Ονοματεπώνυμο: Περόγαμβρος Γεώργιος	Όνομα PC:
Ομάδα: 2	Ημερομηνία: 6/4/2022

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 Χρησιμοποίησα τις εντολές ifconfig interface ip όπου interface η αντίστοιχη διεπαφή και ip η αντίστοιχη διεύθυνση.

1.2 Πρόσθεσα τη γραμμή gateway_enable=”YES”.

1.3 Χρησιμοποίησα την εντολή route add -net 192.168.2.0/24 192.168.1.1.

1.4 Παρατηρούμε τις σημαίες UGS, που σημαίνουν:

U: Η διαδρομή είναι ενεργή

G: Ο προορισμός είναι πύλη, που θα αποφασίσει για το πώς θα προωθήσει τα πακέτα περαιτέρω

S: Η διαδρομή έχει οριστεί στατικά.

1.5 Χρησιμοποίησα την εντολή ping 192.168.2.2. Το ping δεν είναι επιτυχές επειδή ενώ τα πακέτα φτάνουν στον PC2, αυτός δεν ξέρει πως θα απαντήσει.

1.6 Χρησιμοποίησα την εντολή tcpdump -i em0 “icmp” και tcpdump -i em1 “icmp”. Και στα 2 LAN παρατηρούνται μόνο τα icmp echo request που παράγει ο PC1. Αυτό συμβαίνει επειδή ο PC1 θέλει να επικοινωνήσει με ένα υπολογιστή του υποδικτύου 192.168.2.0/24 και λόγω της στατικής εγγραφής που προσθέσαμε πριν στέλνει τα πακέτα στο R1, ο οποίος τα προωθεί στο PC2 αφού έχει ενεργή την προώθηση πακέτων. Τα πακέτα φτάνουν στον PC2, ο οποίος όμως δεν ξέρει πως θα επικοινωνήσει με τον PC1 που βρίσκεται σε άλλο υποδίκτυο αφού δεν έχει κάποια κατάλληλη εγγραφή στον πίνακα δρομολόγησής του.

1.7 Χρησιμοποίησα την εντολή route add -net 192.168.1.0/24 192.168.2.1.

1.8 Ναι, τώρα υπάρχει επικοινωνία

1.9 Δεν χρειάζεται να αλλάξουμε κάτι στον πίνακα δρομολόγησης του R1 καθώς έχουμε ενεργοποιήσει την προώθηση πακέτων και έτσι αν πατήσουμε netstat -rn βλέπουμε πως υπάρχουν ήδη εγγραφές για τα αντίστοιχα υποδίκτυα.

2

2.1 Χρησιμοποίησα την εντολή route del 192.168.2.0/24

2.2 Χρησιμοποίησα την εντολή ifconfig em0 192.168.1.2/20

2.3 Βρίσκονται στο ίδιο υποδίκτυο.

2.4 Όχι, δεν είναι, αφού ο PC1 προσπαθεί να στείλει κατευθείαν τα μηνύματα στους PC2 και PC3, χωρίς να τα προωθήσει μέσω του R1 και αφού βρίσκονται σε διαφορετικά LAN, τα μηνύματα δεν φθάνουν ποτέ.

2.5 Το ping είναι επιτυχές. Ο PC1 στέλνει αρχικά ένα arp request για να μάθει τη mac του PC2, τον οποίο βλέπει στο ίδιο δίκτυο. Αυτό το arp λαμβάνεται από τον R1 ο οποίος απαντάει με τη δική του MAC αφού λειτουργεί ως proxy για το PC2. Έτσι ο PC1 στέλνει το icmp echo request στον R1 ο οποίος έπειτα το προωθεί στο PC2. Από εκεί και πέρα ο PC2 απαντάει μέσω του R1 όπως έκανε και στο πρώτο μέρος.

2.6 Το ping αποτυγχάνει, καθώς, αν και το μήνυμα φθάνει στον PC3 αυτός δεν θα απαντήσει

αφού για αυτόν ο PC1 ανήκει σε διαφορετικό υποδίκτυο για το οποίο δεν έχει κάποια διαδρομή στον πίνακα δρομολόγησής του.

2.7 Χρησιμοποίησα την εντολή route add -net 192.168.1.0/24 192.168.2.1

2.8 Χρησιμοποίησα την εντολή apr -da.

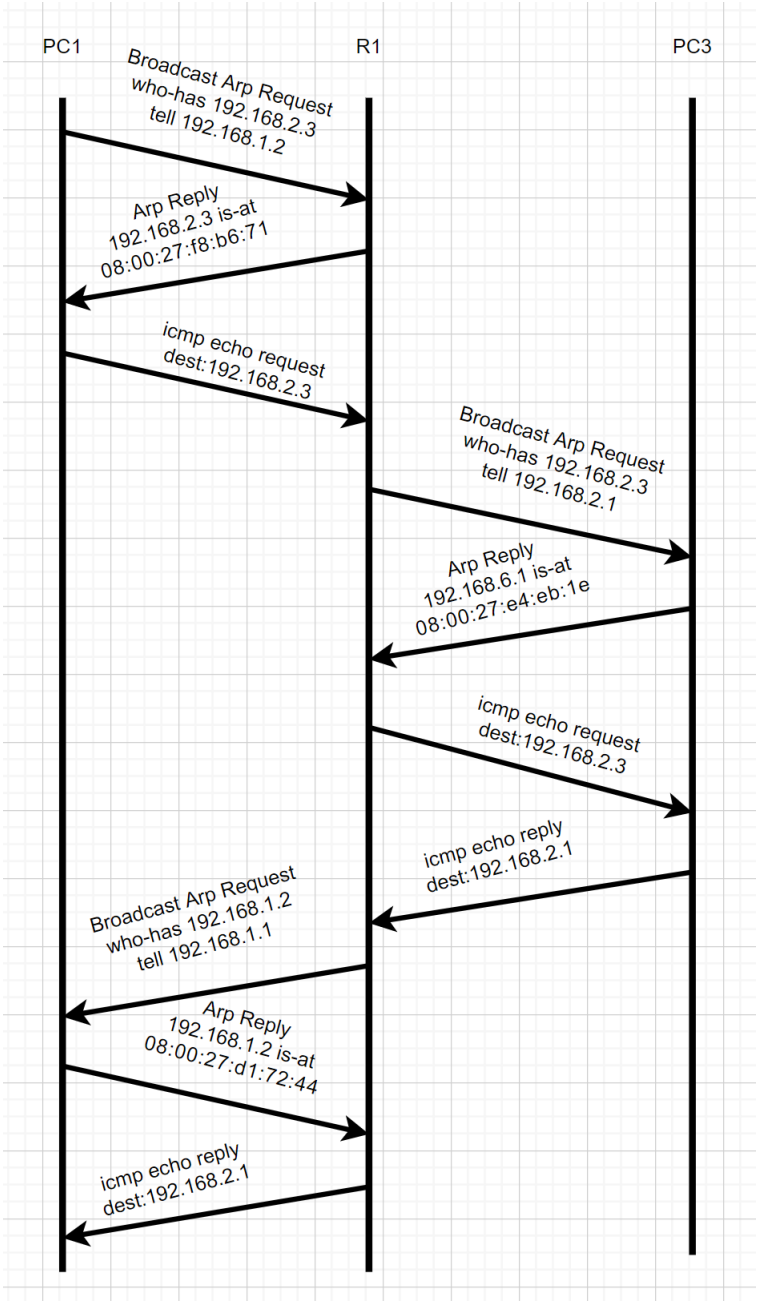
2.9 Χρησιμοποίησα τις εντολές tcpdump -i em0 -e tcpdump -i em1 -e ping -c 1 192.168.2.3

2.10 Ο R1 απαντάει στο apr request βάζοντας τη δικιά του MAC (αυτή της διεπαφής em0 που βρίσκεται στο LAN1) ως MAC της ip του PC3.

2.11 Προς τη mac της em0 του R1: 08:00:27:f8:b6:71

2.12 Από τη mac της em1 του R1: 08:00:27:c7:e9:6a

2.13



2.14 Το μεγαλύτερο μήκος προθέματος για τον PC1 για το οποίο εξακολουθεί και λειτουργεί το παραπάνω ping, είναι το 22, καθώς από το 23 και μετά ο PC1 βλέπει τον PC3 σε διαφορετικό υποδίκτυο για το οποίο δεν έχει εγγραφή στον πίνακα δρομολόγησής του και έτσι δεν θα ξέρει πως να επικοινωνήσει.

2.15 Χρησιμοποίησα την εντολή ifconfig em0 192.168.1.2/23.

2.16 Χρησιμοποίησα την εντολή route add -net 192.168.2.0/24 -interface em0.

2.17 Εμφανίζεται η MAC της em0 του PC1.

2.18 Το ping είναι επιτυχές. Αφού το επόμενο βήμα για το υποδίκτυο 192.168.2.0/24 είναι η em0 το αρχικό broadcast arp θα σταλθεί στο LAN1 και έτσι θα το ακούσει ο R1 ο οποίος, ως proxy, θα απαντήσει με τη δικιά του MAC και η διαδικασία θα συνεχιστεί παρόμοια με πριν.

2.19 Χρησιμοποίησα την εντολή sysctl net.link.ether.inet.proxyall=1.

2.20 Χρησιμοποίησα την εντολή route change 192.168.2.0/24 192.168.1.1.

2.21 Χρησιμοποίησα την εντολή ifconfig em0 192.168.1.2/24.

2.22 Η διαδρομή διαγράφηκε.

3

3.1 Χρησιμοποίησα τις εντολές ifconfig em0 192.168.1.1/24 και ifconfig em1 172.17.17.1/30.

3.2 Χρησιμοποίησα τις εντολές ifconfig em0 172.17.17.2/30 και ifconfig em1 192.168.2.1/24.

3.3 Το ping αποτυγχάνει με μήνυμα σφάλματος Destination Host Unreachable.

3.4 Στο LAN1 παρατηρούνται δύο μηνύματα ICMP. Ένα echo request από τον PC1 στον R1, αφού αυτός είναι το επόμενο βήμα του για το υποδίκτυο 192.168.2.0/24 και ένα host από τον R1 στον PC1 με το σφάλμα Host Unreachable καθώς ο R1 δεν μπορεί να επικοινωνήσει με τη ζητούμενη διεύθυνση. Στο WAN1 δεν υπάρχουν μηνύματα ICMP καθώς ο R1 δεν έχει εγγραφή για το υποδίκτυο του PC2 οπότε δεν προωθεί κάποιο μήνυμα στο WAN1.

3.5 Το πρώτο βήμα που είναι στον R1 δεν έχει κάποιο σφάλμα. Το δεύτερο σταματάει πάλι στον R1 και έχει το σύμβολο !H που σημαίνει Unreachable.

3.6 Χρησιμοποίησα την εντολή route add -net 192.168.2.0/24 172.17.17.2

3.7 Το ping εξακολουθεί να αποτυγχάνει.

3.8 Παρατηρούμε ένα arp request από τον R2 που θέλει να μάθει την mac του PC2 προκειμένου να προωθήσει το ICMP ech request που του προώθησε ο R1, μαζί με το αντίστοιχο arp reply από τον PC2, μετά το echo request και το αντίστοιχο echo reply που στέλνει ο PC2 στην 192.168.2.1 (η οποία ανήκει πλέον στον R2) αφού ο πίνακας δρομολόγησής του PC2 έχει ως gateway για το υποδίκτυο 192.168.1.0/24 την 192.168.2.1. Τέλος, ο R2 απαντάει στον PC2 με ένα ICMP Host Destination Unreachable, μιας και ο δικός του πίνακας δεν έχει εγγραφή σχετικά με το υποδίκτυο του PC1.

3.9 Δεν παρατηρούνται μηνύματα ICMP echo request αλλά UDP datagrams, αφού η traceroute χρησιμοποιεί UDP σαν προεπιλογή.

3.10 Ναι, παρατηρούμε αρχικά ένα UDP datagram και έπειτα ένα μήνυμα σφάλματος ICMP udp port unreachable.

3.11 Δεν παρατηρείται μήνυμα λάθους ICMP host unreachable από τον R2, καθώς δεν δημιουργούνται μηνύματα icmp λάθους ως απάντηση σε άλλα μηνύματα λάθους (icmp udp port unreachable), ώστε να αποφευχθούν βρόγχοι μηνυμάτων λάθους.

3.12 Χρησιμοποίησα την εντολή route add -net 192.168.1.0/24 172.17.17.1

3.13 Ναι το traceroute είναι επιτυχές. Παράγονται μηνύματα icmp time exceeded όταν το ttl μηδενιστεί πριν φτάσει στον προορισμό του και ένα icmp udp port unreachable όταν το udp φτάσει στο PC2.

3.14 Το ping αποτυγχάνει με μήνυμα λάθος no route to host.

3.15 Χρησιμοποίησα την εντολή route del 192.168.1.0/24

3.16 Χρησιμοποίησα την εντολή route add defeault 192.168.2.1

3.17 Το ping είναι επιτυχές.

3.18 Το πρώτο δεν ήταν επιτυχές καθώς ο PC2 δεν είχε εγγραφή στον πίνακα δρομολόγησής του για το υποδίκτου του 172.17.17.1. Στο δεύτερο ping είχε την default gateway, στην οποία έστειλε τα μηνύματα

και η οποία (R2) γνωρίζει πως να επικοινωνήσει με τον R1. Αντίστοιχα, ο R1 έχει ως επόμενο βήμα για το υποδίκτυο του PC2 το R2 και άρα μπόρεσε να απαντήσει.

4

4.1 Αφού συνέδεσα το καλώδιο, χρησιμοποίησα την εντολή ifconfig em0 192.168.2.3/24

4.2 Χρησιμοποίησα την εντολή route add -net 192.168.1.0/24 192.168.2.1

4.3 Πρέπει να έχουμε από μία κάρτα στα LAN1, WAN1, WAN2. Χρησιμοποίησα τις εντολές ifconfig em0 192.168.1.1/24, ifconfig em1 172.17.17.1/30, ifconfig em2 172.17.17.5/30

4.4 Πρέπει να έχουμε από μία κάρτα στα WAN1, LAN2, WAN2. Χρησιμοποίησα τις εντολές ifconfig em0 172.17.17.2/30, ifconfig em1 192.168.2.1/24, ifconfig em2 172.17.17.9/30

4.5 Πρέπει να έχουμε από μία κάρτα στα WAN1, WAN2. Χρησιμοποίησα τις εντολές ifconfig em0 172.17.17.6/30, ifconfig em1 172.17.17.10/30

4.6 Χρησιμοποίησα την εντολή route add -net 192.168.2.0/24 172.17.17.2

4.7 Χρησιμοποίησα την εντολή route add -net 192.168.1.0/24 172.17.17.1

4.8 Χρησιμοποίησα τις εντολές route add -net 192.168.1.0/24 172.17.17.5 και route add -net 192.168.2.0/24 172.17.17.9

4.9 Χρησιμοποίησα την εντολή route add 192.168.2.3 172.17.17.6. Η σημαία που υποδεικνύει πως είναι διαδρομή προς υπολογιστή είναι η H.

4.10 Χρησιμοποίησα την εντολή traceroute 192.168.2.2. Βλέπω 3 βήματα (192.168.1.1, 172.17.17.2, 192.168.2.2)

4.11 Χρησιμοποίησα την εντολή ping 192.168.2.2. Η τιμή του ttl είναι 62, άρα έχουμε 3 βήματα.

4.12 Χρησιμοποίησα την εντολή traceroute 192.168.2.3. Βλέπω 4 βήματα (192.168.1.1, 172.17.17.6, 172.17.17.2, 192.168.2.3)

4.13 Χρησιμοποίησα την εντολή ping 192.168.2.3. Η τιμή του ttl είναι 62, άρα έχουμε 3 βήματα

4.14 Το ICMP Echo Request ακολουθεί την διαδρομή R1->R3->R2->PC3

4.15 Το ICMP Echo Reply ακολουθεί τη διαδρομή R2→R1→PC1, καθώς το R2 έχει στατική εγγραφή για το δίκτυο 192.168.1.0/24 μέσω του R1, χωρίς να έχει κάποια εγγραφή μεγαλύτερου προθέματος για το PC1. Έτσι παρόλο που το echo request πηγαίνει μέσω του R3 (αφού προωθείται από το R1 που έχει την εγγραφή για το PC3 μέσω του R3), το echo reply προωθείται από το R2 απευθείας στο R1.

4.16 Χρησιμοποίησα την εντολή tcpdump -i em1.

4.17 Όχι, δεν παρατηρούνται.

4.18 Ναι, έχουμε ζεύγη udp και icmp udp port unreachable.

4.19 Ναι, χρησιμοποίησα τις εντολές route change -net 192.168.2.0/24 172.17.17.6 και route change -net 192.168.1.0/24 172.17.17.10.

4.20 Για το PC2 η δρομολόγηση γίνεται προς το δίκτυό του (destination:192.168.2.0/24), ενώ για το PC3 απευθείας προς το host (destination:192.168.2.3).

4.21 Επιλέγεται η διαδρομή απευθείας στον Host, αφού σε αυτή έχουμε ταίριασμα μεγαλύτερου μήκους προθέματος.

5

5.1 Χρησιμοποίησα την εντολή route change -net 192.168.2.0/24 172.17.17.5

5.2 Χρησιμοποίησα την εντολή ping -c 1 192.168.2.2. Το ping δεν ήταν επιτυχές, έχουμε μήνυμα λάθους time to live exceeded.

5.3 Προέρχεται από την 172.17.17.6.

5.4 Από την em0 του R3 (WAN2).

5.5 Έχουμε την εντολή tcpdump -i em0 -e “icmp[0]=8”.

5.6 Από το PC1 στάλθηκε μόνο 1 πακέτο icmp echo request, ενώ στο WAN2 εμφανίσθηκαν 63.

5.7 Χρησιμοποίησα τις εντολές tcpdump -i em0 -e -l | tee lan1 και tcpdump -i em0 -e -l | tee wan2

5.8 Εμφανίζονται 64 βήματα. Η διαδρομή είναι από το PC1 στο R1 και μετά μια λούπα από το R1 στο R3 και από το R3 στο R1.

5.9 Με τη χρήση της εντολής grep “echo request” wan2 | wc -l βρήκαμε πως στάλθηκαν 64 ICMP echo request από το PC1.

5.10 Με τη χρήση της εντολής grep “echo request” wan2 | wc -l βρήκαμε πως εμφανίστηκαν 2016 ICMP echo request στο WAN2. Αυτό είναι λογικό καθώς για πακέτο με αρχικό ttl 1 από το PC1, το πακέτο θα φτάσει στον R1 και θα έχουμε time to live exceeded (δεν θα μπει στο WAN2), για αρχικό ttl 2 θα εμφανισθεί και ένα echo request που θα σταλθεί στον R3, για ttl 3 άλλο ένα echo request που θα σταλθεί από τον R3 πίσω στον R1 κτλ. Άρα, αφού από τον PC1 θα σταλθούν 64 πακέτα με ttl από 1 έως 64, στο wan2 θα εμφανισθούν 1+2+3+...+63 icmp echo request.

5.11 Χρησιμοποίησα την εντολή grep “exceeded” wan2 | wc -l και βρήκα πως εμφανίστηκαν 32 πακέτα time to live exceeded στο wan2, αφού από τα 64 time to live exceeded που στάλθηκαν συνολικά τα μισά στάλθηκαν από τον R1 (κατευθείαν στο LAN1 χωρίς να μπουν στο WAN2) και τα άλλα μισά από τον R3 (μπήκαν πρώτα στο WAN2). Συγκεκριμένα, όταν το αρχικό request του PC1 είχε μονό ttl το time to live exceeded στέλνεται από τον R1 και όταν έχει ζυγό από το R3.

5.12 Θα χρησιμοποιήσουμε το κατάλληλο φίλτρο στο tcpdump (“icmp[0]=8 για τα request και icmp[0]=11 για τα time to live exceeded). Όταν σταματήσουμε την καταγραφή με ctl+c θα δούμε τα αποτελέσματα.

5.13 Τα ICMP echo request του ping έχουν σταθερό ttl=64, ενώ του traceroute ξεκινάνε από ttl=1 και φθάνουν μέχρι ttl=64(εκτός αν φτάσουμε τον προορισμό νωρίτερα).

5.14 Διότι το ttl μειώνεται κατά ένα όταν το πακέτο περνάει από έναν κόμβο που δεν είναι ο προορισμός και όταν φθάσει το μηδέν απορρίπτεται.

6

6.1 Η διεύθυνση υποδικτύου του LAN1 είναι η 172.17.17 .0/25

6.2 Η διεύθυνση υποδικτύου του LAN2 είναι η 172.17.17 .192/26

6.3 Η διεύθυνση υποδικτύου του LAN3 είναι η 172.17.17 .160/27

6.4 Χρησιμοποίησα τις εντολές ifconfig em0 172.17.17.1/25(PC1) και ifconfig em0 172.17.17.126/25(R1)

6.5 Χρησιμοποίησα τις εντολές ifconfig em0 172.17.17.161/27(PC4) και ifconfig em0 172.17.17.190/27(R3)

6.6 Χρησιμοποίησα τις εντολές ifconfig em1 172.17.17.193/26(R2), ifconfig em0 172.17.17.254/26(PC3) και ifconfig em0 172.17.17.253/26(PC2)

6.7 Χρησιμοποίησα τις εντολές route add default 172.17.17.126, route add default 172.17.17.193, route add default 172.17.17.190

6.8 Χρησιμοποίησα τις εντολές route add 172.17.17.192/26 172.17.17.130 και route add

172.17.17.160/27 172.17.17.130

6.9 Χρησιμοποίησα τις εντολές route add 172.17.17.0/25 172.17.17.137 και route add

172.17.17.160/27 172.17.17.137

6.10 Χρησιμοποίησα τις εντολές route add 172.17.17.0/25 172.17.17.133 και route add

172.17.17.192/26 172.17.17.133

6.11 Ήταν επιτυχή όλα τα ping

7

7.1 PC2: 08:00:27:ef:b2:a1 PC3: 08:00:27:e4:eb:1e

7.2 Χρησιμοποίησα την εντολή ifconfig em0 172.17.17.254/26

7.3 Εμφανίστηκε το μήνυμα λάθους arp: 08:00:27:e4:eb:1e is using my IP address 172.17.17.254 on em0!

7.4 Εμφανίστηκε το μήνυμα λάθους arp: 08:00:27:ef:b2:a1 is using my IP address 172.17.17.254 on em0!

7.5 Ναι, έχει οριστεί. Το νόημα των μηνυμάτων λάθους είναι να ενημερώσει πως η διεύθυνση IP που χρησιμοποιούμε σε αυτή τη διεπαφή χρησιμοποιείται και από κάποιο άλλο μηχάνημα.

7.6 Όχι, αφού όταν αλλάξουμε IP ο πίνακας δρομολόγησης επαναϋπολογίζεται.

7.7 Χρησιμοποίησα την εντολή route add default 172.17.17.193

7.8 Χρησιμοποίησα την εντολή arp -da

7.9 Χρησιμοποίησα την εντολή tcpdump -i em1 “arp”

7.10 Χρησιμοποίησα την εντολή tcpdump -i em0 -n “tcp”

7.11 Δεν καταφέραμε να συνδεθούμε με μήνυμα λάθους ssh_exchange_identification: read: Connection reset by peer.

7.12 Ήταν επιτυχές.

7.13 Έχουμε την εγγραφή

(172.17.17.254) at 08:00:27:e4:eb:1e on em1 expires in 1082 seconds [ethernet]

7.14 Πρώτα απάντησε το PC2 και μετά το PC3.

7.15 Ανήκει στο PC3.

7.16 Συνδεθήκαμε στο PC3. Το βρήκαμε μέσω της mac από την εντολή ifconfig.

7.17 Άλλοι τρόποι είναι οι εξής:

Μετά τη σύνδεση να κάνουμε tcpdump στα PC2 και PC3 και να δούμε σε ποιο από τα δύο καταγράφεται κίνηση.

Να κάνουμε arp -a στα PC2 και PC3 και να παρατηρήσουμε σε ποιον εμφανίζεται η ssh σύνδεση.

Να κάνουμε who στα PC2 και PC3 και να παρατηρήσουμε σε ποιον υπάρχει συνδεδεμένος ο χρήστης lab με ssh.

7.18 Αρχικά ο PC1 στέλνει το πρώτο πακέτο της τριμερούς χειραψίας με flag S, το οποίο ο R2 πρέπει να προωθήσει στην 172.17.17.254, οπότε και κάνει arp request στο LAN2. Πρώτος απαντάει ο PC2, οπότε και ο R2 παραδίδει το πακέτο. Ο PC2 απαντάει με flags S. τα οποία φτάνουν στον PC1, που απαντάει με flags .(ack). Όμως πριν φτάσει στον R2 η απάντηση του PC1, ο PC3 απαντάει στο arp request με αποτέλεσμα ο R2 να παραδίδει την απάντηση του PC1 στον PC3, ο οποίος λαμβάνει ένα σκέτο ack. Τότε, ο PC3 στέλνει flag reset και ο PC2 ξαναπροσπαθεί και στέλνει flags S. με τον PC1 να απαντάει με flags P. . Αυτό συμβαίνει 4 φορές συνολικά μέχρι που σταματάνε να προσπαθούν και η σύνδεση αποτυγχάνει. Στη δεύτερη προσπάθεια ο R2 έχει ήδη την εγγραφή πως η ip 172.17.17.254 αντιστοιχεί στη MAC του PC3, οπότε δεν στέλνει arp request και έτσι η τριμερής χειραψία γίνεται

επιτυχώς από την αρχή ως το τέλος μεταξύ των PC1 και PC3.