Εργαστηριακή Άσκηση 5

Στατική δρομολόγηση

Ονοματεπώνυμο: Άννα Κουτσώνη	**Όνομα PC:** DESKTOP-90FT571
Ομάδα: 1	**Ημερομηνία:** 12/03/2024

Άσκηση 1

1.1 PC1: ifconfig em0 inet 192.168.1.2/24
PC2: ifconfig em0 inet 192.168.2.2/24
1.2 R1: ifconfig em0 inet 192.168.1.1/24
ifconfig em1 inet 192.168.2.1/24
sysrc ifconfig_em0="inet 192.168.1.1 netmask 255.255.255.0"
sysrc ifconfig_em1="inet 192.168.2.1 netmask 255.255.255.0"
1.3 sysrc gateway_enable=”YES”
1.4 service netif restart && service routing restart
1.5 route add -net 192.168.2.0/24 192.168.1.1
1.6 netstat -r
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.
1.7 Δεν λαμβάνεται απάντηση. Καταγράφοντας τα πακέτα που στέλνονται με tcpudmp παρατηρούμε ότι ο PC1 στέλνει κανονικά ICMP echo requests αλλά ο PC2 δεν στέλνει ICMP echo replies.
1.8 Τόσο στο LAN1 όσο και στο LAN2 παράγονται ICMP echo requests. Δεν παράγονται ICMP echo replies γιατί ο PC2 δεν έχει καμία σχετική εγγραφή στον πίνακα δρομολόγησης του ώστε να ξέρει που να στείλει τα πακέτα.
1.9 route add -net 192.168.1.0/24 192.168.2.1
1.10 Ναι, υπάρχει.
1.11 Γιατί ο R1 διαθέτει εξ’αρχής δύο διεπαφές, μία στο κάθε υποδίκτυο και έτσι έχει ήδη τις σχετικές εγγραφές στον πίνακα δρομολόγησης του.

Άσκηση 2

2.1 route del 192.168.2.0/24
2.2 ifconfig em0 inet 192.168.1.2/20
2.3 Στο ίδιο
2.4 Όχι δεν είναι. Παίρνουμε μήνυμα host is down.
2.5 Επιτυγχάνει διότι πλέον είναι ο δρομολογητής λειτουργεί ως proxy και απαντάει στο ARP Request του PC1 με τη δική του MAC αφού ο PC2 ανήκει σε υποδίκτυο στο οποίο ο R1 μπορεί να προωθήσει τα πακέτα.
2.6 Αποτυγχάνει γιατί δεν έχει προστεθεί στον πίνακα προώθησης του PC3 εγγραφή για το υποδίκτυο 192.168.1.0 του PC1.
2.7 route add -net 192.168.1.0/24 192.168.2.1

2.8 arp -a -d
2.9 tcpdump -i em0 -vvv -e
tcpdump -i em1 -vvv -e
ping -c 1 192.168.2.3
2.10 Απαντάει με ARP reply δίνοντας τη δική του MAC της em0
2.11 Προς τη MAC em0 του R1
2.12 Από τη MAC em1 του R1
2.13 PC1→broadcast: ARP request
R1→PC1: ARP reply
PC1→R1: ICMP echo request
R1→broadcast: ARP request
PC3→R1: ARP reply
R1→PC3: ICMP echo request
PC3→R1: ICMP echo reply
R1→PC1: ARP request
PC1→R1: ARP reply
R1→PC1: ICMP reply
2.14 Για να συνεχίζει να επιτυγχάνει το ping θα πρέπει οι PC1,PC3 να ανήκουν στο ίδιο υποδίκτυο ώστε να υπάρχει επικοινωνία, θα πρέπει δηλαδή να έχουν κοινό αριθμό δικτύου. Για να συμβαίνει αυτό το μέγιστο μήκος προθέματος είναι 22.
2.15 ifconfig em0 inet 192.168.1.2/23
2.16 route add -net 192.168.2.0/24 -interface em0
2.17 link#1 (εμφανίζεται αντί της MAC της em0)
2.18 Ναι επιτυγχάνει διότι πλέον στον πίνακα δρομολόγησης του PC1 υπάρχει καταχωρημένη διαδρομή για το υποδίκτυο 192.168.2.0 του PC3 και ξέρει που πρέπει να προωθήσει τα πακέτα.(στον proxy ARP R1).
2.19 sysctl net.link.ether.inet.proxyall=0
2.20 route change -net 192.168.2.0/24 192.168.1.1
2.21 ifconfig em0 inet 192.168.1.2/24
2.22 Διαγράφηκε
2.23 route add -net 192.168.2.0/24 192.168.1.1
2.24 Αποσυνδέουμε το καλώδιο (αποεπιλέγουμε το Cable Connected)

Άσκηση 3

3.1 ifconfig em1 inet 172.17.17.1/30
sysrc ifconfig_em1="inet 172.17.17.1 netmask 255.255.255.252"
3.2 ifconfig em0 inet 172.17.17.2/30
sysrc ifconfig_em0="inet 172.17.17.2 netmask 255.255.255.252"
ifconfig em1 inet 192.168.2.1/24
sysrc ifconfig_em1="inet 192.168.2.1 netmask 255.255.255.0"
Για επανεκκίνηση των διεπαφών: service netif restart
3.3 sysrc gateway_enable=”YES”
service routing restart
3.4 Destination Host Unreachable
3.5 tcpdump -i em0 στο R1 για την καταγραφή της κίνησης στο LAN1.

Παρατηρούμε ότι παράγονται ICMP echo request από τον PC1 και ICMP host unreachable από τον R1.
tcpdump -i em1 στο R1 για την καταγραφή της κίνησης στο WAN1.
Παρατηρούμε ότι δεν καταγράφεται καμία κίνηση. Αυτό συμβαίνει γιατί ο R1 λαμβάνει τα ICMP echo requests του PC1 αλλά δεν έχει καμία σχετική με τον PC2 εγγραφή στον πίνακα δρομολόγησης του οπότε δεν ξέρει που να προωθήσει τα πακέτα και επιστρέφει τα παραπάνω μηνύματα ICMP host unreachable που παρατηρούνται στο LAN1.

3.6 Λαμβάνουμε !H που όπως βλέπουμε από man traceroute σημαίνει Host Unreachable.

3.7 route add -net 192.168.2.0/24 172.17.17.2

3.8 Όχι δεν λαμβάνουμε απάντηση.

3.9 Με tcpdump -i em1 καταγράφουμε την κίνηση στο LAN2
Παρατηρούμε ότι παράγονται τα εξής μηνύματα:
ICMP echo request που στέλνονται από τον PC1 και προωθούνται από τον R2 στον PC2. Ο PC2 παράγει και στέλνει ICMP echo reply αλλά ο R2 δεν έχει σχετική εγγραφή ώστε να τα προωθήσει στον PC1 και έτσι επιστρέφει στον PC2 ICMP host unreachable.

3.10 Καταγράφονται μόνο πακέτα UDP τα οποία η traceroute στέλνει by default στο FreeBSD.

3.11 Παράγονται ICMP udp port unreachable

3.12 Γιατί απαγορεύεται η αποστολή ICMP error message ως απάντηση σε άλλο ICMP error message (στην περίπτωση μας ICMP udp port unreachable) προκειμένου να αποφευχθεί η υπερβολική αχρείαστη κίνηση και τα loop στο σύστημα.

3.13 route add -net 192.168.1.0/24 172.17.17.1

3.14 Ναι μπορούμε. Παράγονται ICMP time exceeded in-transit(το TTL μηδενίζεται στη διεπαφή 172.17.17.2) και ICMP udp port unreachable.

3.15 Λαμβάνουμε μήνυμα no route to host.

3.16 route del 192.168.1.0/24

3.17 route add default 192.168.2.1

3.18 Το ping είναι τώρα επιτυχές.

3.19 Στην πρώτη περίπτωση το ping δεν ήταν επιτυχές διότι δεν υπήρχε σχετική εγγραφή στον πίνακα δρομολόγησης και ο PC2 δεν ήξερε που να στείλει το πακέτο. Αντίθετα στην δεύτερη περίπτωση έχει οριστεί πλέον ως προκαθορισμένη πύλη ο R2 στην οποία ο PC2 στέλνει το πακέτο και στη συνέχεια ο R2 προωθεί το πακέτο στον R1 στη διεπαφή του στο WAN1.

Άσκηση 4

4.1 ifconfig em0 inet 192.168.2.3/24
route add -net 192.168.1.0/24 192.168.2.1

4.2 ifconfig em2 inet 172.17.17.5/30
sysrc ifconfig_em2="inet 172.17.17.5 netmask 255.255.255.252"
Για επανεκκίνηση των διεπαφών: service netif restart

4.3 ifconfig em2 inet 172.17.17.9/30
sysrc ifconfig_em2="inet 172.17.17.9 netmask 255.255.255.252"

Για επανεκκίνηση των διεπαφών: service netif restart

4.4 ifconfig em0 inet 172.17.17.6/30
sysrc ifconfig_em0="inet 172.17.17.6 netmask 255.255.255.252"
ifconfig em1 inet 172.17.17.10/30
sysrc ifconfig_em1="inet 172.17.17.10 netmask 255.255.255.252"
Για επανεκκίνηση των διεπαφών: service netif restart

4.5 sysrc gateway_enable=”YES”
service routing restart

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 H.

4.10 3 βήματα

4.11 ttl=62 άρα 2 βήματα

4.12 4 βήματα

4.13 ttl=62 άρα 2 βήματα

4.14 Με tcpdump σε όλα τα υποδίκτυα για να καταγράψουμε όλη τη σχετική κίνηση παρατηρούμε ότι το ICMP echo request ακολουθεί την εξής διαδρομή: PC1→R1→R3→R2→PC3
Έχουμε ορίσει στον R1 στατική εγγραφή για το PC3 μέσω του R3.

4.15 Το ICMP echo reply ακολουθεί την εξής διαδρομή: PC3→R2→R1→PC1
Έχουμε ορίσει στον R2 στατική εγγραφή για το υποδίκτυο 192.168.1.0/24 του PC1 μέσω του R1.

4.16 tcpdump -i em1

4.17 Όχι δεν παρατηρούμε

4.18 Παρατηρούμε ότι φτάνει ένα πακέτο UDP στον PC3. Παράγονται από αυτόν ICMP udp port unreachable και για αυτό και δεν ολοκληρώνεται και το traceroute.

4.19 Ναι είναι επιτυχές

4.20 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
Το traceroute από το PC1 στο PC3 ολοκληρώνεται επιτυχώς.

4.21 route show 192.168.2.2
route show 192.168.2.3
Ο PC2 έχει έξτρα το πεδίο mask και ως destination την διεύθυνση του υποδικτύου 192.168.2.0 ενώ ο PC3 την δική του διεύθυνση 192.168.2.3. Επιπλέον ο PC3 έχει flag HOST.

4.22 Η εγγραφή για την διεύθυνση του PC3. Δηλαδή η 192.168.2.3→172.17.17.6

4.23 route change -net 192.168.2.0/24 172.17.17.5

4.24 Όχι δεν είναι επιτυχές

4.25 Εμφανίζεται μήνυμα λάθους Time to live exceeded από τη διεπαφή 172.17.17.6 στο WAN2. Αυτό συμβαίνει γιατί έχει δημιουργηθεί ένας βρόχος μεταξύ του R1 και του R3 και στέλνουν συνεχώς το πακέτο ο ένας στον άλλο μέχρι τελικά να μηδενιστεί το TTL.

4.26 tcpdump -i em0 -vvv -e ‘icmp[icmptype] == icmp-echo’

4.27 Εμφανίστηκαν 63

4.28 32 από τον R1 και 31 από τον R2

Παράγουν πακέτα εναλλάξ αλλά αφού το ping ξεκινάει από το PC1 και άρα πρώτο το R1 στέλνει ICMP παράγει τελικά 1 παραπάνω.

4.29 R1: tcpdump -i em2 -vvv -e 'icmp[icmptype] == icmp-echo'
R3: tcpdump -i em0 -vvv -e 'icmp[icmptype] == icmp-timxceed'

4.30 64 βήματα που πηγαίνουν ως εξής 192.168.1.1→172.17.17.6

4.31 Στάλθηκαν 2016 ICMP echo requests διότι 0+1+2+3+...+63=2016

4.32 Λήφθηκαν 32 πακέτα ICMP Time exceeded στο WAN2. Όπως και πριν τα μισά(32) θα παραχθούν από τον R3 και ανιχνεύονται στο WAN2 και τα άλλα μισά από τον R1 και δεν καταγράφονται στο WAN2.

Άσκηση 5

5.1 172.17.17.0/25

5.2 172.17.17. 192/26

5.3 172.17.17. 160/27

5.4 ifconfig em1 inet 172.17.17.129/30
sysrc ifconfig_em1="inet 172.17.17.129 netmask 255.255.255.252"
ifconfig em2 inet 172.17.17.133/30
sysrc ifconfig_em2="inet 172.17.17.133 netmask 255.255.255.252"

5.5 PC1: ifconfig em0 inet 172.17.17.1/25
R1: ifconfig em0 inet 172.17.17.126/25
sysrc ifconfig_em0="inet 172.17.17.126 netmask 255.255.255.128"

5.6 ifconfig em0 inet 172.17.17.130/30
sysrc ifconfig_em0="inet 172.17.17.130 netmask 255.255.255.252"
ifconfig em2 inet 172.17.17.138/30
sysrc ifconfig_em2="inet 172.17.17.138 netmask 255.255.255.252"

5.7 PC2: ifconfig em0 inet 172.17.17.253/26
PC3: ifconfig em0 inet 172.17.17.254/26
R2: ifconfig em1 inet 172.17.17.193/26
sysrc ifconfig_em1="inet 172.17.17.193 netmask 255.255.255.192"

5.8 ifconfig em0 inet 172.17.17.134/30
sysrc ifconfig_em0="inet 172.17.17.134 netmask 255.255.255.252"
ifconfig em1 inet 172.17.17.137/30
sysrc ifconfig_em1="inet 172.17.17.137 netmask 255.255.255.252"

5.9 PC4: ifconfig em0 inet 172.17.17.161/27
R3: ifconfig em2 inet 172.17.17.190/27
sysrc ifconfig_em2="inet 172.17.17.190 netmask 255.255.255.224"

5.10 PC1: route add default 172.17.17.126
PC2: route add default 172.17.17.193
PC3: route add default 172.17.17.193
PC4: route add default 172.17.17.190

5.11 R1:
LAN2: route add -net 172.17.17.192/26 172.17.17.130
LAN3: route add -net 172.17.17.160/27 172.17.17.130

5.12 R2:

LAN1: route add -net 172.17.17.0/25 172.17.17.137
LAN3: route add -net 172.17.17.160/27 172.17.17.137

5.13 R3:
LAN1: route add -net 172.17.17.0/25 172.17.17.133
LAN2: route add -net 172.17.17.192/26 172.17.17.133

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

Όλα τα ping έιναι επιτυχή.

Άσκηση 6

6.1 PC2: 08:00:27:00:1e:46
PC3: 08:00:27:9f:9c:87

6.2 ifconfig em0 inet 172.17.17.254/26

6.3 Λαμβάνουμε την εξής ένδειξη λάθους στο PC2: Mar 19 12.59.53 PC kernel: arp: 08:00:27:9f:9c:87 is using my IP address 172.17.17.254 on em0!

6.4 Στο PC3 εμφανίζεται αντίστοιχη ένδειξη λάθους: Mar 19 12:59:53 PC kernel: arp: 08:00:27:00:1e:46 is using my IP address 172.17.17.254 on em0!

6.5 Ναι, έχει οριστεί. Τα μηνύματα λάθους λειτουργούν ως προειδοποίηση.

6.6 Όχι λόγω της αλλαγής IP διαγράφεται η εγγραφή για τον R2 ως προεπιλεγμένη πύλη στο PC2.

6.7 route add default 172.17.17.193

6.8 PC2,PC3,R2: arp -a -d

6.9 tcpdump -i em1 -n arp

6.10 tcpdump -n tcp

6.11 ssh lab@172.17.17.254
Εμφανίζεται μήνυμα Connection reset by peer

6.12 Ναι είναι επιτυχής

6.13 172.17.17.254 at 08:00:27:00:1e:46

6.14 Πρώτος απάντησε ο PC3

6.15 Στο PC2 που απάντησε δεύτερο

6.16 Συνδεθήκαμε στο PC2

6.17 Με ifconfig και βλέποντας την MAC

6.18 Ο PC3 απαντά πρώτος στο ARP request και λαμβάνει έτσι το πρώτο πακέτο της τριπλής χειραψίας (SYN). Έπειτα ο PC3 στέλνει στον PC1 το δεύτερο πακέτο της τριπλής χειραψίας (SYN,ACK). Όταν ο PC1 στέλνει το τρίτο πακέτο της τριπλής χειραψίας έχει απαντήσει και ο PC2 στο ARP request και έχει καταχωρηθεί πλέον η δική του MAC στη διεύθυνση 172.17.17.254 κι έτσι λαμβάνει αυτός το τρίτο πακέτο της χειραψίας (ACK) αλλά καθώς δεν έλαβε το πρώτο και συνεπώς δεν γνωρίζει κάτι για την σύνδεση, την κάνει reset και το SHH αποτυγχάνει. Τη δεύτερη φορά ο PC2 λαμβάνει τόσο το πρώτο όσο και το τρίτο πακέτο της τριπλής χειραψίας και στέλνει το δεύτερο κι έτσι η σύνδεση είναι επιτυχής.

6.19 Τα στέλνει για να τερματιστεί η πρώτη ανεπιτυχής προσπάθεια σύνδεσης την οποία κάνει reset ο PC2(που τη δεύτερη φορά συνδέεται με επιτυχία όπως αναφέρθηκε παραπάνω).