Ονοματεπώνυμο: Παναγιώτης Ζευγολατάκος	**Όνομα PC:** panos-PC
Ομάδα: 1	**Ημερομηνία:** 21/03/2021

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 PC1: ifconfig em0 192.168.1.2/24

PC2: ifconfig em0 192.168.2.2/24

R1: ifconfig em0 192.168.1.1/24, ifconfig em1 192.168.2.1/24

1.2 Πρόσθεσα τη γραμμή gateway_enable="YES" (την έβγαλα από σχόλιο) και έκανα reboot

1.3 route add -net 192.168.2.0/24 192.168.1.1

1.4 U: Η διαδρομή είναι ενεργή (up).

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

S: Η διαδρομή έχει οριστεί στατικά.

1.5 Απέτυχε.

1.6 Παρατηρώ πως τα ICMP Echo Request φτάνουν στο R1 και στη συνέχεια το R1 στέλνει πακέτα ARP Request για τη διεύθυνση του PC2, το οποίο PC2 τα λαμβάνει, ωστόσο δεν ξέρει πως να απαντήσει λόγω έλλειψης εγγραφής στον πίνακα δρομολόγησης.

1.7 route add -net 192.168.1.0/24 192.168.2.1

1.8 Ναι, πετυχαίνει.

1.9 Όταν αποδοθεί μια διεύθυνση IP στις διεπαφές των PC1, PC2, προστίθενται στον πίνακα δρομολόγησης οι κόμβοι που ανήκουν στο αντίστοιχο LAN, επομένως δε χρειάζεται να προστεθούν οι εγγραφές από το χρήστη.

2

2.1 route del 192.168.2.0/24

2.2 ifconfig em0 192.168.1.2/20

2.3 Από την προοπτική του PC1 βρίσκονται στο ίδιο υποδίκτυο εφόσον τα πρώτα 20 bits τους είναι πλέον τα ίδια (20 λόγω του νέου προθέματος του PC1).

2.4 Όχι

2.5 Είναι επιτυχές. Το R1 λαμβάνει τα ARP Request του PC1 και απαντά ως το PC2, δίνοντας βέβαια τη δική του διεύθυνση MAC, λαμβάνοντας το πακέτο ICMP και προωθώντας το στο PC2.

2.6 Αποτυγχάνει επειδή το PC3 δεν έχει στατική εγγραφή για το δίκτυο του PC1 όπως το PC2, επομένως δεν ξέρει πως να προωθήσει τα ICMP Reply.

2.7 route add -net 192.168.1.0/24 192.168.2.1

2.8 arp -ad

2.9 tcpdump -n -e -i em0, tcpdump -n -e -i em1

2.10 Παρατηρώ πως στο ARP Reply το R1 δίνει τη δική του MAC διεύθυνση ως τη MAC διεύθυνση που αντιστοιχεί στην διεύθυνση IP 192.168.2.3

2.11 Προς τη διεύθυνση MAC της διεπαφής em0 του R1.

2.12 Από τη διεύθυνση MAC της διεπαφής em1 του R1

2.13 (Δύσκολο να σχεδιάσω στο Word, θα τα γράψω όπως τα έγραψα στην 4η εργαστηριακή άσκηση)

ARP Request PC1 (για τη διεύθυνση MAC του PC3)

ARP Reply R1→ PC1 (με τη δική του διεύθυνση MAC ως διεύθυνση MAC του PC3)

ICMP Request PC1→ R1

ARP Request R1 (για τη διεύθυνση MAC του PC3)

ARP Reply PC3→R1

ICMP Request R1→ PC3 (προώθηση του προηγούμενου)

ICMP Reply PC3→ R1

ICMP Reply R1→ PC1

2.14 Το πρόθεμα μπορεί να είναι μέχρι και /22. Εφόσον η διεύθυνση του PC3 είναι 192.168.2.3 (Όπου 2 σε δυαδική αναπαράσταση: 00000**0**10 και με bold μέχρι που φτάνει το πρόθεμα /22), μέχρι /22 η εφαρμογή της μάσκας θα δουλεύει σωστά και από την προοπτική του PC1 θα βρίσκονται στο ίδιο υποδίκτυο.

2.15 ifconfig em0 192.168.1.2/23

2.16 route add -net 192.168.2.0/24 -interface em0

2.17 Εμφανίζεται η διεύθυνση MAC της διεπαφής em0

2.18 Είναι επιτυχές, εφόσον με την εφαρμογή της μάσκας δε θεωρούσε πως βρισκόταν στο ίδιο υποδίκτυο, επομένως χρειαζόταν να οριστεί διαδρομή προς αυτό (πράγμα που έγινε από το χρήστη).

2.19 sysctl net.link.ether.inet.proxywall=0

2.20 route change -net 192.168.2.0/24 192.168.1.1

2.21 ifconfig em0 192.168.1.2/24

2.22 Διαγράφηκε, οπότε εκτελώ: 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

3.4 Δεν παράγονται μηνύματα ICMP στο WAN1, εφόσον ο R1 δεν ξέρει πως να προωθήσει τα πακέτα ICMP του PC1.

3.5 Η ένδειξη λάθους !H σημαίνει πως είναι Unreachable.

3.6 route add -net 192.168.2.0/24 172.17.17.2

3.7 Όχι.

3.8 Βλέπω μηνύματα ICMP host unreachable που στέλνει το R2 στο PC2, αφού προσπαθήσει να στείλει ICMP Reply το PC2.

3.9 Δεν παρατηρώ μηνύματα ICMP, παρατηρώ μηνύματα UDP, εφόσον η εντολή traceroute στα συστήματα UNIX λειτουργεί με UDP.

3.10 Στο LAN2 παράγονται μηνύματα udp port 33441 unreachable.

3.11 Αν χρησιμοποιηθεί ICMP error message για απάντηση σε ICMP error message θα δημιουργηθεί βρόγχος.

3.12 route add -net 192.16.1.0/24 172.17.17.1

3.13 Μπορώ, αν και τα μηνύματα που παράγονται στο WAN1 είναι ICMP time exceeded in-transit ή udp port _ unreachable

3.14 Παρατηρώ no route to host.

3.15 route del 192.168.1.0/24

3.16 route add default 192.168.2.1

3.17 Πετυχαίνει, εφόσον προωθούνται από την προκαθορισμένη πύλη R2.

3.18 Παρόλο που δε θέσαμε ακριβή δρομολόγηση για τη διεύθυνση 172.17.17.1, γνωρίζουμε πως είναι η διεπαφή em1 του R1, η οποία επικοινωνεί με το R2, οπότε χρειάστηκε μόνο να θέσουμε ως προκαθορισμένη πύλη το R2 και αυτό θα προωθήσει τα ICMP στο R1 (και τις απαντήσεις πίσω στο 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 LAN1: ifconfig em0 192.168.1.1/24

WAN1: ifconfig em1 172.17.17.1/30

WAN2: 172.17.17.5/30

4.4 WAN1: ifconfig em0 172.17.17.2/30

LAN1: ifconfig em1 192.168.2.1/24

WAN2: ifconfig em2 172.17.17.9/30

4.5 WAN2: ifconfig em0 172.17.17.6/30

WAN3: ifconfig em1 172.17.17.10/30

4.6 route add -net 192.168.2.0/24 172.17.17.2

4.7 route add -net 192.168.1.0/24 172.17.17.1

4.8 route add -net 192.168.1.0/24 172.17.17.5, route add -net 192.168.2.0/24 172.17.17.9

4.9 route add -host 192.168.2.3 172.17.17.6, Η σημαία είναι η H.

4.10 3.

4.11 TTL=62 (64-2), άρα πάλι 3.

4.12 4.

4.13 TTL=62 (64-2), άρα 3.

4.14 PC1→ R1→ R3→ R2→ PC3

4.15 PC2→ R2→ R1→ PC1

4.16 tcpdump -n -e -i em1

4.17 Όχι.

4.18 Ναι, φτάνουν και παράγονται udp port _ unreachable

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

4.20 Παρατηρώ πως για τη διεύθυνση 192.168.2.2 επιλέγεται η διαδρομή με βάση το δίκτυο 192.168.2.0, ενώ για τη διεύθυνση 192.168.2.3 επιλέγεται η διαδρομή με βάση την ίδια τη διεύθυνση, εφόσον την είχαμε ορίσει με την εντολή route add -host 192.168.2.3 172.17.17.6

4.21 Επιλέγεται η εγγραφή που το δρομολογεί βάσει της διεύθυνσής του (δηλ. Destination:192.168.2.3 Gateway:172.17.17.6)

5

5.1 route change -net 192.168.2.0/24 172.17.17.5

5.2 Όχι.

5.3 Εμφανίζεται time to live exceeded από τη διεπαφή em0 του R3.

5.4 Στη διεπαφή em0 του R3 ή στη διεπαφή em2 του R1.

5.5 tcpdump -e -i em0 'icmp'

5.6 Παράχθηκε 1 αλλά εμφανίστηκαν 64.

5.7 tcpdump -n -e -i em0 | tee 5_5_5

5.8 Εμφανίζονται 64 βήματα. Η διαδρομή είναι η R1,R3,R1,R3,…,R3 .

5.9 grep -a "echo" 5_5_5 | wc -l

Παρατηρώ πως στάλθηκαν 64 από το PC1.

5.10 grep -a “echo” 5_5_5 | wc -l

Παίρνω ως αποτέλεσμα τον αριθμό 2016, ο οποίος είναι το άθροισμα της ζωής κάθε πακέτου που κατέληξε στο βρόγχο (με μια μικρή απόκλιση, εφόσον δεν είναι ακριβώς 64*64/2).

5.11 grep -a “time exceeded” 5_5_5 | wc -l

Παίρνω ως αποτέλεσμα τον αριθμό 30, ο οποίος είναι ο αριθμός των πακέτων που κατέληξαν στο R3 (τα υπόλοιπα 34 κατέληξαν στο R1).

5.12 tcpdump -n -e -i em0 ‘icmp[icmptype]==8’ για echo request

tcpdump -n -e -i em0 ‘icmp[icmptype]==11’ για time exceeded

Και κοιτάμε τον αριθμό στο τέλος της καταγραφής.

5.13 Διαφέρουν στο TTL, στο ping έχουν σταθερό TTL=64 ενώ στο traceroute έχουν μεταβλητό TTL, αφού υπάρχει 1 πακέτο για κάθε 1 TTL.

5.14 Εξαιτίας του TTL (όταν γίνει 0 γίνονται discard).

6

Προεργασία:
LAN1 → 10 00 00 00
LAN2 → 11 00 00 00
LAN3 → 10 10 00 00
129 → 10 00 00 01
130 → 10 00 00 10
133 → 10 00 01 01
134 → 10 00 01 10
137 → 10 00 10 01
138 → 10 00 10 10

6.1 172.17.17.0/25 ($128=2^7$ → 32-7=25)

6.2 172.17.17.192/26 ($64=2^6$ → 32-6=26)

6.3 172.17.17.160/27 ($32=2^5$ → 32-5=27)

6.4 PC1: ifconfig em0 172.17.17.1/25

R1: ifconfig em0 172.17.17.126/25

6.5 PC4: ifconfig em0 172.17.17.161/27

R1: ifconfig em2 172.17.17.190/27

6.6 PC2: ifconfig em0 172.17.17.253/26

PC3: ifconfig em0 172.17.17.254/26

R2: ifconfig em1 172.17.17.193/26

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 PC1: ping 172.17.17.253
PC2: ping 172.17.17.161
PC3: ping 172.17.17.1

7

7.1 PC2 → 08:00:27:d5:a2:b7

PC3 → 08:00:27:f1:a9:fa

7.2 ifconfig em0 172.17.17.254/26

7.3 Ναι, πως ανήκει στο PC3.

7.4 Ναι, πως χρησιμοποιείται η διεύθυνση IP του στο PC2.

7.5 Ναι. Εμφανίστηκε γιατί δεν είναι σωστό/καλή πρακτική να έχουν δύο διαφορετικές συσκευές στο ίδιο υποδίκτυο την ίδια διεύθυνση IP.

7.6 Όχι, διότι με την αλλαγή διεύθυνσης IP διαγράφεται η προεπιλεγμένη πύλη.

7.7 route add default 172.17.17.193

7.8 arp -ad (PC2, PC3, R2)

7.9 tcpdump -n -e -vv -i em1 'arp'

7.10 tcpdump -n -e -vv -i em0 'tcp'

7.11 ssh_exchange_identification: read: Connection reset by peer

7.12 Ναι

7.13 (η 4η εγγραφή είναι για το PC3)

```
root@pc:~ # arp -a
? (172.17.17.137) at 08:00:27:77:c4:86 on em2 expires in 476 seconds [ethernet]
? (172.17.17.138) at 08:00:27:a0:ed:23 on em2 permanent [ethernet]
? (172.17.17.193) at 08:00:27:39:7b:fa on em1 permanent [ethernet]
? (172.17.17.254) at 08:00:27:f1:a9:fa on em1 expires in 1128 seconds [ethernet]
? (172.17.17.129) at 08:00:27:0b:ea:04 on em0 expires in 476 seconds [ethernet]
? (172.17.17.130) at 08:00:27:7f:ad:4a on em0 permanent [ethernet]
```

7.14 Απάντησε πρώτο το PC2.

(08:00:27:39:7b:fa > ff:ff:ff:ff:ff:ff →ARP Request

08:00:27:d5:a2:b7 > 08:00:27:39:7b:fa → ARP Reply από το PC2

08:00:27:f1:a9:fa > 08:00:27:39:7b:fa → ARP Reply από το PC3)

```
root@pc:~ # tcpdump -n -e -vv -i em1 'arp'
tcpdump: listening on em1, link-type EN10MB (Ethernet), capture size 65535 bytes
capability mode sandbox enabled
11:42:26.523402 08:00:27:39:7b:fa > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), l
ength 42: Ethernet (len 6), IPv4 (len 4), Request who-has 172.17.17.254 tell 172
.17.17.193, length 28
11:42:26.523636 08:00:27:d5:a2:b7 > 08:00:27:39:7b:fa, ethertype ARP (0x0806), l
ength 60: Ethernet (len 6), IPv4 (len 4), Reply 172.17.17.254 is-at 08:00:27:d5:
a2:b7, length 46
11:42:26.523650 08:00:27:f1:a9:fa > 08:00:27:39:7b:fa, ethertype ARP (0x0806), l
ength 60: Ethernet (len 6), IPv4 (len 4), Reply 172.17.17.254 is-at 08:00:27:f1:
a9:fa, length 46
^C
3 packets captured
15 packets received by filter
0 packets dropped by kernel
```

7.15 Στο PC3.

7.16 Στο PC3.

7.17 Εκτελώντας την εντολή w στο PC3 όσο το PC1 είναι συνδεδεμένο μπορώ να δω πως το PC1 είναι συνδεδεμένο σε αυτό. Εναλλακτικά, εκτελώντας την εντολή netstat -n μπορώ να δω τη σύνδεση του PC1 στο PC3 (εφόσον το PC1 είναι συνδεδεμένο στο PC3, είτε τρέξω την εντολή στο PC1, είτε την τρέξω στο PC3 βλέπω το ίδιο αποτέλεσμα).

7.18 Στην πρώτη προσπάθεια, στην καταγραφή στο PC2, τα flags είναι S και S. (δηλαδή Syn και Syn,Ack) και επαναλαμβανόταν το δεύτερο τεμάχιο της τριμερούς χειραψίας μέχρι να σταματήσει η προσπάθεια. Από την καταγραφή του PC3, βλέπω πως το PC3 δίνει και αυτό τη δική του διεύθυνση MAC σε ARP Reply, οδηγώντας έτσι σε αποτυχία σύνδεσης, εφόσον άλλαξε ο στόχος κατά τη διάρκεια της σύνδεσης.

Στη δεύτερη προσπάθεια δεν γίνονται ARP Request, εφόσον έχει αντιστοιχηθεί η διεύθυνση MAC του PC3 στη διεύθυνση 172.17.17.254, επειδή ήρθε τελευταία.