Ονοματεπώνυμο: Ιωάννης Γιαννούκος	**Όνομα PC:** John John
Ομάδα: 1	**Ημερομηνία:** 1/4/2023

Εργαστηριακή Άσκηση 5
Στατική δρομολόγηση

Άσκηση 1

(Αφού δημιουργήσω το εικονικό μηχάνημα R1, προσθέτω την γραμμή «`gateway_enable="YES"`» στο αρχείο /etc/rc.conf για να ενεργοποιείται αυτόματα η προώθηση πακέτων, ακόμα και όταν το μηχάνημα αυτό εκτελεί επανεκκίνηση).

1.1) Ορίζω τις διευθύνσεις IPv4 στα εικονικά μηχανήματα με τις εξής εντολές φλοιού:
"`ifconfig em0 inet 192.168.1.2/24`" → PC1
"`ifconfig em0 inet 192.168.2.2/24`" → PC2
"`ifconfig em0 inet 192.168.1.1/24`" → R1
"`ifconfig em1 inet 192.168.2.1/24`" → R1

1.2) Για να ενεργοποιηθεί η λειτουργία προώθησης πακέτων IPv4 στον R1, προσθέτω την εξής γραμμή στο αρχείο /etc/rc.conf: «`gateway_enable= "YES"`».

1.3) Προσθέτω στο PC1 στατική εγγραφή για το δίκτυο 192.168.2.0.24 που βρίσκεται ο υπολογιστής PC2 με την εντολή "`route add -net 192.168.2.0/24 192.168.1.1`".

1.4) Εμφανίζω τον πίνακα δρομολόγησης του PC1 με την εντολή "`netstat -r4`". Παρατηρώ ότι οι σημαίες για τη διαδρομή προς το δίκτυο 192.168.2.0/24 είναι οι UGS. Η κάθε μία από αυτές σημαίνει το εξής:

- U → Η διαδρομή είναι ενεργή (up)
- G → Ο προορισμός είναι πύλη, που θα αποφασίσει για το πώς θα προωθήσει τα πακέτα περαιτέρω
- S → Η διαδρομή έχει οριστεί στατικά

1.5) Δοκιμάζω την εντολή ping από το PC1 στο PC2 ως εξής: "`ping -c 3 192.168.2.2`". Επίσης, σε νέο παράθυρο του PC1 ξεκινώ μια καταγραφή tcpdump για να βλέπω καθαρά την κίνηση που δημιουργείται.

Παρατηρώ ότι, παρόλο που το PC1 στέλνει τα πακέτα ICMP echo request, δεν λαμβάνει τα αντίστοιχα πακέτα ICMP echo reply από το PC2.

1.6) Εκτελώ στον R1 σε δύο παράθυρα τις εντολές "`tcpdump -i emX`", X=0,1, για να δω ευδιάκριτα την κίνηση που δημιουργείται στα LAN{1,2}. Παρατηρώ ότι τα πακέτα ICMP echo request που δημιουργούνται στο LAN1 από το PC1 προωθούνται μέσω του R1 στο LAN2, ωστόσο το PC1 εξακολουθεί να μην λαμβάνει τα αντίστοιχα πακέτα ICMP echo reply από το PC2. Αυτό συμβαίνει, επειδή το PC2 δεν έχει κάποια εγγραφή στον πίνακα δρομολόγησής του για την διεύθυνση του PC1 ή, εν γένει, για την διεύθυνση του δικτύου του PC1. Σημειώνω ότι μπορώ να εμφανίσω τον πίνακα δρομολόγησης του PC2 με την εντολή "`netstat -r4`" (με την επιλογή '4' εμφανίζονται μόνο οι διευθύνσεις IPv4).

1.7) Προσθέτω στο PC2 στατική εγγραφή για το δίκτυο 192.168.1.0/24 όπου βρίσκεται ο υπολογιστής PC1 με την εντολή "`route add -net 192.168.1.0/24 192.168.2.1`".

1.8) Ναι, πλέον το PC2 απαντά επιτυχώς στα πακέτα ICMP που του στέλνει το PC1.

1.9) Από την παραπάνω διαδικασία παρατηρώ ότι δεν χρειάζεται να γίνει καμία αλλαγή στον πίνακα δρομολόγησης του R1. Αυτό εξηγείται από το γεγονός ότι ο R1 ως δρομολογητής μπορεί να ενημερώνει αυτόματα τον πίνακά του με βάση το πρωτόκολλο δρομολόγησής του.

Άσκηση 2

2.1) Στο PC1 καταργώ τη στατική εγγραφή για το δίκτυο 192.168.2.0/24 με την εντολή "`route del 192.168.2.0/24`".

2.2) Αλλάζω στο PC1 το μήκος προθέματος της IPv4 διεύθυνσης από /24 σε /20 με την εντολή "`ifconfig em0 inet 192.168.1.2/20`".

2.3) Από την προοπτική του PC1, τα PC{2,3} βρίσκονται στο ίδιο υποδίκτυο.

2.4) Κάνω ping από το PC1 στα PC{2,3} και βλέπω ότι αυτά αποτυγχάνουν.

(Ενεργοποιώ τη λειτουργία proxy ARP στον R1 με την εντολή "`sysctl net.link.ether.inet.proxyall=1`").

2.5) Δοκιμάζω ξανά να κάνω ping από το PC1 στο PC2 στέλνοντας ακριβώς ένα πακέτο και βλέπω ότι το ping πλέον επιτυγχάνει.

2.6) Δοκιμάζω ξανά να κάνω ping από το PC1 στο PC3 στέλνοντας ακριβώς ένα πακέτο και βλέπω ότι το ping εξακολουθεί να αποτυγχάνει. Αυτό συμβαίνει, επειδή το PC3 δεν έχει κάποια εγγραφή στον πίνακα δρομολόγησής του για την διεύθυνση του PC1 ή του δικτύου του PC1.

2.7) Προσθέτω στατική εγγραφή στο PC3 για το δίκτυο 192.168.1.0/24 με την εντολή "`route add -net 192.168.1.0/24 192.168.2.1`".

2.8) Καθαρίζω στα PC{1,3} και R1 τον πίνακα ARP με την εντολή "`arp -a -d`".

2.9) Ξεκινώ καταγραφές στον R1 για τα LAN{1,2}, φροντίζοντας να εμφανίζονται στην οθόνη και οι διευθύνσεις MAC των πλαισίων που τα μεταφέρουν με την εντολή "`tcpdump -i emX -e`" X=0,1 , και, στη συνέχεια, επαναλαμβάνω το προηγούμενο ping στέλνοντας 1 ακριβώς πακέτο ICMP request από το PC1 στο PC3 με την εντολή "`ping -c 1 192.168.2.3`".

2.10) Η απάντηση του R1 στο ARP request που λαμβάνει από το PC1 παρατηρώ ότι περιέχει την διεύθυνση MAC του ίδιου του R1. Αυτό συμβαίνει επειδή έχουμε ενεργοποιήσει την λειτουργεία proxy ARP στον R1.

2.11) Το PC1 αποστέλλει το πακέτο ICMP request προς την διεύθυνση MAC της διεπαφής του R1 στο LAN1.

2.12) Το PC3 λαμβάνει το πακέτο ICMP request από την διεύθυνση MAC της διεπαφής του R1 στο LAN2.

2.13)

PC1 → (Broadcast) : ARP request	Το PC1 ζητά την MAC του PC3
R1 → PC1 : ARP reply	Ο R1 απαντά με την MAC της διεπαφής του στο LAN1
PC1 → R1 : ICMP echo request	Το PC1 στέλνει ICMP στον R1
R1 → (Broadcast) : ARP request	Ο R1 ζητά την MAC του PC3
PC3 → R1 : ARP reply	Το PC3 απαντά με την MAC του
R1 → PC3 : ICMP echo request	Ο R1 στέλνει ICMP στο PC3
PC3 → R1 : ICMP echo reply	Το PC3 απαντά στον R1 με ICMP reply
R1 → PC1 : ICMP echo reply	Ο R1 απαντά στο PC1 με ICMP reply

2.14) Η μεγαλύτερη τιμή μήκους προθέματος που μπορεί να τεθεί στο PC1 ώστε να συνεχίσει να λειτουργεί το παραπάνω ping είναι 22. Η τιμή δικαιολογείται από το γεγονός ότι τα PC{1,3} πρέπει να βρίσκονται στο ίδιο υποδίκτυο για να είναι εφικτή η επικοινωνία μεταξύ τους, δηλαδή πρέπει ο αριθμός δικτύου τους να είναι κοινός. Από τις διευθύνσεις IPv4 τους βλέπω ότι το πρώτο bit που διαφέρει μεταξύ τους είναι το 23ο (bit22). Επομένως, θα πρέπει μέχρι και το 22ο bit οι διευθύνσεις τους να είναι όμοιες.

2.15) Ορίζω στο PC1 ως μήκος προθέματος το 23 με την εντολή "`ifconfig em0 inet 192.168.1.2/23`". Δοκιμάζοντας να κάνω ping, εμφανίζεται πλέον το μήνυμα "No route to host", αφού τα μηχανήματα ανήκουν πλέον σε διαφορετικό υποδίκτυο.

2.16) Στο PC1 ορίζω ως επόμενο βήμα για το δίκτυο 192.168.2.0/24 τη διεπαφή του στο LAN1 με την εντολή "`route add -net 192.168.2.0/24 -interface em0`".

2.17) Στον πίνακα δρομολόγησης του PC1 πλέον εμφανίζεται ως πύλη για το δίκτυο 192.168.2.0/24 η διεύθυνση MAC της διεπαφής του στο LAN1 (em0).

2.18) Το ping από το PC1 στο PC3 επιτυγχάνει, επειδή, παρόλο που οι δύο υπολογιστές ανήκουν σε διαφορετικά υποδίκτυα, υπάρχει η εγγραφή στο PC1 για το δίκτυο που ανήκει το PC3 με την πληροφορία ότι πρέπει να χρησιμοποιηθεί η διεπαφή em0 (LAN1). Αυτό, όπως φαίνεται, αρκεί για να επικοινωνήσουν οι δύο υπολογιστές.

2.19) Στον R1 ακυρώνω τη λειτουργία proxy ARP με την εντολή "`sysctl net.link.ether.inet.proxyall=0`".

2.20) Στο PC1 ορίζω ως επόμενο βήμα για το 192.168.2.0/24 τον R1 με την εντολή "`route add -net 192.168.2.0/24 192.168.1.1`".

2.21) Επαναφέρω το μήκος προθέματος του PC1 στην αρχική τιμή /24 με την εντολή "`ifconfig em0 inet 192.168.1.2/24`".

2.22) Η εγγραφή στον πίνακα δρομολόγησης του PC1 προς το 192.168.2.0/24 δεν φαίνεται πλέον. Αυτό συμβαίνει επειδή το μήκος προθέματος της διεύθυνσης IP του PC1 άλλαξε.

2.23) Ορίζω πάλι τη διαδρομή προς το 192.168.2.0/24 μέσω του R1 στο PC1 με την εντολή "`route add -net 192.168.2.0/24 192.168.1.1`".

Άσκηση 3

3.1) Ορίζω τις διευθύνσεις IPv4 στις διεπαφές του R1 στα τοπικά δίκτυα LAN1 και WAN1 με τις εντολές "`ifconfig em0 inet 192.168.1.1/24 ; ifconfig em1 inet 172.17.17.1/30`".

3.2) Ορίζω τις διευθύνσεις IPv4 στις διεπαφές του R2 στα τοπικά δίκτυα WAN1 και LAN2 με τις εντολές "`ifconfig em0 inet 192.168.2.1/24 ; ifconfig em1 inet 172.17.17.2/30`".

3.3) Δοκιμάζω να εκτελέσω ping από το PC1 στο PC2 με την εντολή "`ping 192.168.2.2`" και στο παράθυρο εμφανίζεται το μήνυμα «Destination Host Unreachable», το οποίο προέρχεται από τον δρομολογητή R1.

3.4) Με την εντολή "`tcpdump -i em0 `" στο R1 βλέπω την κίνηση από πακέτα ICMP που δημιουργείται στο LAN1. Παρατηρώ, λοιπόν, ότι παράγονται ICMP echo request μηνύματα από το PC1 και «ICMP host 192.168.2.2 unreachable» μηνύματα από τον R1. Επίσης, αφού εκτελέσω την εντολή "`tcpdump -i em1`" στον R1, παρατηρώ ότι δεν παράγονται πακέτα στο WAN1.

Από την παραπάνω διαδικασία, δηλαδή, καταλαβαίνω ότι ο R1 λαμβάνει τα μηνύματα ICMP echo request από το PC1 στο LAN1, βλέπει ότι δεν έχει κάποια σχετική εγγραφή στον πίνακα δρομολόγησής του με την διεύθυνση IP του PC2, και έτσι στέλνει μήνυμα ICMP host unreachable πίσω στο PC1 από το LAN1, χωρίς να προωθήσει/στείλει κανένα πακέτο στο WAN1.

3.5) Δοκιμάζω τώρα να εκτελέσω την εντολή "`traceroute 192.168.2.2`" από το PC1 στο PC2. Παρατηρώ ότι εμφανίζεται η ένδειξη λάθους "!H", η οποία σημαίνει το προαναφερθέν μήνυμα λάθους "host unreachable".

3.6) Προσθέτω στον R1 στατική εγγραφή για το 192.168.2.0/24 μέσω του R2 με την εντολή "`route add -net 192.168.2.0/24 172.17.17.2`".

3.7) Τώρα, μπορούν τα μηνύματα ICMP echo request που στέλνει το PC1 να φτάσουν στο PC2, ωστόσο ο R2 δεν έχει κάποια εγγραφή στον πίνακα δρομολόγησής του για να στείλει τα μηνύματα ICMP echo reply που λαμβάνει από το PC2 στο PC1, και έτσι απαντά στο PC2 με το μήνυμα "Host Unreachable". Επομένως, συνολικά το ping αποτυγχάνει.

3.8) Κάνοντας μία καταγραφή στο PC2 με "`tcpdump -vvv -e`" παρατηρώ την κίνηση που δημιουργείται στο LAN2 και βλέπω τις εξής επικοινωνίες:

- R2 → PC2 : ICMP echo request
- PC2 → R2 : ICMP echo reply
- R2 → PC2 : ICMP host unreachable

Το 1ο πακέτο, ICMP echo request, είναι το πακέτο που έχει αρχικά στείλει το PC1 στο PC2. Το 2ο πακέτο, ICMP echo reply, είναι το μήνυμα-απάντηση που προσπαθεί το PC2 να στείλει πίσω στο PC1 για να ολοκληρωθεί το ping. Το 3ο πακέτο, ICMP host unreachable, παράγεται από τον R2 ως αποτέλεσμα του ότι δεν έχει κάποια πληροφορία για να στείλει πακέτα στο δίκτυο 192.168.1.0/24, και με αυτό το πακέτο ενημερώνει το PC2 ότι η αποστολή του πακέτου του δεν μπορεί να πραγματοποιηθεί.

3.9) Δοκιμάζω ξανά να εκτελέσω την εντολή "`traceroute 192.168.2.2`" από το PC1 (στο PC2). Δεν παρατηρώ μηνύματα ICMP echo request στο WAN1, αλλά μόνο τεμάχια UDP με διεύθυνση πηγής την IP του PC1 και προορισμούς αυτήν του PC2. Φυσικά, αυτό συμβαίνει επειδή η εντολή traceroute δεν παράγει ICMP echo request μηνύματα, αλλά μόνο δεδομενογράμματα UDP. Επισημαίνεται ότι τα δεδομενογράμματα αυτά έχουν πηγή το PC1 και προορισμό το PC2. Εάν ο R2 περιείχε κάποια εγγραφή για να δρομολογήσει πακέτα στο υποδίκτυο που ανήκει το PC1, τότε θα παρατηρούνταν δεδομενογράμματα UDP και προς τις δύο κατευθύνσεις.

3.10) Εκτελώντας "`tcpdump -e -vvv`" στο PC2 παρατηρώ ότι στο LAN2 παράγονται τεμάχια UDP και πακέτα ICMP udp port unreachable. Επίσης, παρατηρώ ότι καθώς το traceroute «τρέχει», κάθε πακέτο ICMP που φτάνει στο LAN2 προσπαθεί να «φτάσει» σε διαφορετική θύρα του PC2.

3.11) Δεν παρατηρώ μηνύματα ICMP host unreachable στο LAN2, επειδή η αποστολή πολλαπλών πακέτων του τύπου ICMP Error Message είναι απαγορευμένοι από ένα σύνολο ειδικών κανόνων, για να αποφευχθεί το μπλοκάρισα ενός δικτύου από υπερβολική αχρείαστη κίνηση.
3.12) Προσθέτω στον R2 στατική εγγραφή για το 192.168.1.0/24 μέσω του R1 με την εντολή "`route add -net 192.168.1.0/24 172.17.17.1`".

3.13) Ναι, πλέον μπορώ να κάνω traceroute από το PC1 στο PC2. Τα μηνύματα που παράγονται στο WAN1 είναι τα εξής:
- ICMP time exceeded in-transit
- ICMP udp port unreachable
- UDP τεμάχια (απλά)

3.14) Κάνοντας ping από το PC2 στον R1 με την εντολή "`ping 172.17.17.1`" εμφανίζονται μηνύματα "No route to host".

3.15) Διαγράφω στο PC2 τη στατική εγγραφή για το 192.168.1.0/24 με την εντολή "`route del 192.168.1.0/24`".

3.16) Προσθέτω στο PC2 ως προεπιλεγμένη πύλη την 192.168.2.1 με την εντολή "`route add default 192.168.2.1`".

3.17) Κάνοντας ping από το PC2 στη διεύθυνση 172.17.17.1, πλέον παρατηρώ ότι το ping επιτυγχάνει.

3.18) Στην 1η περίπτωση, το PC2 αδυνατεί να στείλει το πακέτο ICMP επειδή η διεύθυνση προορισμού του ανήκει σε διαφορετικό υποδίκτυο από αυτό· επίσης δεν έχει οριστεί κάποια προεπιλεγμένη πύλη για να διαχειρίζεται πακέτα με προορισμό διαφορετικά υποδίκτυα.
Στην 2η περίπτωση, το PC2 μπορεί να στείλει πακέτα οποιουδήποτε άλλου υποδικτύου στην προεπιλεγμένη πύλη του, δηλαδή στην περίπτωσή μας στον R2, ο οποίος με τη σειρά έχει πληροφορίες για την διεπαφή του R1 στο WAN1.

Άσκηση 4

4.1) Ενεργοποιώ τη διεπαφή του PC3 στο LAN2 και ορίζω διεύθυνση IPv4 με την εντολή "`ifconfig em0 inet 192.168.2.3/24`".

4.2) Στο PC3 ορίζω στατική διαδρομή για το υποδίκτυο 192.168.1.0/24 μέσω του R2 με την εντολή "`route add -net 192.168.1.0/24 192.168.2.1`".

4.3) Οι κάρτες δικτύου του R1 πρέπει να βρίσκονται στα τοπικά δίκτυα LAN1 και WAN{1,2}. Για να ορίσω τις διευθύνσεις τους εκτελώ τις εξής εντολές:
"`ifconfig em0 inet 192.168.1.1/24 ; ifconfig em1 inet 172.17.17.1/30 ; ifconfig em2 inet 172.17.17.5/30`".

4.4) Οι κάρτες δικτύου του R2 πρέπει να βρίσκονται στα τοπικά δίκτυα LAN2 και WAN{1,3}. Για να ορίσω τις διευθύνσεις τους εκτελώ τις εξής εντολές:
"`ifconfig em0 inet 192.168.2.1/24 ; ifconfig em1 inet 172.17.17.2/30 ; ifconfig em2 inet 172.17.17.9/30`".

4.5) Οι κάρτες δικτύου του R3 πρέπει να βρίσκονται στα τοπικά δίκτυα WAN{2,3}. Για να ορίσω τις διευθύνσεις τους εκτελώ τις εξής εντολές:
"`ifconfig em0 inet 172.17.17.6/30 ; ifconfig em1 inet 172.17.17.10/30`".

4.6) Προσθέτω στατική εγγραφή στον R1 ώστε να προωθεί πακέτα για το LAN2 μέσω του R2 με την εντολή "`route add -net 192.168.2.0/24 172.17.17.2`".

4.7) Προσθέτω στατική εγγραφή στον R2 ώστε να προωθεί πακέτα για το LAN1 μέσω του R1 με την εντολή "`route add -net 192.168.1.0/24 172.17.17.1`".

4.8) Προσθέτω στατικές εγγραφές στον R3 ώστε να προωθεί πακέτα για το LAN1 μέσω του R1 και για το LAN2 μέσω του R2 με τις εξής αντίστοιχες 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) Προσθέτω στον R1 στατική εγγραφή για το PC3 μέσω του R3 με την εντολή "`route add -net 192.168.2.3 172.17.17.6`".

4.10) Κάνοντας traceroute από το PC1 στο PC2 βλέπω ότι γίνονται 3 βήματα.

4.11) Κάνοντας ping από το PC1 στο PC2 βλέπω ότι γίνονται 3 βήματα. Σημειώνεται ότι, επειδή μόνο οι δρομολογητές μειώνουν κατά 1 την τιμή TTL ενός πακέτου, μπορώ να αποφανθώ για τα βήματα υπολογίζοντας την

διαφορά των TTL των πακέτων και προσθέτοντας 1 για να βρω τα βήματα (η διαφορά των τιμών TTL στην περίπτωσή μας είναι 2).

4.12) Κάνοντας traceroute από το PC1 στο PC3 βλέπω ότι γίνονται 4 βήματα.

4.13) Κάνοντας ping από το PC1 στο PC3 βλέπω ότι γίνονται 3 βήματα. Σημειώνεται, όπως και στο υποερώτημα (4.11) ότι για να αποφανθώ για τα βήματα που επιτέλεσε το ICMP echo reply από το PC3 στο PC1 αφαιρώ την τιμή TTL του από το 64 και προσθέτω 1.

4.14) Το ICMP echo request προς το PC3 (του ερωτήματος 4.12) ακολουθεί την διαδρομή PC1 → R1 → R3 → R2 → PC3.

4.15) Το ICMP echo reply προς το PC1 (του ερωτήματος 4.12) ακολουθεί την διαδρομή PC3 → R2 → R1 → PC1.

4.16) Προσομοιώνω μια βλάβη στη σύνδεση του R1 προς το WAN1 απενεργοποιώντας την αντίστοιχη διεπαφή με την εντολή "`ifconfig em1 down`". Έπειτα, ξεκινώ μια καταγραφή στον R2 ώστε να συλλαμβάνονται πακέτα στο LAN2 με την εντολή "`tcpdump -i em0`".

4.17) Δοκιμάζω traceroute από το PC1 στο PC2 με την εντολή "`traceroute 192.168.2.2`" και αφήνω να ολοκληρωθούν τουλάχιστον 3 βήματα. Παρατηρώ πως δεν παράγονται πακέτα UDP στο PC2.

4.18) Δοκιμάζω τώρα traceroute από το PC1 στο PC3 με την εντολή "`traceroute 192.168.2.3`" και αφήνω να ολοκληρωθούν τουλάχιστον 3 βήματα. Παρατηρώ πως παράγονται πακέτα UDP στο PC3.

4.19) Αλλάζω στους πίνακες δρομολόγησης των R{1,2} τις υπάρχουσες διαδρομές προς τα LAN{1,2} ώστε όλη η κίνηση μεταξύ τους να διέρχεται μέσω του R3 με τις εξής εντολές "`route change 192.168.2.0/24 172.17.17.6`" και "`route change 192.168.1.0/24 172.17.17.10`". Με traceroute επιβεβαιώνω πως υπάρχει η επικοινωνία των PC{1,3}.

4.20) Στον R1 με τη βοήθεια της εντολής route βλέπω την πληροφορία για τις διαδρομές προς τις διευθύνσεις IPv4 των PC{2,3} με την εντολή "`route show 192.168.2.2 ; route show 192.168.2.3`" (μπορώ να εκτελέσω τις δύο εντολές σε ξεχωριστά παράθυρα για να μπορώ να διακρίνω ευκολότερα τις διαφορές μεταξύ των αποτελεσμάτων τους). Παρατηρώ, λοιπόν, ότι ο πίνακας δρομολόγησης του R1 αναφέρει ότι τα πακέτα για το PC2 έχουν προορισμό το υποδίκτυο 192.168.2.0/24, ενώ

αυτά για το PC3 έχουν προορισμό την διεύθυνση IPv4 του PC3, 192.168.2.3 (netmask 255.255.255.255).

4.21) Όταν κάνω ping από το PC1 στο PC3, η εγγραφή του πίνακα δρομολόγησης στον R1 που επιλέγεται είναι αυτή για την διεύθυνση του PC3 (και όχι αυτή για το υποδίκτυο 192.168.2.0/24), επειδή η δρομολόγηση ενός πακέτου πάντα γίνεται με την εγγραφή που η διεύθυνση προορισμού της και αυτή του πακέτου έχουν το μεγαλύτερο μήκος κοινού προθέματος. Αφού, λοιπόν, υπάρχει η διεύθυνση του PC3, τότε αυτή θα έχει το μέγιστο μήκος προθέματος (32) και θα επιλεχθεί αυτή.

Άσκηση 5

5.1) Τροποποιώ στον R3 την υπάρχουσα στατική εγγραφή για το δίκτυο 192.168.2.0/24 ώστε να στέλνει την κίνηση στον R1 αντί στον R2 με την εντολή "`route change 192.168.2.0/24 172.17.17.5`".

5.2) Εκτελώ ping στέλνοντας 1 πακέτο ICMP echo request από το PC1 στο PC2. Παρατηρώ ότι το ping αποτυγχάνει.

5.3) Η αποτυχία του ping του προηγούμενου ερωτήματος δικαιολογείται από το γεγονός ότι υποερώτημα (5.1) δημιουργήσαμε σκόπιμα ένα βρόχο μεταξύ των R{1,3} και το πακέτο στέλνεται συνεχώς από τον R1 στον R3 και αντίστροφα. Το μήνυμα λάθους "Time to live exceeded" προέρχεται από την διεπαφή του R3 στο WAN2 (172.17.17.6).

5.4) Ξεκινώ δύο καταγραφές· μία στην διεπαφή του R1 στο LAN1 και μία στην διεπαφή του R3 στο WAN2, αποθηκεύοντας τα αποτελέσματά τους στα αρχεία file1.txt και file2.txt, αντίστοιχα, με τις εξής εντολές αντίστοιχα:
"`tcpdump -i em0 -l | tee file1.txt`" και
"`tcpdump -i em0 -l | tee file2.txt`".

5.5) Επαναλαμβάνω το ping από το PC1 στο PC2 (με την εντολή "`ping -c 1 192.168.2.2`") και μόλις ολοκληρωθεί σταματώ τις καταγραφές στα R{1,3}.
Με τις παρακάτω εντολές παρατηρώ ότι καταγράφηκαν 1 πακέτο ICMP echo request, 62 πακέτα ICMP redirect και 1 πακέτο ICMP time exceeded στην καταγραφή του R1 στο LAN1:
"`grep -c 'ICMP echo request' file1.txt`",
"`grep -c 'ICMP redirect' file1.txt`" και

“`grep -c ‘ICMP time exceeded’ file1.txt`”.
Επίσης, με τις παρακάτω εντολές παρατηρώ ότι καταγράφηκαν 63 πακέτα ICMP echo request, 31 πακέτα ICMP redirect και 1 πακέτο ICMP time exceeded στην καταγραφή του R3 στο WAN1:
“`grep -c ‘ICMP echo request’ file2.txt`”,
“`grep -c ‘ICMP redirect’ file2.txt`” και
“`grep -c ‘ICMP time exceeded’ file2.txt`”.

5.6) Ξεκινώ 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 με την εντολή
“`tcpdump -i em0 -e -vvv “icmp[0] == 8”`”. (file3.txt)

5.7) Εκτελώ πάλι ping ενός μόνο πακέτου από το PC1 στο PC2 με την εντολή “`ping -c 1 192.168.2.2`” και, αφού ολοκληρωθεί, σταματώ την καταγραφή του R3 στο WAN2. Από την καταγραφή βλέπω ότι εμφανίσθηκαν 63 ICMP echo request πακέτα, 32 από τα οποία έχουν πηγή τον R1 και 31 άλλα που έχουν πηγή τον R3.

5.8) Ξεκινώ 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 με τις αντίστοιχες εντολές
“`tcpdump -i em0 -vvv “icmp[0] == 5”`” (file4.txt) και
“`tcpdump -i em0 -vvv “icmp[0] == 5”`” (file5.txt).

5.9) Εκτελώ πάλι ping ενός μόνο πακέτου από το PC1 στο PC2 με την εντολή “`ping -c 1 192.168.2.2`” και, αφού ολοκληρωθεί, σταματώ την καταγραφή των R{1,3}. Παρατηρώ ότι στο WAN2 εμφανίζονται 31 ICMP redirect πακέτα. Αυτό είναι αναμενόμενο, αφού γνωρίζουμε ότι ο R1 έστειλε 31 ICMP echo request πακέτα στον R3 (από το ερώτημα 5.7), και ότι για κάθε πακέτο ICMP echo request που ο R3 λαμβάνει από τον R1 στέλνει ένα ακριβώς πακέτο ICMP redirect, επειδή από τον πίνακα δρομολόγησής του βλέπει ότι πρέπει να προωθήσει το ICMP echo request στην διεπαφή από την οποία έλαβε το πακέτο. (Σημειώνεται ότι το πακέτο ICMP echo request είναι μόνο ένα και απλά στέλνεται συνεχώς από τον R1 στον R3 και αντίστροφα).

5.10) Στο LAN1 εμφανίζονται 31 πακέτα ICMP redirect με πηγή τον R1. Αυτό συμβαίνει επειδή ο R1 λαμβάνει 31 φορές το πακέτο ICMP echo request από τον R3, και έτσι στέλνει 31 φορές πακέτα ICMP redirect στον PC1.

5.11) Ξεκινώ νέες καταγραφές όπως στην ερώτηση 5.4 με τις εντολές "`tcpdump -i em0 -l | tee file6.txt`" και "`tcpdump -i em0 -l | tee file7.txt`" και εκτελώ την εντολή "`traceroute -I -q 1 192.168.2.2`" από το PC1 στο PC2. Μέχρις ότου ολοκληρωθεί η εκτέλεση της εντολής εμφανίζονται 64 βήματα. Η διαδρομή που καταγράφεται έχει αρχή τον R1 και έπειτα τους R{3,1} εναλλάξ (63 φορές).

5.12) Σταματώ τις καταγραφές που ξεκίνησα στους R{1,3}. Συνολικά από το PC1 στάλθηκαν 64 πακέτα ICMP echo request και στο WAN2 εμφανίστηκαν 2016 πακέτα ICMP echo request.

Για τα πακέτα ICMP του LAN1, γνωρίζω ότι η traceroute παράγει πακέτα με τιμές στο πεδίο TTL στο εύρος από 1 μέχρι 64.

Όσον αφορά στα πακέτα ICMP στο WAN2 τα πακέτα αυτά θα φτάνουν με τιμές TTL στο εύρος [0,63]. Επομένως, τα 63 αυτά πακέτα στο WAN2 θα ανταλλάσσονται συνεχώς μεταξύ των R{1,3} μέχρι να μηδενιστεί η τιμή TTL τους. Επομένως, αρκεί να προσθέσουμε όλους τους ακεραίους από το 0 έως το 63, δηλαδή ο αριθμός των πακέτων δίνεται από τον παρακάτω τύπο:

$$\sum_{k=0}^{63} k = 2016$$

5.13) Στο WAN2 εμφανίσθηκαν 32 μηνύματα ICMP time exceeded. Η τιμή αυτή δικαιολογείται από το γεγονός ότι τα μηνύματα αυτά μπορεί να έχουν πηγή μόνο τον R3, αφού όλα τα μηνύματα ICMP time exceeded που παρήχθησαν από τον R1 στάλθηκαν κατευθείαν στο LAN1. Έτσι, είναι λογικό τα μισά από τα 64 πακέτα που παράχθηκαν να δημιουργήσουν μηνύματα ICMP time exceeded με πηγή τον R3.

5.14) Ένας άλλος τρόπος για να μετρήσω τα μηνύματα ICMP echo request ή ICMP time exceeded χωρίς να χρειαστεί να αποθηκεύσω τα αποτελέσματα της tcpdump είναι η εισαγωγή φίλτρου πριν ξεκινήσω την καταγραφή, έτσι ώστε να συλληφθούν συγκεκριμένα πακέτα. Για παράδειγμα, για να μετρήσω τα ICMP echo requests πακέτα σε μία καταγραφή εκτελώ την εντολή "`tcpdump "icmp[0] == 8"`" και αφού την σταματήσω με Ctrl+C εμφανίζεται σχετικό μήνυμα με τον αριθμό των πακέτων που καταγράφηκαν.

Άσκηση 6

6.1) Για να κωδικοποιηθούν 120 υπολογιστές στο LAN1 θα πρέπει ο αριθμός host να έχει μήκος 7 bits (ο αριθμός $2^7 = 128$ είναι ο αμέσως μεγαλύτερος του 100 που είναι δύναμη του 2). Άρα, ο αριθμός δικτύου θα πρέπει να έχει μήκος 32 – 7 = 25 bits και, έτσι, η διεύθυνση υποδικτύου του LAN1 είναι 172.17.17.0/25. (…0000 0000)

6.2) Για να κωδικοποιηθούν 60 υπολογιστές στο LAN2 θα πρέπει ο αριθμός host να έχει μήκος 6 bits (ο αριθμός $2^6 = 64$ είναι ο αμέσως μεγαλύτερος του 60 που είναι δύναμη του 2). Άρα, ο αριθμός δικτύου θα πρέπει να έχει μήκος 32 – 6 = 26 bits και, έτσι, η διεύθυνση υποδικτύου του LAN2 είναι 172.17.17.192/26. (…1100 0000)

6.3) Για να κωδικοποιηθούν 30 υπολογιστές στο LAN3 θα πρέπει ο αριθμός host να έχει μήκος 5 bits (ο αριθμός $2^5 = 32$ είναι ο αμέσως μεγαλύτερος του 30 που είναι δύναμη του 2). Άρα, ο αριθμός δικτύου θα πρέπει να έχει μήκος 32 – 5 = 27 bits και, έτσι, η διεύθυνση υποδικτύου του LAN3 είναι 172.17.17.160/27. (…1010 0000)

Στο σημείο αυτό, σημειώνεται ότι για ένα μπλοκ διευθύνσεων η διεύθυνση με τον μικρότερο αριθμό host είναι η διεύθυνση που χαρακτηρίζει το δίκτυο, και αυτή με τον μεγαλύτερο αριθμό host είναι η διεύθυνση εκπομπής (broadcast). Επομένως, οι 2 αυτές διευθύνσεις δεν μπορούν ποτέ να αποδοθούν σε υπολογιστές. Έτσι, εάν θέλουμε σε ένα υποδίκτυο να μπορούν να υπάρξουν τουλάχιστον n υπολογιστές/διαφορετικές διευθύνσεις IP, θα πρέπει ο αριθμός host να έχε μήκος k, όπου 2^k να είναι ο ακριβώς μεγαλύτερος ακέραιος του n και να ισχύει $2^k \geq n + 2$.

Επίσης, Στο παρακάτω σχήμα φαίνεται ο τρόπος με τον οποίο έχει χωριστεί το μπλοκ διευθύνσεων στα LANs:

0 … 127	…	160…191	192 … 255
LAN1 /25	X	LAN3	LAN2 /26
128 PCs	32 PCs	32 PCs	64 PCs

6.4) Στο LAN1 ορίζω ως διεύθυνση IPv4 για το PC1 αυτή με τη μικρότερη τιμή host, δηλαδή την 172.17.17.1/25, ενώ για τον R1 αυτήν με τη μεγαλύτερη τιμή host, δηλαδή την 172.17.17.126/25.

6.5) Αντίστοιχα, στο LAN3 ορίζω ως διεύθυνση IPv4 για το PC4 αυτή με τη μικρότερη τιμή host, δηλαδή την 172.17.17.161/27, ενώ για τον R3 αυτήν με τη μεγαλύτερη τιμή host, δηλαδή την 172.17.17.190/27.

6.6) Στο υποδίκτυο του LAN2 ορίζω ως διεύθυνση IPv4 για τον R2 αυτή με τη μικρότερη τιμή host, δηλαδή την 172.17.17.193/26, ενώ για τα PC{2,3} αυτές με τις μεγαλύτερες τιμές host, δηλαδή τις 172.17.17.253/26 και 172.17.17.254/26, αντίστοιχα.

6.7) Ορίζω στα PC ως προεπιλεγμένη πύλη τους αντίστοιχους δρομολογητές με τις εντολές "`route add default 172.17.17.X`" X=126,193,190.

6.8) Στον R1 ορίζω στατικές εγγραφές ώστε να προωθεί πακέτα για τα LAN{2,3} μέσω του R2 με την εντολή
"`route add -net 172.17.17.192/26 172.17.17.130`" και
"`route add -net 172.17.17.160/27 172.17.17.130`"

6.9) Στον R2 ορίζω στατικές εγγραφές, ώστε να προωθεί πακέτα για τα LAN{1,3} μέσω του R3 με τις εντολές
"`route add -net 172.17.17.0/25 172.17.17.137`" και
"`route add -net 172.17.17.160/27 172.17.17.137`".

6.10) Στον R3 ορίζω στατικές εγγραφές, ώστε να προωθεί πακέτα για τα LAN{1,2} μέσω του R1 με τις εντολές
"`route add -net 172.17.17.0/25 172.17.17.133`" και
"`route add -net 172.17.17.192/26 172.17.17.133`".

6.11) Κάνοντας τα pings PC1 → PC2, PC2 → PC4, PC3 → PC1, επιβεβαιώνω ότι υπάρχει επικοινωνία ανάμεσα σε όλα τα LANs.

Άσκηση 7

7.1) Στον παρακάτω πίνακα καταγράφονται οι MACs των PC{2,3}:

PC	MAC
PC2	08:00:27:fe:57:4c
PC3	08:00:27:21:df:54

7.2) Αλλάζω την διεύθυνση IPv4 του PC2 σε αυτήν του PC3 με την εντολή "`ifconfig em0 inet 172.17.17.254/26`".

7.3) Στην προσπάθεια να αλλάξω την IPv4 address του PC2 σε αυτήν του PC3 λαμβάνω το μήνυμα λάθους «08:00:27:21:df:54 is using my IP address 172.17.17.254 on em0!».

7.4) Ναι, στο PC3 εμφανίστηκε ακριβώς η ίδια ένδειξη λάθους, με το ίδιο μήνυμα (με την MAC του PC2).

7.5) Παρατηρώ ότι, τελικά, η διεύθυνση IPv4 του PC2 άλλαξε. Συμπεραίνω, λοιπόν, ότι τα μηνύματα λάθους που εμφανίστηκαν είναι απλά ενημερωτικά και δεν απαγορεύουν τέτοιου είδους «χειροκίνητες» αλλαγές των διευθύνσεων IP.

7.6) Παρατηρώ ότι ο R2 δεν είναι πλέον ορισμένος ως προεπιλεγμένη πύλη στο PC2. Αυτό συνέβη επειδή άλλαξε η διεύθυνση IP του PC2.

7.7) Ορίζω τον R2 ως προεπιλεγμένη πύλη του PC2 με την εντολή "`route add default 172.17.17.193`".

7.8) Καθαρίζω τους πίνακες ARP των PC{2,3} και R2 με την εντολή "`arp -a -d`".

7.9) Στον R2 ξεκινώ μια καταγραφή χωρίς επίλυση διευθύνσεων, ώστε να συλληφθούν όλα τα τεμάχια ARP στο LAN2 με την εντολή "`tcpdump -i em0 arp`".

7.10) Στα PC{2,3} ξεκινώ καταγραφές χωρίς επίλυση διευθύνσεων, ώστε να συλληφθούν όλα τα τεμάχια TCP με την εντολή "`tcpdump tcp`".

7.11) Από το PC1 προσπαθώ να συνδεθώ με SSH ως χρήστης lab στην διεύθυνση IPv4 του PC3 με την εντολή "`ssh -l lab 172.17.17.254`". Εμφανίζεται σχετική ένδειξη λάθους με το μήνυμα «Fssh_kex_exchange_identification: read: Connection reset by peer Connection reset by 172.17.17.190 port 22».

7.12) Αφού σταματήσω τις καταγραφές, επαναλαμβάνω την προσπάθεια σύνδεσης με SSH και βλέπω ότι αυτή επιτυγχάνει.

7.13) Στον πίνακα ARP του R2 υπάρχει η εγγραφή με την διεύθυνση IPv4 των PC{2,3} η οποία αναφέρει την διεύθυνση MAC του PC2 (…:4c).

7.14) Στην καταγραφή των ARP πακέτων στον R2 φαίνεται ότι το PC3 απάντησε πρώτο και το PC2 απάντησε δεύτερο.

7.15) Η διεύθυνση MAC που περιέχει ο πίνακας ARP του R2 ανήκει στο PC2 (τον υπολογιστή που απάντησε δεύτερος).

7.16) Με την 2η προσπάθεια σύνδεσης με SSH παρατηρώ ότι συνδέθηκα στο PC2. Αυτό το συμπεραίνω εκτελώντας την εντολή "`ifconfig em0 ether`" στο PC1 (μέσα στο παράθυρο που εκτελείται το SSH) και βλέποντας ότι η διεύθυνση MAC που εμφανίζεται ανήκει στο PC2.

7.17) Το παραπάνω μπορώ, επίσης, να το συμπεράνω εκτελώντας την εντολή "`who`" από το PC2, για να εμφανίσω τους λογαριασμούς που είναι συνδεδεμένοι στο παρόν μηχάνημα.

7.18) Την πρώτη φορά το SSH δεν λειτούργησε σωστά, επειδή ο R2 για το χρονικό διάστημα που δεν είχε λάβει ακόμα το ARP reply του PC2, εγκαταστάθηκε σύνδεση με το PC3. Μόλις, όμως, έλαβε το ARP reply πακέτο από το PC2 και έστειλε το επόμενο πακέτο στο PC2 πλέον, το PC2 έστειλε πακέτα TCP με ενεργοποιημένη την σημαία RST για να σηματοδοτήσει ότι η σύνδεση ότι η σύνδεση δεν είναι ενεργή. Στη συνέχεια, στάλθηκαν περαιτέρω πακέτα TCP με την σημαία RST από το PC1.

Την δεύτερη φορά, ο R2 είχε ήδη στον πίνακα ARP του την εγγραφή που αντιστοιχούσε την διεύθυνση IP με την διεύθυνση MAC του PC2. Έτσι, η σύνδεση δεν χρειάστηκε να γίνει reset και συνεχίστηκε αενάως.