Ονοματεπώνυμο: Βασιλάκος Μιχαήλ
Ομάδα: 2
Όνομα PC: laptop
Ημερομηνία: 8/6/22

Άσκηση 1

1.1 tcpdump -i em0 -envvv
1.2 dhclient em0
1.3

PC1		NS1
DHCP Discover	->	
	<-	ICMP Echo request
	<-	DHCP Offer
DHCP Request	->	
	<-	DHCP ACK
ARP Request (192.168.2.5)	->	
	<-	ICMP Echo request
ARP Request (192.168.2.1)	->	
	<-	ARP Reply
ICMP Echo reply	->	
DHCP Request	->	
	<-	DHCP ACK
ICMP (Port Unreachable)	->	

1.4 DHCP Discover
DHCP Offer
DHCP Request
DHCP ACK
1.5 η διεύθυνση που αποδόθηκε στο PC1 είναι 192.168.2.5
η διεύθυνση του εξυπηρετητή DHCP είναι 192.168.2.1
1.6 η ανανέωση πρέπει να γίνει μετά από 60 δευτερόλεπτα
1.7 το πρωτόκολλο μεταφοράς που χρησιμοποιείται είναι το UDP
1.8 η θύρα του εξυπηρετητή είναι η 67 ενώ του πελάτη είναι η 68
1.9

DHCP Discover:	αποστολέας 0.0.0.0	παραλήπτης 255.255.255.255
DHCP Offer:	αποστολέας 192.168.2.1	παραλήπτης 192.168.2.5
DHCP Request:	αποστολέας 0.0.0.0	παραλήπτης 255.255.255.255
DHCP ACK:	αποστολέας 192.168.2.1	παραλήπτης 192.168.2.5

1.10

	MAC πηγής	MAC προορισμού
DHCP Discover:	08:00:27:85:b5:75	ff:ff:ff:ff:ff:ff
DHCP Offer:	08:00:27:c2:36:e4	08:00:27:85:b5:75
DHCP Request:	08:00:27:85:b5:75	ff:ff:ff:ff:ff:ff
DHCP ACK:	08:00:27:c2:36:e4	08:00:27:85:b5:75

1.11 ως διεύθυνση πηγής χρησιμοποιεί τη διεύθυνση 0.0.0.0 (ακαθόριστη)
1.12 παρατηρήσαμε πλαίσιο ARP που χρησιμοποιείται ως gratuitous ARP από το PC1 αφού λάβει τη διεύθυνση IP από τον εξυπηρετητή DHCP ώστε να ενημερώσει τους άλλους hosts στο δίκτυο για τη νέα του διεύθυνση
επιπλεόν παρατηρήσαμε μηνύματα ARP από το PC1 ώστε να βρεί τη MAC του NS1 και να στείλει το DHCP Request για την ανανέωση της IP του, αφού αυτό το μήνυμα έχει ως διεύθυνση προορισμού τη διεύθυνση του εξυπηρετητή
1.13 παρατηρήθηκε ένα μήνυμα ICMP Echo request από τον εξυπηρετητή DHCP προς τη διεύθυνση που προσέφερε αργότερα στο PC1

το μήνυμα αυτό στέλνεται ώστε να εντοπιστούν τυχόν hosts που χρησιμοποιούν τη διεύθυνση που έχει σκοπό ο εξυπηρετητής να προσφέρει

1.14 πρόκειται για gratuitous ARP με το οποίο ενημερώνει τους hosts που βρίσκονται στο ίδιο δίκτυο με εκείνον για τη διεύθυνση που του αποδόθηκε και να προστεθούν οι κατάλληλες εγγραφές στους πίνακες ARP

1.15 παρατηρήθηκε ανταλλαγή πακέτων ICMP αμέσως μετά την απόδοση της διεύθυνσης
αυτό ίσως γίνεται για να αναγκαστεί να μάθει το PC1 μέσω ARP τη MAC του NS1

1.16 η εκχώρηση της διεύθυνσης διαρκεί για 120 δευτερόλεπτα

1.17 στο μήνυμα DHCP Request περιέχεται επιπλεόν η πληροφορία για το Server-ID

1.18 το δεύτερο μήνυμα δεν είναι broadcast αλλά είναι unicast προς τον DHCP Server από τον οποίο το PC1 δανείστηκε τη διεύθυνσή του
οι διευθύνσεις IP και MAC πηγής τώρα έχουν τις αντίστοιχες διευθύνσεις του PC1, ενώ οι διευθύνσεις IP και MAC προορισμού τις διευθύνσεις του NS1
από τα options έχουν διαγραφεί οι τιμές για το server-id και το requested-id, καθώς τώρα περιέχονται στην επικεφαλίδα

1.19 ?

1.20 τα δάνεια αποθηκεύονται στο αρχείο /var/db/dhcpd/dhcpd.leases

1.21 οι εγγραφές γίνονται κάθε 60 δευτερόλεπτα

1.22 οι πληροφορίες που περιέχονται στην κάθε εγγραφή είναι η χρονική στιγμή της ανάθεσης της διεύθυνσης, η χρονική στιγμή της λήξης της, τη χρονική στιγμή της τελευταίας συναλλαγής με τον πελάτη (cltt), το binding state (active), το next binding state (free), το rewind binding state (free), τη MAC του πελάτη, το uid και το hostname του πελάτη

1.23 /var/db/dhclient.leases.em0

1.24 περιέχει τη διεπαφή, τη διεύθυνση IP που του αποδόθηκε, το μήκος προθέματος, τον προεπιλεγμένο δρομολογητή, τη διεύθυνση broadcast, το χρόνο του lease, τον τύπο του τελευταίου μηνύματος που έλαβε, το id του dhcp server και τις χρονικές στιγμές για την ανανέωση του lease, για το rebind και για τη λήξη της εγγραφής

1.25 45 δευτερόλεπτα

1.26 ο πελάτης ζήτησε 10 παραμέτρους από τον εξυπηρετητή

1.27 ο εξυπηρετητής προσδιορίζει τις παραμέτρους *Subnet-Mask, BR* και *Default-Gateway*

1.28 tcpdump -i em0 -envvv

1.29 service isc-dhcpd stop

1.30 ifconfig em0
service isc-dhcpd start

1.31 ifconfig em0
αποδόθηκε πάλι διεύθυνση στο PC1

1.32 ο πελάτης στέλνει 5 μηνύματα DHCP request με το διάστημα ανάμεσά τους να μεγαλώνει από τα 3 στα 5, μετά στα 10 και από εκεί στα 20 δευτερόλεπτα

1.33 η απάντηση που στέλνει ο NS1 είναι ICMP udp port 67 unreachable, το οποίο σημαίνει πως η υπηρεσία που ακούει στη θύρα 67 (DHCP server) δεν είναι διαθέσιμη

1.34 ο προορισμός του τελευταίου DHCP Request είναι η διεύθυνση εκπομπής 255.255.255.255

1.35 μετά τη λήξη του χρόνου επανασύνδεσης το PC1 θεωρεί πως ο εξυπηρετητής δεν λειτουργεί πλέον και προσπαθεί να ανανεώσει τη διεύθυνση IP που του έχει αποδοθεί μέσω άλλου διαθέσιμου εξυπηρετητή DHCP

1.36 η διεύθυνση προορισμού IPv4 των DHCP Discover είναι η διεύθυνση broadcast 255.255.255.255, ενώ η αντίστοιχη MAC είναι η διεύθυνση broadcast ff:ff:ff:ff:ff:ff

το πεδίο που φανερώνει πως το PC1 έχασε τη διεύθυνση IPv4 που του είχε αποδοθεί είναι η διεύθυνση IPv4 πηγής, η οποία είναι η απροσδιόριστη διεύθυνση 0.0.0.0

1.37 ο λόγος που παράγεται το ICMP Echo request προς τη διεύθυνση IP που προσφέρει ο εξυπηρετητής στον πελάτη είναι για να βεβαιωθεί ο εξυπηρετητής πως η διεύθυνση αυτή δεν είναι σε χρήση από κάποιον άλλο host

1.38 το αρχείο με τα δάνεια παύει να καταγράφει τα leases του μέχρι να πάρει το επόμενο DHCP ACK οπότε και συνεχίζει να ανανεώνει το αρχείο

1.39 το DHCP χρησιμοποιεί το stateless πρωτόκολλο στρώματος μεταφοράς UDP, οπότε το φιλτράρισμα της κίνησης μέσω ενός firewall σε περίπτωση που χρησιμοποιούσαμε τυχαία θύρα για τον πελάτη θα ήταν πολύ πιο περίπλοκη για τον διαχειριστή του δικτύου

Άσκηση 2

2.1 ::1 localhost localhost.ntua.lab
127.0.0.1 localhost localhost.ntua.lab
192.168.2.5 PC1.ntua.lab PC1
192.168.2.6 PC2.ntua.lab PC2

2.2 ping PC2 -> απάντηση από το 192.168.2.6 (PC2)
ping pc2 -> απάντηση από το 192.168.2.6 (PC2)
ping pc2.NTUA.LAB -> απάντηση από το 192.168.2.6 (PC2)
δεν έχει σημασία η χρήση πεζών ή κεφαλαίων γραμμάτων

2.3 ping PC1
το ping είναι επιτυχές

2.4 *cannot resolve PC1: Host name lookup failure*

2.5 local-data: "PC1.ntua.lab. IN A 192.168.2.5"
local-data: "PC2.ntua.lab. IN A 192.168.2.6"

2.6 local-data-ptr: "192.168.2.5 PC1.ntua.lab."
local-data-ptr: "192.168.2.6 PC2.ntua.lab."

2.7 unbound-checkconf /var/tmp/unbound.conf
cp /var/tmp/unbound.conf /usr/local/etc/unbound/unbound.conf
service unbound restart

2.8 tcpdump -i em0 -nvvv

2.9 ifconfig em0 192.168.2.5/28 delete
dhclient em0

2.10 το PC1 έλαβε τη διεύθυνση 192.168.2.5

2.11 ο εξυπηρετητής αυτή τη φορά έδωσε επιπλέον πληροφορίες για το Domain-Name και τον Domain-Name-Server

2.12 δημιουργήθηκε /etc/resolv.conf στο PC1 και περιέχει τις πληροφορίες του προηγούμενου ερωτήματος

2.13 host 192.168.2.5
το όνομα που αντιστοιχεί είναι PC1.ntua.lab.

2.14 host ns1
η διεύθυνση του ns1 είναι 192.168.2.1

2.15 ping ns1
ναι

2.16 ifconfig em0 192.168.2.6/28
dhclient em0

2.17 192.168.2.6

2.18 ping pc1

ναι

2.19 το PC2 έλαβε τη διεύθυνση του PC1 από τον εξυπηρετητή DNS, αφού έχουμε διαγράψει την αντίστοιχη εγγραφή από το /etc/hosts

2.20 192.168.2.7 PC2.ntua.lab PC2
ping pc2
το ping αποτυγχάνει

2.21 εφόσον η εγγραφή βρίσκεται στον DNS και είναι σωστή και διαθέσιμη και το PC1 αποτυγχάνει στο ping μπορούμε να συμπεράνουμε πως πρώτα γίνεται αναζήτηση στο αρχείο /etc/hosts και αν δεν βρεθεί η απάντηση εκεί τότε γίνεται αναζήτηση στον DNS server

2.22 cat /etc/nsswitch.conf
hosts: files dns
τα αρχεία του τοπικού συστήματος βρίσκονται σε μεγαλύτερη προτεραιότητα από τον DNS server, οπότε η σειρά αναζήτησης συμφωνεί με αυτή που παρατηρήσαμε από το ping

2.23 host pc2
192.168.2.6

2.24 η εντολή host εκτελεί DNS lookup, οπότε παρακάμπτει το λανθασμένο αρχείο /etc/hosts

2.25 rm /etc/resolv.conf
resolvconf -u
cat /etc/resolv.conf
το περιεχόμενο του αρχείου είναι ίδιο με πριν

2.26 tcpdump -i em0 -nvvv '(not (port 67 or port 68))'

2.27 host ntua.lab.

2.28 ναι

2.29 το πρωτόκολλο μεταφοράς που χρησιμοποιείται στο DNS είναι UDP

2.30 η θύρα του εξυπηρετητή είναι πάντα η 53, ενώ του πελάτη στην καταγραφή ήταν διαφορετική σε κάθε μήνυμα που αντάλλασε με τον εξυπηρετητή, αφού χρησιμοποίηση τις θύρες 13814, 43202 και 29711

2.31 η θύρα DNS είναι η 53

2.32 tcpdump -i em0 -nvv port 53

2.33 host ns1

2.34 ανταλλάχθηκαν συνολικά 6 μηνύματα

2.35 τα μηνύματα αντιστοιχούν σε ερωτήματα Address Mapping record (A), IPv6 Address record (AAAA) και Mail exchanger record (MX) για το όνομα ns1.ntua.lab.

2.36 όλα τα ερωτήματα DNS έλαβαν απάντηση

2.37 drill ns1
drill ns1.ntua.lab

2.38 στην πρώτη περίπτωση έγινε αναζήτηση για το όνομα ns1. και έλαβε απάντηση Authority Section με τον αρμόδιο DNS server
στη δεύτερη έγινε αναζήτηση για το ns1.ntua.lab. και έλαβε απάντηση 192.168.2.1

2.39 στην εντολή drill η χρήση του επιθέματος είναι απαραίτητη για τη σωστή λειτουργία, ενώ στην εντολή host δεν είναι αναγκαία η χρήση του

2.40 δεν παράγονται ερωτήματα DNS σε καμία από τις δύο περιπτώσεις

2.41 ping ns1

2.42 παράχθηκαν 2 μηνύματα DNS, ένα DNS query για Address Mapping record και ένα DNS response στο ερώτημα αυτό

2.43 παράγεται ένα ζεύγος DNS query - DNS response για κάθε εκτέλεση της εντολής ping

2.44 προφανώς η απάντηση του DNS αποθηκεύεται στο PC1 για όσο χρειαστεί η εκτέλεση της εκάστοτε εντολής και με την ολοκλήρωσή της η εγγραφή διαγράφεται αμέσως

Άσκηση 3

3.1 vi /etc/rc.conf
hostname="SRV.ntua.lab"
lighttpd_enable="YES"
3.2 mkdir /usr/local/www/data
3.3 vi /usr/local/www/data/index.html
3.4 reboot
3.5 service lighttpd status
3.6 netstat -na -f inet
η θύρα που ακούει ο εξυπηρετητής HTTP είναι η 80, η οποία βλέπουμε πως είναι στην κατάσταση listening
3.7 ifconfig em0 192.168.2.3/28
3.8 vi /var/tmp/unbound.conf
local-data: "SRV.ntua.lab. IN A 192.168.2.3"
3.9 local-data-ptr: "192.168.2.3 SRV.ntua.lab."
3.10 unbound-checkconf /var/tmp/unbound.conf
cp /var/tmp/unbound.conf /usr/local/etc/unbound/unbound.conf
reboot
3.11 tcpdump -nvv
3.12 fetch http://srv.ntua.lab
3.13 χρησιμοποιήθηκε το πρωτόκολλο μεταφοράς TCP
ο εξυπηρετητής HTTP ακούει στη θύρα 80
3.14 το περιεχόμενο της σελίδας αποθηκεύτηκε στο αρχείο /root/srv.ntua.lab

Άσκηση 4

4.1 sysrc gateway_enable="YES"
4.2 sysrc firewall_enable="YES"
4.3 sysrc firewall_type="open"
4.4 sysrc firewall_nat_enable="YES"
4.5 sysrc ifconfig_em2="inet 192.168.2.17 netmask 255.255.255.240"
4.6 cat /etc/rc.conf
4.7 netstat -rn -f inet
4.8 search ntua.lab
nameserver 192.168.2.1
4.9 sysrc ifconfig_em0="DHCP"
4.10 sysrc ifconfig_em0="inet 192.168.2.4 netmask 255.255.255.240"
sysrc defaultrouter="192.168.2.1"
4.11 service netif restart
service routing restart
4.12 sysrc ifconfig_em0="inet 192.168.2.18 netmask 255.255.255.240"
sysrc defaultrouter="192.168.2.17"
service netif restart
service routing restart
4.13 έγινε

4.14 ping 192.168.2.5
το ping στα μηχανήματα του LAN1 είναι επιτυχές
4.15 ipfw add 2000 deny all from any to 192.168.2.0/28 recv em2
4.16 ping 192.168.2.5
αυτή τη φορά το ping αποτυγχάνει
4.17 ipfw add 1900 allow all from 192.168.2.0/28 to 192.168.2.16/28 via em0 keep-state
4.18 ping srv
το ping είναι επιτυχές
4.19 ναι
4.20 οχι
4.21 ipfw nat 111 config unreg_only if em1 reset
4.22 ipfw add 3000 nat 111 ip from any to any via em1
4.23 ναι
4.24 host 147.102.1.1
το όνομα του host είναι theseas.softlab.ece.ntua.gr.
4.25 tcpdump -i em1 -nv
4.26 10.0.3.15
4.27 147.102.224.101
4.28 9.9.9.9
4.29 tcpdump -i em1 -nv 'port 53'
4.30 παρατηρούμε πως δεν απευθύνονται όλα τα μηνύματα στον ίδιο εξυπηρετητή DNS και μάλιστα αρκετοί από αυτούς μας παραπέμπουν σε άλλους εξυπηρετητές
4.31 tcpdump -i em0 -nv 'port 53'
4.32 courses.cn.ece.ntua.gr.
4.33 το PC1 έκανε DNS query για εγγραφή τύπου A στον NS1 και έλαβε DNS response για εγγραφή τύπου A και CNAME
το NS1 έκανε DNS query για εγγραφή τύπου A και έλαβε εγγραφές τύπου CNAME και A
4.34 tcpdump -i em1 -nvvv 'port 53'
4.35 drill www.cn.ece.ntua.gr
παρατηρούμε ένα μόνο ερώτημα DNS στην καταγραφή
η χρονική διάρκεια ισχύος των απαντήσεων DNS είναι 20 λεπτά (1200 sec)
4.36 tcpdump -i em0 -nvvv 'port 53'
αυτή τη φορά παρατηρούμε πως γίνεται DNS query σε κάθε εκτέλεση της εντολής και ο NS1 απαντά κάθε φορά, όμως η χρονική διάρκεια της εγγραφής δεν ανανεώνεται αλλά συνεχίζει να μειώνεται καθώς πρόκειται για cached τιμή
4.37 συμπεραίνουμε πως ο NS1 αποθηκεύει προσωρινά (cache) τις απαντήσεις που λαμβάνει και λειτουργεί αυτόνομα, χωρίς να χρειάζεται να επαναλαμβάνει την ερώτησή του μέχρι τη λήξη του χρόνου εγκυρότητας της εγγραφής
4.38 ping -c 1 147.102.224.101
ναι
4.39 ping -c 1 www.ntua.gr
όχι, διότι δεν έχει οριστεί εξυπηρετητής DNS ώστε να μάθει την αντίστοιχη IP
4.40 vi /etc/resolv.conf
search ntua.lab
nameserver 192.168.2.17
4.41 ναι
4.42 host www.ntua.lab
η απάντηση που λαμβάνουμε είναι πως το πρόκειται για alias του ntua.lab.
ping www.ntua.lab
cannot resolve www.ntua.lab: Unknown server error
δεν αντιστοιχεί κάποια διεύθυνση IP ώστε να γίνει ping

4.43 local-data: "www.ntua.lab. IN A 192.168.2.18"
service unbound restart
4.44 απαντά το μηχάνημα με IP 192.168.2.18, ή αλλιώς ο SRV

Άσκηση 5

5.1 sysrc hostname="ns2.ntua.lab"
5.2 sysrc ifconfig_em0="inet 192.0.2.1 netmask 255.255.255.248"
sysrc ifconfig_em2="inet 192.0.2.9 netmask 255.255.255.248"
5.3 sysrc ifconfig_em1="DHCP"
5.4 sysrc gateway_enable="YES"
5.5 sysrc firewall_enable="YES"
5.6 sysrc firewall_type="open"
5.7 sysrc firewall_nat_enable="YES"
5.8 deleted: dhcpd_enable="YES"
dhcpd_ifaces="em0"
5.9 unbound_enable="YES"
5.10 unbound-checkconf /var/tmp/unbound.conf
cp /var/tmp/unbound.conf /usr/local/etc/unbound/unbound.conf
5.11 reboot
5.12 ipfw nat 222 config if em1 reset same_ports
5.13 ipfw add 1100 nat 222 ip from any to any via em1
5.14 ifconfig_em0="inet 192.0.2.2 netmask 255.255.255.248"
defaultrouter="192.0.2.1"
5.15 service netif restart
service routing restart
host www.google.com
5.16 ping www.ntua.gr
επιτυγχάνει
5.17 ifconfig_em1="inet 192.0.2.10 netmask 255.255.255.248"
defaultrouter="192.0.2.9"
5.18 service netif restart
service routing restart
5.19 ping www.ntua.gr
επιτυγχάνει
5.20 ipfw show
η λειτουργία του nat 111 παραμένει, αφού ο μετρητής του αντίστοιχου κανόνα αυξάνεται
5.21 fetch http://www.ntua.lab
η λειτουργία αποτυγχάνει με το μήνυμα *Connection refused*
5.22 ipfw nat 111 config unreg_only if em1 reset redirect_port tcp 192.168.2.18:80 80
5.23 ναι
5.24 ping www.ntua.lab
η απάντηση έρχεται από τον host με IP 192.0.2.10, ή αλλιώς τον NS1
5.25 ssh lab@www.ntua.lab
συνδεόμαστε στον SRV
5.26 η σύνδεση από τον PC2 γίνεται στον ns1, καθώς η διεύθυνση που επιστρέφει ο DNS του για το www.ntua.lab είναι η διεύθυνση του ns1 και δεν έχουμε φροντίσει να ανακατευθύνουμε μέσω του firewall την κίνηση ssh στον SRV
5.27 ipfw nat 111 config unreg_only if em1 reset redirect_port tcp 192.168.2.18:80 80
redirect_port tcp 192.168.2.18:22 22

5.28 επαναλαμβάνοντας τη σύνδεση αυτή τη φορά συνδεόμαστε στον SRV, όπως μπορούμε να επιβεβαιώσουμε με την εντολή hostname ή ακόμα και κάνοντας ping προς το PC1, αφού η κίνηση αυτή επιτρέπεται για τον NS1 και όχι για τον SRV