LAB-05 (Static Routing)

Ονοματεπώνυμο : Νίκος Μπέλλος (el18183)	Όνομα PC : BELLOS-DELL-G3
Ομάδα : 3	Ημερομηνία : 12/04/2022

Άσκηση 1: Δρομολόγηση σε ένα βήμα

1. `ifconfig em0 inet 192.168.X.Y`
2. `sysrc gateway_enable="YES"`
3. `route add -net 192.168.2.0/24 192.168.1.1`
4. U → route is up
   G → destination is gateway
   S → route is statically set
5. Το PC1 στέλνει επιτυχώς ICMP requests αλλά δεν λαμάνει ICMP replies
6. Ο PC1 ξέρει που να προωθήσει τα πακέτα για το PC2, αλλά ο PC2 δεν έχει στο πίνακα προώθησης κάποια εγγραφή που να του υποδικνύει που να στείλει τα ICMP replies
7. `route add -net 192.168.1.0/24 192.168.2.1`
8. Ναι, υπάρχει
9. Γιατί είναι ενεργοποιημένη η προώθηση πακέτων και προστείθενται αυτόματα τα υποδίκτυα στα οποία ανήκουν οι διεπαφές του R1

Άσκηση 2: Proxy ARP

1. `route del 192.168.2.0/24`
2. `ifconfig em0 inet 192.168.1.2/20`
3. Στο ίδιο
4. Όχι, δεν είναι
5. Ναι, είναι επιτυχές γιατί πλέον ο R1 ακούει στο arp request του PC1 προς τα PC2, PC3 και αντί να τα αγνοήσει και να τα προωθήσει, απαντάει εκείνος με τη δική του MAC, καθώς έχει εγγραφές για το υποδίκτυο 192.168.2.0/24 στο πίνακα προώθησης
6. Γιατι στο PC3 δεν έχουμε προσθέσει στο πίνακα προώθησης την εγγραφή για το 192.168.1.0/24
7. `route add -net 192.168.1.0/24 192.168.2.1`
8. `arp -d -a`
9. `tcpdump -vvv -e -X`
10. Απαντάει με τη δική του MAC
11. Προς τη MAC του R1
12. Από τη MAC του R1 στο em1 (LAN2)
13. PC1 → broadcast : arp request
    R1 → PC1 : arp reply
    PC1 → R1 : icmp request
    R1 → broadcast : arp request
    PC3 → R1 : arp reply

R1 → PC3 : icmp request
PC3 → R1 : icmp reply
R1 → PC1 : arp request
PC1 → R1 : arp reply
R1 → PC1 : icmp reply

14. max prefix length : 22.
    Διότι, οι διευθύνσεις 192.168.2.X των PC2, PC3 θα πρέπει να βρίσκονται στο ίδιο υποδίκτυο με το PC1. Στη 3η οκτάδα της IP επομένως θα πρέπει να μπορεί να παρθεί η τιμή 2 (10 HEX) άρα συνολικά θα πρέπει να διατείθενται 10 bits για τις διευθύνσεις host
15. `ifconfig em0 inet 192.168.1.2/23`
16. `route add -net 192.168.2.0/24 -interface em0`
17. Η MAC της διεπαφής του PC1 στο LAN1
18. Όχι, δεν είναι, γιατί όταν στέλνει το πακέτο στη διεπαφή em0 θα πρέπει το PC3 να ανήκει στο ίδιο υποδίκτυο με το PC1, το οποίο δεν ισχύει με πρόθεμα 23
19. `sysctl net.link.ether.inet.proxyall=0`
20. `route add -net 192.168.2.0/24 192.168.1.1`
21. `ifconfig em0 inet 192.168.1.2/24`
22. Με την αλλαγή προθέματος, η διαδρομή χάθηκε

Άσκηση 3: Δρομολόγηση σε περισσότερα βήματα

1. `ifconfig em0 inet 192.168.1.1/24`, `ifonfig em1 inet 172.17.17.1/30`
2. `ifconfig em0 inet 172.17.17.2/30`, `ifconfig em1 inet 192.168.2.2/24`
3. Error : Destination Host Unreachable
4. Στο LAN1 παράγονται ICMP request από τον PC1 και ICMP replies απο τον R1 ότι ο PC2 δεν βρίσκει τον PC2. Στο WAN1 δεν παράγονται ποτέ πακέτα, γιατί ο R1 δεν τα προωθεί καθώς δεν ξέρει ότι για το υποδίκτυο 192.168.2.0/24 πρέπει να τα προωθήσει από τη θύρα em1
5. Το !H σημαίνει Host Unreachable
6. `route add -net 192.168.2.0/24 172.17.17.2`
7. Όχι, δεν μπορώ
8. ICMP request (από το PC1 → PC2)
   ICMP reply (από το PC2 → PC1)
   ICMP host unreachable (από το R2 → PC2)
9. Όχι, δεν παρατηρώ μηνύματα ICMP request, αλλά μονο UDP πακέτα. Για να μην μπλοκάρονται τα TCP μηνήματα από το firewall
10. Παράγονται ICMP 192.168.2.2 udp port unreachable (δοκιμάζει πολλές πόρτες)
11. Έχει απαγορευτεί η αποστολή πολλαπλών μηνυμάτων λάθους ICMP
12. `route add -net 192.168.1.0/24 172.17.17.1`
13. Ναι μπορώ, παράγονται τα μηνύματα
    ICMP time exceeded in-transit
    ICMP <PC2_addr> udp port unreachable
14. No route to host

15. `route del 192.168.1.0/24`
16. `route add default 192.168.2.1`
17. Το ping εκτελείται με επιτυχία
18. Λόγω το default gateway στο πίνακα δρομολόγησης του PC2 τη δεύτερη φορά θα στείλει σωστά το ping στο R2 ο οποίος με τη σειρά του θα το προωθήσει στο R1

Άσκηση 4: Ένα πιο πολύπλοκο δίκτυο με εναλλακτικές διαδρομές

1. `ifconfig em0 up`, `ifconfig em0 192.168.2.3/24`
2. `route add -net 192.168.1.0/24 192.168.2.1`
3. Στα δίκτυα LAN1, WAN1, WAN2 → ip addresses with `ifconfig emX <ip_addr>`
4. Στα δίκτυα LAN2, WAN1, WAN3 → ip addresses with `ifconfig emX <ip_addr>`
5. Στα δίκτυα WAN2, WAN3 → ip addresses with `ifconfig emX <ip_addr>`
6. `route add -net 192.168.2.0/24 172.17.17.2`
7. `route add -net 192.168.1.0/24 172.17.17.1`
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`
9. `route add -host 192.168.2.3 172.17.17.6`
10. 3 βήματα
11. 2 βήματα
12. 4 βήματα
13. 2 βήματα
14. Τη διαδρομή R1 → R3 → R2 → PC3
15. Τη διαδρομή R2 → R1 → PC1, διότι στο πίνακα δρομολόγησης του R2 τα πακέτα προς το LAN1 πάνε από τη διεπαφή στο WAN1
16. `tcpdump -i em1`
17. Οχι, δεν παράγονται
18. Ναι, παράγονται
19. `route change -net 192.168.2.0/24 172.17.17.6`,
    `route change -net 192.168.1.0/24 172.17.17.10`
20. Ότι στο PC2 ως destination είναι η διεύθυνση του υποδικτύου, ενώ στο PC3 η ίδια η διεύθυνση
21. Η εγγραφή που έχει ολόκληρη τη διεύθυνση του PC3

Άσκηση 5: Βρόχοι κατά τη δρομολόγηση

1. `route change -net 192.168.2.0/24 172.17.17.5`
2. Όχι, δεν είναι
3. Από την 172.17.17.6
4. Στο WAN2
5. `tcpdump "icmp[0]==8"` → echo requests
6. Από το PC1 παράχθηκε ένα echo request ενώ στο WAN2 εμφανίστηκαν 64

7. `tcpdump -i emX -w "log"`
8. Εμφανίζονται 64 βήματα μεταξύ του R1 και του R3
9. `tcpdump -r log-lan1 | grep "ICMP echo request" | wc -l` → Καταγράφηκαν 64 πακέτα
10. Εμφανίζονται 2016 πακέτα ICMP echo request. Στο WAN2 θα φτάσουν συνολικά 64 πακέτα γιατί η traceroute παράγει πακέτα με ttl = 1 - 64. Το μικρότερο ttl θα είναι 0 στο WAN2, ενώ το μεγαλύτερο 63 και αυτά τα πακέτα θα ανταλάσονται συνέχεια μέχρι να μηδενιστεί το TTL. Άρα το πλήθος τους να ισούται με αριθμητική πρόοδο από το 0 - 63 = 63 * 64 / 2 = 2016
11. 32 πακέτα → Επειδή η καταγραφή γίνεται στο R3 καταγράφονται μόνο τα πακέτα που είχαν ttl = 0 όταν έφτασαν στον R3 τα οποία θα είναι τα μισά από αυτα που παράχθηκαν και πιο συγκεκριμένα αυτά που είχαν ζυγό ttl όταν παράχθηκαν από το PC1
12. Βάζουμε ειδικό φίλτρο για να καταγράφει μόνο ICMP packets και προσθέτουμε το -c στο tcpdump
13. Η διαφορά τους είναι στο TTL
14. Γιατί το TTL σε κάθε επαναμετάδωση μειώνεται κατά 1 μέχρι να μηδενιστεί

Άσκηση 6: Χωρισμός σε υποδίκτυα

1. LAN1 : 172.17.17.0/25
2. LAN2 : 172.17.17.192/26
3. LAN3 : 172.17.17.160/27
4. PC1 : 172.17.17.1/25
   R1 (em0) : 172.17.17.126/25
5. PC4 : 172.17.17.161/27
   R3 (em2) : 172.17.17.190/27
6. R2 (em1) : 172.17.17.193/26
   PC2 : 172.17.17.253/26
   PC3 : 172.17.17.254/26
7. PC1 → `route add default 172.17.17.126`
   PC2 → `route add default 172.17.17.190`
   PC3 → `route add default 172.17.17.190`
   PC4 → `route add default 172.17.17.193`
8. R1 →
   `route add -net 172.17.17.192/26 172.17.17.130`
   `route add -net 172.17.17.160/27 172.17.17.130`
9. R2 →
   `route add -net 172.17.17.0/25 172.17.17.137`
   `route add -net 172.17.17.160/27 172.17.17.137`
10. R3 →
    `route add -net 172.17.17.0/25 172.17.17.133`
    `route add -net 172.17.17.192/26 172.17.17.133`
11. Τα ping είναι επιτυχή

Άσκηση 7: Ταυτόσημες διευθύνσεις IP

1. PC2 : 08:00:27:fd:48:d7
   PC3 : 08:00:27:be:32:1b

2. IPv4 PC2 : 172.17.17.190/26
3. Ναι έλαβα ένδειξη ότι το PC3 έχει την ίδια IP στο δίκτυο
4. Ναι, εμφανίστηκε
5. Ναι, έχει ορισθεί. Το νόημα είναι για την ειδοποίηση και την αντιμετώπιση του προβλήματος. Δεν απαγορεύεται να έχουν δύο συσκευές την ίδια IP, απλά αυτο είναι πιθανό να προκαλέσει προβλήματα
6. Όχι, έχει διαγραφεί λόγω της αλλαγής της IP
7. `route add default 172.17.17.193`
8. `arp -d -a`
9. `tcpdump -i em1 arp`
10. `tcpdump tcp`
11. `ssh lab@172.17.17.254` → Υπήρχε μόνο authenticity warning
12. Η προσπάθεια ήταν επιτυχής
13. (172.17.17.254) at 08:00:27:be:32:1b
14. Πρώτος απάντησε ο PC2
15. Η MAC είναι του PC3
16. Συνδεθήκμε στο PC3
17. Από την εντολή who στο μηχάνημα PC3
18. Τη πρώτη φορά η εγγραφή του R2 για τον PC2 ήταν λανθασμένη και έτσι πήρε αυτός το ένα πακέτο της τριπλής χειραψίας, έτσι ο PC3 εκανε reset τη σύνδεση.