είναι ενεργή (up).**

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

Internet:
Destination        Gateway            Flags     Netif Expire
127.0.0.1          link#2             UH          lo0
192.168.1.0/24     link#1             U           em0
192.168.1.2        link#1             UHS         lo0
192.168.2.0/24     192.168.1.1        UGS         em0
```

Η σημαία G σημαίνει ότι ο προορισμός είναι πύλη, που θα αποφασίσει για το πώς θα προωθήσει τα πακέτα περαιτέρω. Η σημαία S σημαίνει ότι η διαδρομή έχει οριστεί στατικά.

1.5) Δοκιμάστε την εντολή ping από το PC1 στο PC2. Τι παρατηρείτε; **Το ping είναι ανεπιτυχές.**

```
root@PC1:~ # ping 192.168.2.2
PING 192.168.2.2 (192.168.2.2): 56 data bytes
^C
--- 192.168.2.2 ping statistics ---
6 packets transmitted, 0 packets received, 100.0% packet loss
```

1.6) Με χρήση του tcpdump στο R1 ελέγξτε εάν παράγονται πακέτα ICMP στο LAN1 και το LAN2. Εξηγήστε.

Παρατηρούμε ότι το PC1 στέλνει επιτυχώς ICMP Echo Requests τα οποία και λαμβάνει/προωθεί ο R1 ωστόσο δεν λαμβάνονται ICMP Echo Replies από τον R1/PC1. Αυτό συμβαίνει διότι παρόλο που έχουμε ορίσει εγγραφή στον πίνακα δρομολόγησης του PC1 ώστε να παραδίδονται ορθά τα πακέτα με προορισμό το PC2, δεν έχουμε κάνει το αντίστοιχο από τη μεριά του PC2 και έτσι τα ICMP Echo Replies δεν δρομολογούνται ορθά.

1.7) Προσθέστε στο PC2 στατική εγγραφή για το δίκτυο 192.168.1.0/24 όπου βρίσκεται ο υπολογιστής PC1.

```
root@PC2:~ # route add -net 192.168.1.0/24 192.168.2.1
add net 192.168.1.0: gateway 192.168.2.1
```

1.8) Δοκιμάστε πάλι την εντολή ping από το PC1 στο PC2. Υπάρχει τώρα επικοινωνία; **Ναι**

```
root@PC1:~ # ping 192.168.2.2
PING 192.168.2.2 (192.168.2.2): 56 data bytes
64 bytes from 192.168.2.2: icmp_seq=0 ttl=63 time=0.749 ms
64 bytes from 192.168.2.2: icmp_seq=1 ttl=63 time=1.505 ms
^C
--- 192.168.2.2 ping statistics ---
2 packets transmitted, 2 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.749/1.127/1.505/0.378 ms
```

1.9) Εξηγήστε γιατί δεν χρειάζεται να γίνει καμία αλλαγή στον πίνακα δρομολόγησης του R1.

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

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
```

Οι διεπαφές του R1 ανήκουν στα ίδια υποδίκτυα με τα αντίστοιχα μηχανήματα. Έτσι οι εγγραφές που ορίζονται αυτόματα στον πίνακα δρομολόγησης λόγω των διεπαφών εξυπηρετούν στο ταίριασμα των εκάστοτε προορισμών. (έχουμε ενεργοποιήσει την προώθηση πακέτων)

Άσκηση 2: Proxy ARP

Για το PC3:

```
root@PC:~ # ifconfig em0 192.168.2.3/24
root@PC:~ # ping 192.168.2.2
PING 192.168.2.2 (192.168.2.2): 56 data bytes
64 bytes from 192.168.2.2: icmp_seq=0 ttl=64 time=1.972 ms
64 bytes from 192.168.2.2: icmp_seq=1 ttl=64 time=0.644 ms
^C
--- 192.168.2.2 ping statistics ---
2 packets transmitted, 2 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.644/1.308/1.972/0.664 ms
```

2.1) Στο PC1 καταργήστε τη στατική εγγραφή για το δίκτυο 192.168.2.0/24.

```
root@PC1:~ # route del 192.168.2.0/24
del net 192.168.2.0
```

2.2) Αλλάξτε στο PC1 το μήκος προθέματος της IPv4 διεύθυνσης από /24 σε /20.

```
root@PC1:~ # ifconfig em0 192.168.1.2/20
```

2.3) Από την προοπτική του PC1, τα PC2 και PC3 βρίσκονται στο ίδιο ή σε διαφορετικό υποδίκτυο IP; **Στο ίδιο**

2.4) Κάντε ping από το PC1 στα PC2 και PC3. Είναι επιτυχές; **Όχι**

```
root@PC1:~ # ping 192.168.2.2
PING 192.168.2.2 (192.168.2.2): 56 data bytes
^C
--- 192.168.2.2 ping statistics ---
3 packets transmitted, 0 packets received, 100.0% packet loss
```

```
root@PC1:~ # ping 192.168.2.3
PING 192.168.2.3 (192.168.2.3): 56 data bytes
^C
--- 192.168.2.3 ping statistics ---
3 packets transmitted, 0 packets received, 100.0% packet loss
```

Ενεργοποιούμε τη λειτουργία proxy ARP στον δρομολογητή.

2.5) Επαναλάβετε το ping από το PC1 στο PC2 στέλνοντας 1 πακέτο ICMP request. Είναι το ping επιτυχές; **Ναι**

```
root@PC1:~ # ping -c 1 192.168.2.2
PING 192.168.2.2 (192.168.2.2): 56 data bytes
64 bytes from 192.168.2.2: icmp_seq=0 ttl=63 time=1.683 ms

--- 192.168.2.2 ping statistics ---
1 packets transmitted, 1 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 1.683/1.683/1.683/0.000 ms
```

Όταν η λειτουργία proxy ARP δεν ήταν ενεργοποιημένη, το ping δεν ήταν επιτυχές διότι το ARP Request για τη διεύθυνση 192.168.2.2 δεν έπαιρνε Reply.

(Όπως υποδείξαμε σε προηγούμενο ερώτημα το PC1 βλέπει το PC2 στο ίδιο υποδίκτυο και σύμφωνα με τον πίνακα προώθησής του προωθεί το πακέτο στο LAN1, και άρα προβαίνει σε ARP Request στο LAN1 για την IPv4 του PC2)

Με ενεργοποιημένη τη λειτουργία proxy ARP στο R1, ο δρομολογητής απαντά στο ARP Request με την δική του διεύθυνση MAC αφού βλέπει ότι η διεύθυνση IPv4 του ARP Request ανήκει σε υπολογιστή υποδικτύου που είναι συνδεδεμένο με αυτόν. Άρα το ICMP Echo Request στέλνεται στον R1 και αυτός με τη σειρά του προωθεί το πακέτο στον PC2. Το Echo Reply στέλνεται επιτυχώς από τον PC2 αφού είχαμε προσθέσει εγγραφή στον πίνακα δρομολόγησής του για το υποδίκτυο 192.168.1.0/24 να κατευθύνει την κίνηση στην διεπαφή 192.168.2.1.

2.6) Επαναλάβετε το ping από το PC1 στο PC3. Γιατί αποτυγχάνει;

```
root@PC1:~ # ping 192.168.2.3
PING 192.168.2.3 (192.168.2.3): 56 data bytes
^C
--- 192.168.2.3 ping statistics ---
2 packets transmitted, 0 packets received, 100.0% packet loss
```

Αποτυγχάνει διότι η διεύθυνση προορισμού (που ανήκει στον PC1) του ICMP Echo Reply δεν βρίσκει ταίριασμα στον πίνακα δρομολόγησης και συνεπώς το πακέτο απορρίπτεται. (Το PC3 δεν βλέπει το PC1 στο ίδιο υποδίκτυο).

2.7) Προσθέστε στατική εγγραφή στο PC3 για το δίκτυο 192.168.1.0/24.

```
root@PC:~ # route add -net 192.168.1.0/24 192.168.2.1
add net 192.168.1.0: gateway 192.168.2.1
```

2.8) Καθαρίστε στα PC1, PC3 και R1 τον πίνακα ARP. **arp -da**

2.9) Ξεκινήστε καταγραφές στον R1 για το LAN1 και το LAN2, φροντίζοντας να εμφανίζονται στην οθόνη και οι διευθύνσεις MAC των πλαισίων που τα μεταφέρουν, και επαναλάβετε το προηγούμενο ping στέλνοντας 1 ακριβώς πακέτο ICMP request. **tcpdump -i em0 -e -vvv, tcpdump -i em1 -e -vvv, ping -c 1 192.168.2.3**

2.10) Τι παρατηρείτε στην απάντηση του R1 στο ARP request που λαμβάνει από το PC1;

```
root@PC1:~ # ping -c 1 192.168.2.3
PING 192.168.2.3 (192.168.2.3): 56 data bytes
64 bytes from 192.168.2.3: icmp_seq=0 ttl=63 time=2.290 ms

--- 192.168.2.3 ping statistics ---
1 packets transmitted, 1 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 2.290/2.290/2.290/0.000 ms
```

Απαντάει με τη MAC της διεπαφής του στο LAN1

```
Mar 23 14:18:49 PC login[888]: ROOT LOGIN (root) ON ttyv1
14:19:14.593846 08:00:27:d1:96:68 (oui Unknown) > Broadcast, ethertype ARP (0x08
06), length 60: Ethernet (len 6), IPv4 (len 4), Request who-has 192.168.2.3 tell
 192.168.1.2, length 46
14:19:14.593861 08:00:27:e9:9f:d5 (oui Unknown) > 08:00:27:d1:96:68 (oui Unknown
), ethertype ARP (0x0806), length 42: Ethernet (len 6), IPv4 (len 4), Reply 192.
168.2.3 is-at 08:00:27:e9:9f:d5 (oui Unknown), length 28
```

2.11) Προς ποια διεύθυνση MAC αποστέλλει το PC1 το πακέτο ICMP request; **Στη MAC της διεπαφής του R1 στο LAN1**

```
14:19:14.594392 08:00:27:d1:96:68 (oui Unknown) > 08:00:27:e9:9f:d5 (oui Unknown
), ethertype IPv4 (0x0800), length 98: (tos 0x0, ttl 64, id 30717, offset 0, fla
gs [none], proto ICMP (1), length 84)
    192.168.1.2 > 192.168.2.3: ICMP echo request, id 49667, seq 0, length 64
```

2.12) Από ποια διεύθυνση MAC λαμβάνει το πακέτο ICMP request το PC3; **Από τη MAC της διεπαφής του R1 στο LAN2**

```
14:19:14.594720 08:00:27:9e:7e:4e (oui Unknown) > 08:00:27:d4:97:27 (oui Unknown
), ethertype IPv4 (0x0800), length 98: (tos 0x0, ttl 63, id 30717, offset 0, fla
gs [none], proto ICMP (1), length 84)
    192.168.1.2 > 192.168.2.3: ICMP echo request, id 49667, seq 0, length 64
```

2.13) Σχεδιάστε την ανταλλαγή όλων των πακέτων (ICMP και ARP) που παρατηρήσατε μεταξύ των PC1, PC3 και R1 σημειώνοντας το είδος τους και δίνοντας μια σύντομη εξήγηση του σκοπού τους.

PC1 Broadcast ARP Request για την IPv4 του PC3

R1 ARP Reply στον PC1 δίνοντας την δική του διεύθυνση MAC για την IPv4 του PC3

PC1 ICMP Echo Request με διεύθυνση προορισμού την IPv4 του PC3 και MAC διεπαφής του R1

R1 Broadcast ARP Request για την IPv4 του PC3

PC3 ARP Reply στον R1

R1 προωθεί το ICMP Echo Request με διεύθυνση προορισμού την IPv4 του PC3 και MAC αυτή του PC3.

PC3 ICMP Echo Reply με διεύθυνση προορισμού την IPv4 του PC1 και MAC διεπαφής του R1

R1 Broadcast ARP Request για την IPv4 του PC1

PC1 ARP Reply στον R1

R1 προωθεί το ICMP Echo Reply με διεύθυνση προορισμού την IPv4 του PC1 και MAC αυτή του PC1.

2.14) Ποια είναι η μεγαλύτερη τιμή μήκους προθέματος (δηλαδή, το μικρότερο μέγεθος υποδικτύου) που μπορεί να τεθεί στο PC1 ώστε να συνεχίσει να λειτουργεί το παραπάνω ping;

Όπως αναφέραμε και σε προηγούμενο ερώτημα, αφού δεν έχουμε προσθέσει εγγραφή για την IPv4 του PC3 για να προωθηθεί ένα πακέτο στην διεπαφή του PC1 πρέπει να υπάρχει ταίριασμα με μια υπάρχουσα εγγραφή στον πίνακα δρομολόγησής του. Στον πίνακα αυτόν υπάρχει μόνο η εγγραφή για το ίδιο υποδίκτυο του PC1. Συνεπώς για να βρούμε την μεγαλύτερη τιμή μήκους προθέματος αρκεί να αναλογιστούμε ποιο είναι το μέγιστο subnet mask ώστε το PC3 να ανήκει στο ίδιο υποδίκτυο με το PC1. Παρατηρούμε ότι η μεγαλύτερη τιμή μήκους προθέματος είναι 22 bits.

2.15) Ορίστε στο PC1 ως μήκος προθέματος την αμέσως μεγαλύτερη τιμή από αυτήν που βρήκατε προηγουμένως, ώστε το ping να αποτυγχάνει.

```
root@PC1:~ # ifconfig em0 192.168.1.2/23
root@PC1:~ # ping -c 1 192.168.2.3
PING 192.168.2.3 (192.168.2.3): 56 data bytes
ping: sendto: No route to host
^C
--- 192.168.2.3 ping statistics ---
1 packets transmitted, 0 packets received, 100.0% packet loss
```

2.16) Στο PC1 ορίστε ως επόμενο βήμα για το δίκτυο 192.168.2.0/24 τη διεπαφή του στο LAN1.

```
root@PC1:~ # route add -net 192.168.2.0/24 -interface em0
add net 192.168.2.0: gateway em0
```

2.17) Τι εμφανίζεται στο πίνακα δρομολόγησης του PC1 ως πύλη για το δίκτυο 192.168.2.0/24; **Η MAC του PC1 στοLAN1**

2.18) Είναι τώρα το ping προς τον PC3 επιτυχές; Γιατί; **Ναι είναι επιτυχές λόγω του δρομολογητή που είναι proxy.**

2.19) Στον R1 ακυρώστε τη λειτουργία proxy ARP. **sysctl net.link.ether.inet.proxyall=0**

2.20) Στο PC1 με χρήση μίας μόνο εντολής ορίστε ως επόμενο βήμα για το 192.168.2.0/24 τον R1.

```
root@PC1:~ # route change 192.168.2.0/24 192.168.1.1
change net 192.168.2.0: gateway 192.168.1.1
```

2.21) Στο PC1 επαναφέρετε το μήκος προθέματος δικτύου στην αρχική τιμή /24.

```
root@PC1:~ # ifconfig em0 192.168.1.2/24
```

2.22) Τι έχει συμβεί στη διαδρομή προς το 192.168.2.0/24 που προ ολίγου ορίσατε;

Διεγράφη από τον πίνακα δρομολόγησης

2.23) Ορίστε πάλι τη δ

```
root@PC:~ # route add -net 192.168.1.0/24 172.17.17.1
add net 192.168.1.0: gateway 172.17.17.1
root@PC1:~ # route add -net 192.168.2.0/24 192.168.1.1
add net 192.168.2.0: gateway 192.168.1.1
```

Άσκηση 3: Δρομολόγηση σε περισσότερα βήματα

3.1) Ορίστε διευθύνσεις IPv4 στις διεπαφές του R1 στα τοπικά δίκτυα LAN1 και WAN1.

```
root@PC:~ # ifconfig em0 192.168.1.1/24
root@PC:~ # ifconfig em1 172.17.17.1/30
```

3.2) Ορίστε διευθύνσεις IPv4 στις διεπαφές του R2 στα τοπικά δίκτυα WAN1 και LAN2.

```
root@PC:~ # ifconfig em0 192.168.2.1/24
root@PC:~ # ifconfig em1 172.17.17.2/30
```

3.3) Δοκιμάστε πάλι την εντολή ping από το PC1 στο PC2. Τι είδους ένδειξη λάθους παρατηρείτε;

```
root@PC1:~ # ping -c 1 192.168.2.2
PING 192.168.2.2 (192.168.2.2): 56 data bytes
92 bytes from 192.168.1.1: Destination Host Unreachable
Vr HL TOS  Len   ID Flg  off TTL Pro  cks      Src      Dst
 4  5  00 0054 7833   0 0000  3f  01 7f21 192.168.1.2  192.168.2.2
```

3.4) Με χρήση του tcpdump ελέγξτε εάν και τι είδους μηνύματα ICMP παράγονται στο LAN1. Παράγονται μηνύματα ICMP στο WAN1; Εξηγήστε τι συμβαίνει. **Στο LAN1 παράγονται ICMP Echo Requests από τον PC1 και ICMP host unreachable από τον R1. Δεν παράγονται πλαίσια στο WAN1. Ο R1 δεν έχει εγγραφή στον πίνακα δρομολόγησής του για το υποδίκτυο 192.168.2.0/24.**

3.5) Δοκιμάστε τώρα την εντολή traceroute από το PC1 στο PC2. Τι σημαίνει η ένδειξη λάθους που παρατηρείτε;

```
root@PC1:~ # traceroute 192.168.2.2
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)  0.626 ms  0.417 ms  1.027 ms
 2  192.168.1.1 (192.168.1.1)  0.859 ms !H  0.875 ms !H  0.839 ms !H
```

Ένδειξη λάθους: !H (destination unreachable)

3.6) Προσθέσετε στον R1 στατική εγγραφή για το 192.168.2.0/24 μέσω του R2

```
root@PC:~ # route add -net 192.168.2.0/24 172.17.17.2
add net 192.168.2.0: gateway 172.17.17.2
```

3.7) Μπορείτε τώρα να κάνετε ping από το PC1 στο PC2; **Όχι**

3.8) Τι είδους μηνύματα ICMP παρατηρείτε στο LAN2 και για ποιο λόγο παράγεται το καθένα;

Παρατηρούμε ICMP Echo Request, ICMP Echo Reply και ICMP host 192.168.12 unreachable

3.9) Δοκιμάστε ξανά την εντολή traceroute από το PC1 στο PC2. Παρατηρείτε μηνύματα ICMP echo request στο WAN1; Εάν όχι, παράγονται άλλου είδους μηνύματα; Γιατί συμβαίνει αυτό; **Δεν παρατηρούμε μηνύματα ICMP Echo Request αλλά UDP datagrams. Η υλοποίηση της traceroute είναι τέτοια ώστε το πακέτο από τον υπολογιστή στον πρώτο δρομολογητή να είναι τυπικά ICMP Echo Request. Ωστόσο οι ενδιάμεσοι δρομολογητές δεν ανταποκρίνονται στα ICMP Echo Requests για λόγους ασφαλείας. Για αυτό τον λόγο η traceroute αποστέλλει UDP πακέτα με υψηλή θύρα προορισμού ώστε να προκληθεί ICMP "port unreachable" από τους δρομολογητές προς τον υπολογιστή.**

3.10) Τι είδους μηνύματα παράγονται στο LAN2;

```
192.168.2.2 > 192.168.1.2: ICMP 192.168.2.2 udp port 33445 unreachable,
```

3.11) Γιατί δεν παρατηρείτε στο LAN2 ICMP host unreachable; **Γιατί ο υπολογιστής-στόχος παρέλαβε UDP πακέτα**

3.12) Προσθέστε στον R2 στατική εγγραφή για το 192.168.1.0/24 μέσω του R1.

3.13) Μπορείτε τώρα να κάνετε traceroute από το PC1 στο PC2; **Ναι μπορούμε**

Τι είδους μηνύματα ICMP παράγονται στο WAN1 και για ποιο λόγο;

```
root@PC1:~ # traceroute 192.168.2.2
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)  0.001 ms  0.000 ms  4.032 ms
 2  172.17.17.2 (172.17.17.2)  0.765 ms  0.448 ms  0.425 ms
 3  192.168.2.2 (192.168.2.2)  0.887 ms  0.906 ms  0.860 ms
```

```
172.17.17.2 > 192.168.1.2: ICMP time exceeded in-transit,
```

```
192.168.2.2 > 192.168.1.2: ICMP 192.168.2.2 udp port 33441 unreachable,
```

Τα μηνύματα ICMP time exceeded in-transit παράγονται διότι η traceroute αποστέλλει πακέτα με μεταβλητό TTL ώστε να ανακαλύψει τους ενδιάμεσους κόμβους. Κάθε φορά που ένα πακέτο περνάει από έναν δρομολογητή η τιμή TTL μειώνεται κατά ένα. Μόλις γίνει μηδέν η τιμή αυτή σε έναν ενδιάμεσο δρομολογητή αποστέλλεται στην πηγή του πακέτου μήνυμα ICMP time exceeded in-transit.

3.14) Κάντε ping από το PC2 στη διεύθυνση 172.17.17.1. Τι παρατηρείτε;

```
root@PC2:~ # ping 172.17.17.1
PING 172.17.17.1 (172.17.17.1): 56 data bytes
ping: sendto: No route to host
ping: sendto: No route to host
^C
--- 172.17.17.1 ping statistics ---
2 packets transmitted, 0 packets received, 100.0% packet loss
```

3.15) Διαγράψτε στο PC2 τη στατική εγγραφή για το 192.168.1.0/24.

```
root@PC2:~ # route del 192.168.1.0/24
del net 192.168.1.0
```

3.16) Προσθέστε στο PC2 ως προεπιλεγμένη πύλη την 192.168.2.1.

```
root@PC2:~ # route add default 192.168.2.1
add net default: gateway 192.168.2.1
```

3.17) Κάντε πάλι ping από το PC2 στη διεύθυνση 172.17.17.1. Τι παρατηρείτε τώρα;

```
root@PC2:~ # ping 172.17.17.1
PING 172.17.17.1 (172.17.17.1): 56 data bytes
64 bytes from 172.17.17.1: icmp_seq=0 ttl=63 time=1.995 ms
64 bytes from 172.17.17.1: icmp_seq=1 ttl=63 time=0.907 ms
^C
--- 172.17.17.1 ping statistics ---
2 packets transmitted, 2 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.907/1.451/1.995/0.544 ms
```

3.18) Εξηγήστε τη διαφορετική συμπεριφορά που παρατηρήσατε στα δύο προηγούμενα ping.

Στο πρώτο ping για την εν λόγω διεύθυνση δεν υπήρχε ταίριασμα στον πίνακα δρομολόγησης του PC2 και συνεπώς το πακέτο απορρίπτονταν. Στο δεύτερο ping πάλι δεν υπάρχει ταίριασμα, ωστόσο το πακέτο δεν απορρίπτεται αλλά αποστέλλεται στην προεπιλεγμένη πύλη. Αυτή με τη σειρά της προωθεί το πακέτο στο R1 και αντίστροφα και συνεπώς έχουμε επιτυχή επικοινωνία.

Άσκηση 4: Ένα πιο πολύπλοκο δίκτυο με εναλλακτικές διαδρομές

4.1) Ενεργοποιήστε τη διεπαφή του PC3 στο LAN2 και ορίστε διεύθυνση IPv4.

```
root@PC:~ # ifconfig em0 up
root@PC:~ # ifconfig em0 192.168.2.3/24
```

4.2) Στο PC3 ορίστε στατική διαδρομή για το υποδίκτυο 192.168.1.0/24 μέσω του R2.

```
root@PC:~ # route add -net 192.168.1.0/24 192.168.2.1
add net 192.168.1.0: gateway 192.168.2.1
```

4.3) Σε ποια εσωτερικά δίκτυα του VirtualBox πρέπει να βρίσκονται οι κάρτες δικτύου του R1 και με ποιες εντολές φλοιού θα ορίσετε τις IP διευθύνσεις τους; **Δίκτυα LAN1, WAN1, WAN2**

```
root@PC:~ # ifconfig em0 192.168.1.1/24
root@PC:~ # ifconfig em1 172.17.17.1/30
root@PC:~ # ifconfig em2 172.17.17.5/30
```

4.4) Σε ποια εσωτερικά δίκτυα του VirtualBox πρέπει να βρίσκονται οι κάρτες δικτύου του R2 και με ποιες εντολές φλοιού θα ορίσετε τις IP διευθύνσεις τους; **Δίκτυα LAN2, WAN1, WAN3**

```
root@PC:~ # ifconfig em0 192.168.2.1/24
root@PC:~ # ifconfig em1 172.17.17.2/30
root@PC:~ # ifconfig em2 172.17.17.9/30
```

4.5) Σε ποια εσωτερικά δίκτυα του VirtualBox πρέπει να βρίσκονται οι κάρτες δικτύου του R3 και με ποιες εντολές φλοιού θα ορίσετε τις IP διευθύνσεις τους; **WAN2, WAN3**

```
root@PC:~ # ifconfig em0 172.17.17.6/30
root@PC:~ # ifconfig em1 172.17.17.10/30
```

4.6) Προσθέστε στατική εγγραφή στον R1 ώστε να προωθεί πακέτα για το LAN2 μέσω του R2.

```
root@PC:~ # route add -net 192.168.2.0/24 172.17.17.2
add net 192.168.2.0: gateway 172.17.17.2
```

4.7) Προσθέστε στατική εγγραφή στον R2 ώστε να προωθεί πακέτα για το LAN1 μέσω του R1.

```
root@PC:~ # route add -net 192.168.1.0/24 172.17.17.1
add net 192.168.1.0: gateway 172.17.17.1
```

4.8) Προσθέστε στατικές εγγραφές στον R3 ώστε να προωθεί πακέτα για το LAN1 μέσω του R1 και για LAN2 μέσω R2.

```
root@PC:~ # route add -net 192.168.1.0/24 172.17.17.5
add net 192.168.1.0: gateway 172.17.17.5
root@PC:~ # route add -net 192.168.2.0/24 172.17.17.9
add net 192.168.2.0: gateway 172.17.17.9
```

4.9) Προσθέστε στον R1 στατική εγγραφή για το PC3 μέσω του R3. Ποια σημαία στον πίνακα δρομολόγησης δηλώνει ότι είναι διαδρομή προς υπολογιστή;

```
root@PC:~ # route add -host 192.168.2.3 172.17.17.6
add host 192.168.2.3: gateway 172.17.17.6
```

Η σημαία 'G' υποδηλώνει ότι η εγγραφή αφορά συγκεκριμένη διεπαφή.

4.10) Δοκιμάστε traceroute από το PC1 στο PC2. Πόσα βήματα βλέπετε; **3 βήματα**

```
root@PC1:~ # traceroute 192.168.2.2
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)  0.472 ms  0.325 ms  0.287 ms
 2  172.17.17.2 (172.17.17.2)  3.316 ms  0.457 ms  0.453 ms
 3  192.168.2.2 (192.168.2.2)  2.057 ms  0.764 ms  0.708 ms
```

4.11) Δοκιμάστε ping από το PC1 στο PC2. Πόσα βήματα βλέπετε από την τιμή του TTL3; **2 βήματα**

```
root@PC1:~ # ping 192.168.2.2
PING 192.168.2.2 (192.168.2.2): 56 data bytes
64 bytes from 192.168.2.2: icmp_seq=0 ttl=62 time=1.041 ms
64 bytes from 192.168.2.2: icmp_seq=1 ttl=62 time=1.035 ms
^C
--- 192.168.2.2 ping statistics ---
2 packets transmitted, 2 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 1.035/1.038/1.041/0.003 ms
```

4.12) Δοκιμάστε traceroute από το PC1 στο PC3. Πόσα βήματα βλέπετε; **4 βήματα**

```
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)  0.000 ms  0.326 ms  0.273 ms
 2  172.17.17.6 (172.17.17.6)  2.860 ms  0.677 ms  0.727 ms
 3  172.17.17.2 (172.17.17.2)  4.307 ms  0.821 ms  0.869 ms
 4  192.168.2.3 (192.168.2.3)  1.570 ms  1.108 ms  1.020 ms
```

4.13) Δοκιμάστε ping από το PC1 στο PC3. Πόσα βήματα βλέπετε από την τιμή του TTL; **2 βήματα**

```
root@PC1:~ # ping 192.168.2.3
PING 192.168.2.3 (192.168.2.3): 56 data bytes
64 bytes from 192.168.2.3: icmp_seq=0 ttl=62 time=1.435 ms
64 bytes from 192.168.2.3: icmp_seq=1 ttl=62 time=1.204 ms
^C
--- 192.168.2.3 ping statistics ---
2 packets transmitted, 2 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 1.204/1.320/1.435/0.116 ms
```

4.14) Ποια από τις δύο διαδρομές προς το PC3 ακολουθεί το ICMP Echo request; **PC1 -> R1 -> R3 -> R2 -> PC3**
Η διαδρομή του ICMP Echo request φαίνεται από την traceroute. Έχουμε ορίσει εγγραφή στον R1 συγκεκριμένα με προορισμό τον PC3 να προωθεί τα πακέτα προς R3.

4.15) Ποια από τις δύο διαδρομές προς το PC1 ακολουθεί το ICMP Echo reply; Δικαιολογήστε. **PC3-> R2 -> R1->PC1**
Στο ping βλέπουμε τις πληροφορίες για το ICMP Echo reply. Έχουμε ορίσει εγγραφή στον R2 να προωθεί την κίνηση στον R2 για το δίκτυο του LAN1.

4.16) Προσομοιώστε βλάβη στη σύνδεση του R1 προς το WAN1 απενεργοποιώντας την αντίστοιχη διεπαφή και ξεκινήστε μια καταγραφή στον R2 ώστε να συλλαμβάνονται πακέτα στο LAN2. **tcpdump -i emo**

4.17) Δοκιμάστε traceroute από το PC1 στο PC2. Αφήστε να ολοκληρωθούν τουλάχιστον 3 βήματα. Παρατηρείτε να φτάνουν ή παράγονται πακέτα UDP στο PC2; **Όχι, δεν φτάνουν ούτε παράγονται πακέτα στο PC**

```
root@PC1:~ # traceroute 192.168.2.2
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)  0.794 ms  0.360 ms  0.304 ms
 2  * * *
 3  * * *
 4  * * *
```

4.18) Δοκιμάστε τώρα traceroute από το PC1 στο PC3. Αφήστε να ολοκληρωθούν τουλάχιστον 4 βήματα. Παρατηρείτε να φτάνουν ή παράγονται πακέτα UDP στο PC3;

Ναι φτάνουν πακέτα UDP στο PC3 όπως φαίνονται παρακάτω

```
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)  0.528 ms  0.306 ms  0.278 ms
 2  172.17.17.6 (172.17.17.6)  0.813 ms  0.537 ms  0.500 ms
 3  * * *
 4  * * *
```

```
17:29:07.899794 IP 192.168.1.2.34344 > 192.168.2.3.33444: UDP, length 12
```

4.19) Χρησιμοποιώντας μία φορά την εντολή route αλλάξτε στους πίνακες δρομολόγησης των R1 και R2 τις υπάρχουσες διαδρομές προς τα LAN1 και LAN2 ώστε όλη η κίνηση μεταξύ τους να διέρχεται μέσω του R3; Επιβεβαιώστε ότι μετά την αλλαγή υπάρχει επικοινωνία κάνοντας traceroute όπως πριν.

```
root@PC:~ # route change -net 192.168.2.0/24 172.17.17.6
change net 192.168.2.0: gateway 172.17.17.6
root@PC:~ # route change -net 192.168.1.0/24 172.17.17.10
change net 192.168.1.0: gateway 172.17.17.10
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)  0.440 ms  0.322 ms  0.298 ms
 2  172.17.17.6 (172.17.17.6)  0.865 ms  0.561 ms  0.560 ms
 3  172.17.17.9 (172.17.17.9)  1.222 ms  0.743 ms  0.782 ms
 4  192.168.2.3 (192.168.2.3)  1.694 ms  1.573 ms  1.793 ms
root@PC1:~ # traceroute 192.168.2.2
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)  0.459 ms  0.331 ms  0.311 ms
 2  172.17.17.6 (172.17.17.6)  0.606 ms  0.592 ms  0.509 ms
 3  172.17.17.9 (172.17.17.9)  0.753 ms  0.734 ms  0.635 ms
 4  192.168.2.2 (192.168.2.2)  1.990 ms  1.483 ms  1.202 ms
```

4.20) Στον R1 με τη βοήθεια της εντολής route δείτε την πληροφορία για τις διαδρομές προς τις διευθύνσεις IPv4 των PC2 και PC3. Ποια διαφορά παρατηρείτε;

Παρατηρούμε ότι για το PC2 υπάρχει εγγραφή για το υποδίκτυο του ενώ για το PC3 υπάρχει εγγραφή προς τον συγκεκριμένο host.

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

Internet:
Destination        Gateway            Flags      Netif Expire
127.0.0.1          link#4             UH          lo0
172.17.17.0/30     link#2             U           em1
172.17.17.1        link#2             UHS         lo0
172.17.17.4/30     link#3             U           em2
172.17.17.5        link#3             UHS         lo0
192.168.1.0/24     link#1             U           em0
192.168.1.1        link#1             UHS         lo0
192.168.2.0/24     172.17.17.6        UGS         em2
192.168.2.3        172.17.17.6        UGHS        em2
```

4.21) Ποια από τις εγγραφές του πίνακα δρομολόγησης στον R1 επιλέγεται όταν κάνετε ping από το PC1 στο PC3;

Επιλέγεται η εγγραφή που περιέχει την διεύθυνση IPv4 του PC3 αφού ακολουθείται ο κανόνας του μέγιστου ταιριάσματος.

Άσκηση 5: Βρόχοι κατά τη δρομολόγηση

5.1) Τροποποιήστε στον R3 την υπάρχουσα στατική εγγραφή για το δίκτυο 192.168.2.0/24 ώστε να στέλνει την κίνηση στον R1 αντί στον R2.

```
root@PC:~ # route change -net 192.168.2.0/24 172.17.17.5
change net 192.168.2.0: gateway 172.17.17.5
```

5.2) Εκτελέστε ping στέλνοντας ένα μόνο ICMP Echo request από το PC1 στο PC2. Είναι το ping επιτυχές; **Όχι**

```
root@PC1:~ # ping -c 1 192.168.2.2
PING 192.168.2.2 (192.168.2.2): 56 data bytes
92 bytes from 192.168.1.1: Redirect Host(New addr: 0.0.0.0)
Vr HL TOS  Len   ID Flg  off TTL Pro  cks      Src      Dst
 4  5  00 0054 7a6b   0 0000  3d  01 7ee9 192.168.1.2  192.168.2.2

92 bytes from 172.17.17.6: Redirect Host(New addr: 0.0.0.0)
Vr HL TOS  Len   ID Flg  off TTL Pro  cks      Src      Dst
 4  5  00 0054 7a6b   0 0000  3e  01 7de9 192.168.1.2  192.168.2.2

92 bytes from 192.168.1.1: Redirect Host(New addr: 0.0.0.0)
Vr HL TOS  Len   ID Flg  off TTL Pro  cks      Src      Dst
 4  5  00 0054 7a6b   0 0000  3b  01 80e9 192.168.1.2  192.168.2.2
```

5.3) Περιγράψτε τι συμβαίνει. Από ποια διεπαφή προέρχεται το μήνυμα λάθους που εμφανίζεται;
Οι διεπαφές 192.168.1.1 (του R1) και 172.17.17.6 (του R3) στέλνουν η μία το πακέτο στην άλλη αποστέλλοντας μήνυμα Redirect Host. Redirects συμβαίνουν όταν ένας δρομολογητής πιστεύει ότι ένα πακέτο έχει δρομολογηθεί μη αποδοτικά και ενημερώνει τον source host ότι πρέπει να προωθήσει τα πακέτα από διαφορετική πύλη.
Εδώ η νέα διεύθυνση που υποδεικνύεται από το Redirect είναι η 0.0.0.0 η οποία συμβολίζει μη έγκυρη ή άγνωστη διεύθυνση. Όταν μια συσκευή είναι ρυθμισμένη να στείλει την κίνηση στη διεύθυνση αυτή τότε απορρίπτει τα πακέτα. (Με τη διεύθυνση 0.0.0.0/0 συμβολίζουμε την προεπιλεγμένη πύλη, αλλά δεν έχουμε τέτοια εγγραφή εδώ)
Εμφανίζεται ακόμη μήνυμα λάθους ICMP time exceeded in-transit που στέλνεται από τον R2 καθώς το πακέτο παλινδρομεί μεταξύ των δρομολογητών, η τιμή TTL μειώνεται συνεχώς μέχρι να γίνει μηδέν και να σταλεί το εν λόγω μήνυμα σφάλματος.

5.4) Ξεκινήστε καταγραφή στη διεπαφή του R1 στο LAN1 αποθηκεύοντας τα αποτελέσματά της σε αρχείο. Αντίστοιχα στη διεπαφή του R3 στο WAN2.

```
root@PC:~ # tcpdump -i em0 -w log -A
```

5.5) Επαναλάβετε το προηγούμενο ping και όταν ολοκληρωθεί σταματήστε τις καταγραφές. Πόσα και ποιου είδους μηνύματα ICMP καταγράφηκαν στα LAN1 και WAN2; **Καταγράφηκαν 64 πακέτα ICMP στο LAN1, 1 ICMP Echo Request, 62 ICMP Redirect και 1 ICMP time exceeded in-transit.**
Καταγράφηκαν 95 πακέτα ICMP στο WAN2, 31 τριάδες μηνυμάτων 2 ICMP Echo Request- 1 ICMP Redirect και τέλος 1 ICMP Echo Request - 1 ICMP time exceeded in-transit.

5.6) Ξεκινήστε νέα καταγραφή στη διεπαφή του R3 στο WAN2 συλλαμβάνοντας μόνο μηνύματα ICMP Echo request, εμφανίζοντας λεπτομέρειες και χρησιμοποιώντας την επιλογή –e ώστε να διακρίνεται η διεπαφή που τα παράγει.

```
root@PC:~ # tcpdump -i em1 -w log -A -e -vvv "icmp[icmptype]==icmp-echo"
```

5.7) Εκτελέστε πάλι το προηγούμενο ping, περιμένετε να ολοκληρωθεί και σταματήστε την καταγραφή. Πόσα μηνύματα ICMP Echo request εμφανίσθηκαν στο WAN2; **Εμφανίστηκαν 63 ICMP Echo request στο WAN2.**
Πόσα έχουν ως πηγή τον R1 και πόσα τον R3; Αιτιολογήστε.
Το ICMP time exceeded in-transit εκπέμπεται από τον R3 και πριν από αυτό εκπέμπεται ICMP Echo request από τον R1 στο R3. Τα υπόλοιπα ICMP Echo request εκπέμπονται μισά μισά από τους R1-R3 καθώς ο ένας δρομολογητής στέλνει στον άλλον το πακέτο. Άρα ως πηγή τον R1 έχουν 32 πακέτα ενώ ως πηγή τον R3 έχουν 31.

5.8) Ξεκινήστε δύο νέες καταγραφές, μία στη διεπαφή του R1 στο LAN1 και μία στη διεπαφή του R3 στο WAN2, συλλαμβάνοντας μόνο μηνύματα ICMP Redirect και εμφανίζοντας λεπτομέρειες.

```
root@PC:~ # tcpdump -i em0 -w log -A -e -vvv "icmp[icmptype]==icmp-redirect"
```

5.9) Επαναλάβετε το προηγούμενο ping και όταν ολοκληρωθεί σταματήστε τις καταγραφές. Πόσα ICMP Redirect εμφανίζονται στο WAN2; Αιτιολογήστε το πλήθος τους λαμβάνοντας υπόψη ότι ο R3 παράγει ένα για κάθε πακέτο IP που πρέπει να προωθήσει μέσω της διεπαφής από την οποία το έλαβε. **Εμφανίζονται 31 πακέτα ICMP Redirect στο WAN2. Όπως είδαμε στο ερώτημα 5.7, ως πηγή τον R3 έχουν 31 πακέτα. Αυτό συμβαίνει αφού ο R3 για κάθε πακέτο**

IP που πρέπει να προωθήσει παράγει και ένα ICMP Redirect.

5.10) Πόσα ICMP Redirect εμφανίζονται στο LAN1; Αιτιολογήστε το πλήθος αυτών που παράγει ο R1.

Εμφανίζονται 62 πακέτα ICMP Redirect στο LAN1. Παράγονται 31 λόγω της προώθησης των ICMP Echo request στον R1. (Από την πρώτη προώθηση στο R1 δεν παράγεται Redirect.) Παράγονται άλλα 31 λόγω του R3.

5.11) Ξεκινήστε νέες καταγραφές όπως στην ερώτηση 5.4 και εκτελέστε traceroute -I -q 1 από το PC1 στο PC2. Πόσα βήματα εμφανίζονται μέχρις ότου ολοκληρωθεί η εκτέλεση της εντολής; Ποια είναι η διαδρομή που καταγράφετε;

Εμφανίζονται 64 βήματα μέχρις ότου ολοκληρωθεί η εκτέλεση της εντολής. Διαδρομή: παλινδρόμηση R1-R3.

5.12) Σταματήστε τις καταγραφές. Πόσα μηνύματα ICMP Echo request στάλθηκαν από το PC1: **64**
και πόσα εμφανίσθηκαν στο WAN2;: **2016**
Αιτιολογήστε το πλήθος τους. **Υπενθυμίζεται ότι η λειτουργία της traceroute είναι η εξής: Προκειμένου να ανακαλυφθεί η διαδρομή προς τον προορισμό στέλνονται ICMP Echo Requests με μεταβαλλόμενη τιμή TTL, η οποία αρχίζει από το 1 και αυξάνεται κατά ένα μέχρι να βρεθεί ο προορισμός (είτε μέχρι μια μέγιστη τιμή, εδώ 64). Στη συγκεκριμένη περίπτωση παράγονται από τον PC1 64 ICMP Echo Requests, με τιμές TTL 1,2,... αφού δεν βρίσκουν τον προορισμό. Στη συνέχεια τα πακέτα παλινδρομούν μεταξύ των δρομολογητών R1-R3. Συνεπώς στο WAN2 έχουμε 1+2+3+...+63 ICMP Echo Request, δηλαδή (63+1)62/2 = 2016.**

5.13) Πόσα μηνύματα ICMP time exceeded εμφανίσθηκαν στο WAN2. Αιτιολογήστε το πλήθος τους.

```
root@PC:~ # tcpdump -i em0 -w log -A -e -vvv "icmp[icmptype]==icmp-timxceed"
```

Εμφανίστηκαν 32 ICMP time exceeded στο WAN2. Τα ICMP Echo Request με ζυγά TTL που παράγονται από το PC1 εν τέλει θα φτάσουν στον R3 με μηδενικό TTL και θα εκπεμφθεί ICMP time exceeded. Άρα 64/2=32.

5.14) Υποδείξτε έναν άλλο τρόπο για να μετρήσετε τα μηνύματα ICMP echo request ή ICMP time exceeded χωρίς να χρειαστεί να αποθηκεύσετε τα αποτελέσματα της tcpdump.

tcpdump -i emo -c "icmp[icmptype] == icmp-echo" , tcpdump -i emo -c "icmp[icmptype] == icmp-timxceed"

Άσκηση 6: Χωρισμός σε υποδίκτυα

6.1) Ποια είναι η διεύθυνση υποδικτύου του LAN1; **172.17.17.0/25**

6.2) Ποια είναι η διεύθυνση υποδικτύου του LAN2; **172.17.17.192/26 (Δεν χρησιμοποιούμε την .128 λόγω δρομολογητών)**

6.3) Ποια είναι η διεύθυνση υποδικτύου του LAN3; **172.17.17.160/27**

6.4) Στο υποδίκτυο του LAN1 ορίστε ως διεύθυνση IPv4 για το PC1 αυτή με τη μικρότερη τιμή host, ενώ για τον δρομολογητή R1 αυτή με τη μεγαλύτερη τιμή host. **PC1: 172.17.17.1/25, R1: 172.17.17.126/25**

6.5) Αντίστοιχα, στο υποδίκτυο του LAN3. **PC4: 172.17.17.161/27, R3: 172.17.17.190/27**

6.6) Στο υποδίκτυο του LAN2 ορίστε ως διεύθυνση IPv4 για τον δρομολογητή R2 αυτή με τη μικρότερη τιμή host, ενώ για PC2, PC3 αυτές με τις μεγαλύτερες τιμές host. **R2: 172.17.17.193/26, PC2: 172.17.17.253/26, PC3: 172.17.17.254/26**

Εντολή για τα παραπάνω ερωτήματα ifconfig em_ <IP address>

6.7) Στα PC ορίστε ως προεπιλεγμένη πύλη τους αντίστοιχους δρομολογητές. **route add default <IP address>**

6.8) Στον R1 ορίστε στατικές εγγραφές ώστε να προωθεί πακέτα για τα LAN2 και LAN3 μέσω του R2.

```
root@PC:~ # route add -net 172.17.17.192/26 172.17.17.130
add net 172.17.17.192: gateway 172.17.17.130
root@PC:~ # route add -net 172.17.17.160/27 172.17.17.130
add net 172.17.17.160: gateway 172.17.17.130
```

6.9) Στον R2 ορίστε στατικές εγγραφές ώστε να προωθεί πακέτα για τα LAN1 και LAN3 μέσω του R3.

```
root@PC:~ # route add -net 172.17.17.0/25 172.17.17.137
add net 172.17.17.0: gateway 172.17.17.137
root@PC:~ # route add -net 172.17.17.160/27 172.17.17.137
add net 172.17.17.160: gateway 172.17.17.137
```

6.10) Στον R3 ορίστε στατικές εγγραφές ώστε να προωθεί πακέτα για το LAN1 και LAN2 μέσω του R1.

```
root@PC:~ # route add -net 172.17.17.0/25 172.17.17.133
add net 172.17.17.0: gateway 172.17.17.133
root@PC:~ # route add -net 172.17.17.192/26 172.17.17.133
add net 172.17.17.192: gateway 172.17.17.133
```

6.11) Επιβεβαιώστε ότι υπάρχει επικοινωνία ανάμεσα σε όλα τα LAN κάνοντας ping από το PC1 στο PC2, το PC2 στο PC4 και από το PC3 το PC1. Εάν όχι, ελέγξτε πρώτα ότι έχετε αποδώσει σωστά τις διευθύνσεις IP στα υποδίκτυα και κατόπιν τις στατικές διαδρομές. **Τα ping είναι επιτυχή.**

Από το PC1 στο PC2:

```
root@PC1:~ # ping 172.17.17.253
PING 172.17.17.253 (172.17.17.253): 56 data bytes
64 bytes from 172.17.17.253: icmp_seq=0 ttl=61 time=2.622 ms
64 bytes from 172.17.17.253: icmp_seq=1 ttl=61 time=1.344 ms
^C
--- 172.17.17.253 ping statistics ---
2 packets transmitted, 2 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 1.344/1.983/2.622/0.639 ms
```

Από το PC2 στο PC4:

```
root@PC2:~ # ping 172.17.17.161
PING 172.17.17.161 (172.17.17.161): 56 data bytes
64 bytes from 172.17.17.161: icmp_seq=0 ttl=61 time=1.632 ms
64 bytes from 172.17.17.161: icmp_seq=1 ttl=61 time=1.228 ms
^C
--- 172.17.17.161 ping statistics ---
2 packets transmitted, 2 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 1.228/1.430/1.632/0.202 ms
```

Από το PC3 το PC1:

```
root@PC:~ # ping 172.17.17.1
PING 172.17.17.1 (172.17.17.1): 56 data bytes
64 bytes from 172.17.17.1: icmp_seq=0 ttl=62 time=1.310 ms
64 bytes from 172.17.17.1: icmp_seq=1 ttl=62 time=1.566 ms
^C
--- 172.17.17.1 ping statistics ---
2 packets transmitted, 2 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 1.310/1.438/1.566/0.128 ms
```

Άσκηση 7: Ταυτόσημες διευθύνσεις IP

7.1) Σημειώστε τις διευθύνσεις MAC των PC2 και PC3.

PC2: `ether 08:00:27:b6:86:41` **PC3:** `ether 08:00:27:d4:97:27`

7.2) Αλλάξτε την IPv4 διεύθυνση του PC2 ώστε να γίνει ίδια με αυτήν του PC3.

```
root@PC2:~ # ifconfig em0 172.17.17.254/26
```

7.3) Λάβατε κάποια ένδειξη λάθους στην προσπάθειά σας να ορίσετε τη διεύθυνση IP του PC2; **Ναι**

```
Mar 28 02:48:51 PC2 kernel: arp: 08:00:27:d4:97:27 is using my IP address 172.17
.17.254 on em0!
```

7.4) Εμφανίσθηκε αντίστοιχη ένδειξη λάθους στο PC3; **Ναι**

```
Mar 28 02:48:50 PC kernel: arp: 08:00:27:b6:86:41 is using my IP address 172.17.
17.254 on em0!
```

7.5) Έχει ορισθεί η διεύθυνση IPv4 στο PC2; Ποιο είναι τότε το νόημα των μηνυμάτων λάθους;

Με τη βοήθεια της εντολής ifconfig emo στο PC2 παρατηρούμε ότι η διεύθυνση IPv4 έχει ορισθεί. Το νόημα των μηνυμάτων λάθους είναι να ενημερώσει τον διαχειριστή του συστήματος ότι δύο διαφορετικά μηχανήματα έχουν την ίδια IPv4, γεγονός που μπορεί να προκαλέσει σφάλματα.

7.6) Παραμένει ο R2 ως προεπιλεγμένη πύλη στο PC2; Γιατί; **Όχι δεν παραμένει η πληροφορία για την προεπιλεγμένη πύλη καθώς διαγράφεται κάθε φορά που αλλάζουμε την IPv4 στην εν λόγω διεπαφή.**

7.7) Στο PC2 ορίστε και πάλι ως προεπιλεγμένη πύλη τον δρομολογητή R2.

```
root@PC2:~ # route add default 172.17.17.193
add net default: gateway 172.17.17.193
```

7.8) Καθαρίστε τους πίνακες ARP σε όλα τα εικονικά μηχανήματα του LAN2. **arp -da**

7.9) Στον δρομολογητή R2 ξεκινήστε μια καταγραφή χωρίς επίλυση διευθύνσεων, ώστε να συλλάβετε όλα τα πακέτα arp στο LAN2. `root@PC:~ # tcpdump -i em0 arp -n`

7.10) Στα PC2 και PC3 ξεκινήστε καταγραφές χωρίς επίλυση διευθύνσεων, ώστε να συλλάβετε όλα τα τεμάχια tcp.

```
root@PC2:~ # tcpdump -i em0 -n tcp
```

7.11) Από το PC1 προσπαθήστε να συνδεθείτε με SSH ως χρήστης lab στην IPv4 διεύθυνση του PC3. Εμφανίσθηκε κάποια ένδειξη λάθους;

```
root@PC1:~ # ssh lab@172.17.17.254
Fssh_kex_exchange_identification: read: Connection reset by peer
Connection reset by 172.17.17.254 port 22
```

7.12) Σταματήστε τις καταγραφές και επαναλάβετε την προσπάθεια.

Ήταν επιτυχής τώρα;

Τώρα ήταν επιτυχής.

```
root@PC1:~ # ssh lab@172.17.17.254
The authenticity of host '172.17.17.254 (172.17.17.254)' can't be established.
ED25519 key fingerprint is SHA256:0TRXkGG8BworakzfsfEkXJFmL4bGmtbxxKZzM+flhaE.
No matching host key fingerprint found in DNS.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:1: 192.168.1.18
    ~/.ssh/known_hosts:4: 172.17.17.190
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.17.17.254' (ED25519) to the list of known hosts
(lab@172.17.17.254) Password for lab@PC.ntua.lab:
Last login: Mon Mar 27 18:54:16 2023 from 172.17.17.1
FreeBSD 12.4-RELEASE r372781 GENERIC

Welcome to FreeBSD!
```

7.13) Καταγράψτε τις σχετικές με τα PC2, PC3 εγγραφές του πίνακα ARP στον R2.

```
? (172.17.17.254) at 08:00:27:d4:97:27 on em0 expires in 1072 seconds [ethernet]
```

7.14) Στην καταγραφή πακέτων arp, ποιο από τα PC2, PC3 απάντησε πρώτο στο ARP request του R2 και ποιο δεύτερο;

```
02:58:57.426792 ARP, Request who-has 172.17.17.254 tell 172.17.17.193, length 28
02:58:57.427189 ARP, Reply 172.17.17.254 is-at 08:00:27:b6:86:41, length 46
02:58:57.427209 ARP, Reply 172.17.17.254 is-at 08:00:27:d4:97:27, length 46
```

Πρώτο στο ARP request του R2 απάντησε το PC2 και δεύτερο το PC3.

7.15) Σε ποιο από τα δύο μηχανήματα, PC2 ή PC3, ανήκει η διεύθυνση MAC που περιέχει ο πίνακας ARP του R2;

Ανήκει στο PC3.

7.16) Σε ποιο από τα δύο μηχάνημα συνδεθήκατε τη δεύτερη φορά; **Στο PC3.**

7.17) Με ποιους άλλους τρόπους μπορείτε να καταλάβετε σε ποιο μηχάνημα έχετε συνδεθεί;

Μπορούμε να τρέξουμε την εντολή ifconfig ενώ είμαστε συνδεδεμένοι στο μηχάνημα και να συγκρίνουμε την MAC.

7.18) Παρατηρώντας στις δύο καταγραφές τα τεμάχια TCP που σχετίζονται με την τριπλή χειραψία σε συνδυασμό με τη σειρά που λήφθηκαν τα ARP reply στον R2, εξηγήστε γιατί το SSH δεν λειτούργησε την πρώτη φορά καθώς και γιατί συνδεθήκατε στο συγκεκριμένο μηχάνημα τη δεύτερη φορά. **Πρώτος απάντησε ο PC2 στον R2 στο ARP Request και το πρώτο τεμάχιο της τριπλής χειραψίας (SYN) στάλθηκε με προορισμό τον PC2, ο οποίος και αποστέλλει και (SYN-ACK) στον PC1. Έπειτα ο PC3 απαντά στο ARP Request, ενημερώνεται ο πίνακας ARP και το τρίτο τεμάχιο της χειραψίας (ACK) στέλνεται στον PC3. Αυτός με τη σειρά του αναγνωρίζει ότι δεν έχει παραλάβει την ορθή αλληλουχία των τεμαχίων και στέλνει τεμάχιο RESET στον PC1.**

```
02:58:57.289276 IP 172.17.17.1.24981 > 172.17.17.254.22: Flags [S], seq 28280071
30, win 65535, options [mss 1460,nop,wscale 6,sackOK,TS val 2656521533 ecr 0], l
ength 0
02:58:57.289305 IP 172.17.17.254.22 > 172.17.17.1.24981: Flags [S.], seq 3544344
613, ack 2828007131, win 65535, options [mss 1460,nop,wscale 6,sackOK,TS val 193
5485873 ecr 2656521533], length 0
02:58:58.288845 IP 172.17.17.254.22 > 172.17.17.1.24981: Flags [S.], seq 3544344
613, ack 2828007131, win 65535, options [mss 1460,nop,wscale 6,sackOK,TS val 193
5486873 ecr 2656521533], length 0
02:59:00.488810 IP 172.17.17.254.22 > 172.17.17.1.24981: Flags [S.], seq 3544344
613, ack 2828007131, win 65535, options [mss 1460,nop,wscale 6,sackOK,TS val 193
5489073 ecr 2656521533], length 0
02:59:04.688758 IP 172.17.17.254.22 > 172.17.17.1.24981: Flags [S.], seq 3544344
613, ack 2828007131, win 65535, options [mss 1460,nop,wscale 6,sackOK,TS val 193
5493273 ecr 2656521533], length 0
```

```
02:58:56.546630 IP 172.17.17.1.24981 > 172.17.17.254.22: Flags [.], ack 35443446
14, win 1027, options [nop,nop,TS val 2656521533 ecr 1935485873], length 0
02:58:56.546659 IP 172.17.17.254.22 > 172.17.17.1.24981: Flags [R], seq 35443446
14, win 0, length 0
02:58:56.547418 IP 172.17.17.1.24981 > 172.17.17.254.22: Flags [P.], seq 0:38, a
ck 1, win 1027, options [nop,nop,TS val 2656521533 ecr 1935485873], length 38
02:58:56.547437 IP 172.17.17.254.22 > 172.17.17.1.24981: Flags [R], seq 35443446
14, win 0, length 0
02:58:57.546456 IP 172.17.17.1.24981 > 172.17.17.254.22: Flags [R], seq 28280071
31, win 0, length 0
02:58:59.746408 IP 172.17.17.1.24981 > 172.17.17.254.22: Flags [R], seq 28280071
31, win 0, length 0
02:59:03.945518 IP 172.17.17.1.24981 > 172.17.17.254.22: Flags [R], seq 28280071
```