

**Ονοματεπώνυμο:** Βασιλάκος Μιχαήλ  
**Ομάδα:** 2  
**Όνομα PC:** laptop  
**Ημερομηνία:** 1/6/22

## Άσκηση 1

- 1.1 `echo 'ifconfig_em0_ipv6="inet6 accept_rtadv"' >> /etc/rc.conf`
- 1.2 `service netif restart`
- 1.3 `fe80::a00:27ff:fe6c:4b9f`
- 1.4 `fe80::a00:27ff:fee9:5091`
- 1.5 οι διευθύνσεις είναι link-local  
ο τρόπος που παράγονται είναι με το πρόθεμα `fe80::/64` και την τροποποιημένη EUI-64 όπως αυτή παράγεται από τη MAC της διεπαφής
- 1.6 `netstat -rn -f inet6`  
εμφανίζονται 9 εγγραφές
- 1.7 μόνο 1 από τις παραπάνω εγγραφές αφορά τη διεπαφή `em0`
- 1.8 ο πίνακας περιέχει 5 εγγραφές σχετικές με το πρόθεμα δικτύου `fe80::/64`
- 1.9 `ping6 ::1`  
απαντά το PC1 καθώς πρόκειται για τη διεύθυνση loopback
- 1.10 `ping6 fe80::a00:27ff:fe6c:4b9f%em0`  
για να είναι επιτυχές το ping είναι απαραίτητη η προσθήκη του συμβόλου "%" μαζί με το όνομα της διεπαφής στο τέλος της διεύθυνσης
- 1.11 `ping6 fe80::a00:27ff:fee9:5091%em0`  
όπως και πριν είναι απαραίτητο το `%em0` στο τέλος της διεύθυνσης
- 1.12 τα μηνύματα `echo reply` προέρχονται από τη διεύθυνση `fe80::a00:27ff:fe6c:4b9f%em0`, άρα από το PC1
- 1.13 λαμβάνουμε 2 απαντήσεις στα ping μας, μία από το PC1 και μία από το PC2
- 1.14 `ifconfig em0 inet6 add fd00:1::2/64`
- 1.15 `ifconfig em0 inet6 add fd00:1::3/64`
- 1.16 πρόκειται για ψευδοτυχαίες μοναδικές τοπικές διευθύνσεις όμοιες των 192.168.0.0/16, 172.16.0.0/12 και 10.0.0.0/8
- 1.17 οι διεπαφές `em0` έχουν τώρα 2 διευθύνσεις, τη link-local και τις τοπικές που ορίσαμε προηγουμένως
- 1.18 εμφανίζονται 11 εγγραφές, οπότε προστέθηκαν 2 εγγραφές
- 1.19 `echo ip_address hostname >> /etc/hosts`
- 1.20 `ping PC2`  
ναι
- 1.21 `arp -a`  
δεν εμφανίζεται καμία εγγραφή στον πίνακα arp
- 1.22 `man ndp`
- 1.23 `ndp -a`
- 1.24 εμφανίζονται 4 εγγραφές
- 1.25 `ndp -p`  
η διάρκεια των εγγραφών είναι άπειρη (`expire=Never`)  
τα προθέματα που μπορούν να χρησιμοποιηθούν από το SLAAC είναι τα `fe80::%em0` και `fe80::%lo0`
- 1.26 `tcpdump -nnvv`
- 1.27 `ndp -c`

- 1.28 στην καταγραφή παρατηρούνται 4 πακέτα IPv6
- 1.29 τα πακέτα IPv6 μεταφέρουν μηνύματα του πρωτοκόλλου ICMP  
η τιμή του next-header είναι ICMPv6
- 1.30 PC1 PC2
- IP6 (ICMP6 neighbor solicitation) ----->  
 <----- IP6 (neighbor advertisement)  
 IP6 (ICMP6 echo request) ----->  
 <----- IP6 (ICMP6 echo reply)
- 1.31 η διεύθυνση προορισμού του neighbor solicitation είναι μηνύματος είναι ff02::1:ff00:3, η οποία είναι και η multicast διεύθυνση που προκύπτει από τη διεύθυνσή του fd00::1::3 προσθέτοντας σε αυτή το πρόθεμα ff02:0:0:0:1:ff00:0/104
- 1.32 η διεύθυνση προορισμού του δεύτερου πακέτου της καταγραφής (neighbor advertisement) είναι fd00:1::2, η οποία είναι και η unicast διεύθυνση του αποστολέα του πρώτου πακέτου
- 1.33 η κατάσταση της εγγραφής για το PC1 έχει το σύμβολο 'S', το οποίο και σημαίνει 'Stale'  
η διάρκεια ζωής της εγγραφής είναι 23 ώρες 46 λεπτά και 25 δευτερόλεπτα
- 1.34 ping6 PC2  
η κατάσταση της εγγραφής ξεκινά από Reachable (R), μετά από 30 περίπου δευτερόλεπτα μεταβαίνει σε Stale (S) και σχεδόν αμέσως επιστρέφει σε Reachable
- 1.35 η διάρκεια της κατάστασης Reachable είναι λίγο πάνω από 30 δευτερόλεπτα (παρατηρήσαμε τιμή 31) και μετά την πάροδο του χρονικού αυτού διαστήματος η κατάσταση γίνεται Stale
- 1.36 η διάρκεια της κατάστασης Stale είναι περίπου μία μέρα (24h59m59s)
- 1.37 μετά τη διακοπή του ping η κατάσταση της εγγραφής για το PC1 μεταβαίνει από Reachable σε Stale
- 1.38 tcpdump -n  
παρατηρούμε πως πέρα από τα ICMP echo μηνύματα εμφανίζονται και μηνύματα ICMP neighbor solicitation και ICMP neighbor advertisement από το PC1 στο PC2 αλλά και αντίστροφα  
τα μηνύματα αυτά στέλνονται κάθε περίπου 35 δευτερόλεπτα, κάθε φορά δηλαδή που η κατάσταση της εκάστοτε εγγραφής παύει να είναι Reachable

## Άσκηση 2

- 2.1 echo 'ipv6\_gateway\_enable="YES"' >> /etc/rc.conf  
service routing restart
- 2.2 ifconfig em0 inet6 fd00:1::3/64 delete  
ifconfig em0 inet6 add fd00:2::2/64
- 2.3 interface em0 -> ip address fd00:1::1/64
- 2.4 interface em1 -> ip address fd00:3::1/126
- 2.5 interface em0 -> ip address fd00:2::1/64
- 2.6 interface em1 -> ip address fd00:3::2/126
- 2.7 route add -net -6 ::/0 fd00:1::1
- 2.8 route add -net -6 ::/0 fd00:2::1
- 2.9 tcpdump -i em0
- 2.10 ndp -c  
ping6 -c 1 PC2

το ping δεν είναι επιτυχές  
αυτό συμβαίνει διότι το PC1 στέλνει πακέτα neighbor solicitation ώστε να μάθει τη διεύθυνση του PC2, όμως ο R1 τα παραλαμβάνει και δεν τα προωθεί στο δίκτυο WAN1 καθώς δεν γνωρίζει πως εκεί βρίσκεται το δίκτυο LAN2

- 2.11 τα μηνύματα που παρατηρούνται στην καταγραφή είναι μηνύματα τύπου ICMP6 neighbor solicitation με διεύθυνση προορισμού ff02::1:ff00:3 η οποία όπως αναφέραμε και παραπάνω είναι η διεύθυνση multicast που προκύπτει από τη διεύθυνση του PC2
- 2.12 ipv6 route fd00:2::/64 fd00:3::2
- 2.13 το ping αποτυγχάνει ξανά, όμως αυτή τη φορά μεταφέρεται το μήνυμα neighbor solicitation μέχρι το LAN2 από όπου όμως ο R2 δεν έχει διαδρομή για το PC1 και για αυτό δεν μεταφέρεται η απάντηση neighbor advertisement ώστε να συνεχίσει το ping
- 2.14 ipv6 route fd00:1::/64 fd00:3::1
- 2.15 ναι
- 2.16 interface em0 -> no ipv6 nd suppress-ra
- 2.17 ipv6 nd prefix fd00:1::/64
- 2.18 interface em0 -> no ipv6 nd suppress-ra
- 2.19 ipv6 nd prefix fd00:2::/64
- 2.20 route delete -net -6 ::/0
- 2.21 tcpdump -i em0 -ne icmp6
- 2.22 service netif restart
- 2.23 αρχικά αποστέλλεται μήνυμα neighbor solicitation από το PC1 για τη διεύθυνση IPv6 multicast που προκύπτει από τη τροποποιημένη EUI-64 ως link-local address στη συνέχεια αποστέλλεται router solicitation από το PC1 προς τη διεύθυνση multicast ff02::2 (all routers)  
έπειτα αποστέλλεται router advertisement από R1 στη διεύθυνση multicast ff02::1 (all hosts)  
τέλος αποστέλλεται neighbor solicitation για τη νέα παγκόσμια διεύθυνση IPv6 που δημιούργησε με το κατάλληλο πρόθεμα δικτύου που έλαβε από το δρομολογητή
- 2.24 παράγονται 2 μηνύματα NS, το πρώτο είναι για να επιβεβαιωθεί η μοναδικότητα της link-local διεύθυνσης του PC1 μέσω DAD, ενώ το δεύτερο είναι για την επιβεβαίωση της μοναδικότητας της νέας παγκόσμιας διεύθυνσης IPv6 όπως αυτή προκύπτει προσθέτωντας το πρόθεμα δικτύου που έλαβε από τον δρομολογητή στη link-local IPv6
- 2.25 η διεύθυνση πηγής που χρησιμοποιείται στα NS μηνύματα είναι η ακαθόριστη διεύθυνση ::0 καθώς το PC1 δεν έχει λάβει ακόμα διεύθυνση IPv6
- 2.26 η διεύθυνση πηγής στο RS μήνυμα είναι η link-local διεύθυνσή του PC1 για την οποία έκανε το πρώτο NS
- 2.27 διεύθυνση προορισμού για τα NS είναι η διεύθυνση την οποία προσπαθεί να αποκτήσει το PC1 ώστε να ελέγξει αν την έχει ήδη στην κατοχή της κάποιο άλλο μηχάνημα  
για το RS διεύθυνση είναι η ff02::2 που είναι διεύθυνση multicast για όλους τους δρομολογητές στη τοπική ζεύξη  
για το RA διεύθυνση προορισμού είναι η ff02::1 που είναι διεύθυνση multicast για όλους τους κόμβους στη τοπική ζεύξη
- 2.28 οι διευθύνσεις MAC προορισμού των μηνυμάτων είναι διευθύνσεις multicast με κατάληξη ίδια με τη διεύθυνση IPv6 προορισμού τους
- 2.29 ndp -p

παρατηρούμε πως έχουμε τα ίδια προθέματα, όμως αυτό για το δίκτυο LAN1 λήγει σε 30 μέρες, σε αντίθεση με πριν που ήταν απεριόριστης διάρκειας

- 2.30 `ifconfig`  
οι διευθύνσεις που έλαβε αυτόματα το PC1 είναι οι link-local και global unicast διευθύνσεις
- 2.31 `netstat -rn -f inet6`  
στον πίνακα δρομολόγησης του PC1 υπάρχει προκαθορισμένη διαδρομή, όπου η προκαθορισμένη πύλη προέκυψε από τη διεύθυνση IPv6 πηγής του μηνύματος RA από τον R1 μπορούμε να κάνουμε ping και στις δύο διευθύνσεις της διεπαφής του PC1 στο LAN1, ενώ από το PC2 μπορούμε να κάνουμε ping μόνο στη global unicast διεύθυνσή της αφού η link-local διεύθυνση είναι διαθέσιμη μόνο για μηχανήματα που έχουν πρόσβαση στην ίδια διεπαφή
- 2.32

### Άσκηση 3

- 3.1 `no ipv6 route fd00:2::/64 fd00:3::2`  
`no ipv6 route fd00:1::/64 fd00:3::1`
- 3.2 `router ripng`  
`network em0`  
`network em1`
- 3.3 `show ipv6 router ripng`  
παρατηρούμε μία μόνο εγγραφή για το δίκτυο LAN2
- 3.4 η διεύθυνση του επόμενου κόμβου είναι η fe80::a00:27ff:fe91:6f3c, η οποία είναι διεύθυνση link-local για τον R2
- 3.5 `ping6 PC2`  
ναι
- 3.6 `tcpdump -i em1 -nnvv`
- 3.7 στην καταγραφή εμφανίζονται πακέτα ripng-resp με προορισμό τη διεύθυνση ff02::9, η οποία είναι η διεύθυνση multicast που ορίζει την ομάδα 'all RIP routers'
- 3.8 η τιμή του hop limit των πακέτων είναι 255 ώστε να μη διέρχεται από δρομολογητές
- 3.9 το RIPng χρησιμοποιεί το πρωτόκολλο στρώματος μεταφοράς UDP και τη θύρα 521, ενώ το RIP χρησιμοποιεί το ίδιο πρωτόκολλο και τη θύρα 520
- 3.10 `no network em0`  
`no network em1`
- 3.11 `write memory`
- 3.12 `service frr restart`
- 3.13 `router ospf6`  
`ospf6 router-id x.x.x.x`
- 3.14 `interface em0 area 0.0.0.0`  
`interface em1 area 0.0.0.0`
- 3.15 `interface em0 area 0.0.0.0`  
`interface em1 area 0.0.0.0`
- 3.16 `show ipv6 route ospf6`  
εμφανίζονται 3 εγγραφές, με το κόστος για τα δίκτυα LAN2 και WAN1 να είναι 100 και το κόστος για το δίκτυο LAN1 να είναι 200  
το κόστος προκύπτει ως το bandwidth της εκάστοτε διεπαφής προς το bandwidth αναφοράς, οπότε το κόστος προς το δίκτυο LAN1 είναι διπλάσιο του κόστους προς τα άλλα δίκτυα αφού περνά από μία διεπαφή περισσότερη

- 3.17 η διεύθυνση του επόμενου κόμβου για το δίκτυο fd00:1::/64 είναι η fe80::a00:27ff:fe2a:eaee, η οποία είναι η link-local διεύθυνση για τη διεπαφή του R1 στο WAN1
- 3.18 tcpdump -i em1 -nnv
- 3.19 στην καταγραφή εμφανίζονται πακέτα OSPFv3 τύπου Hello με διεύθυνση προορισμού την ff02::5, η οποία είναι διεύθυνση multicast για όλους τους δρομολογητές που υλοποιούν το πρωτόκολλο OSPF
- 3.20 το hop limit των πακέτων είναι IPv6 που τα ενθυλακώνουν είναι 1 ώστε να μεταφέρονται μονάχα στους δρομολογητές με τους οποίους υπάρχει άμεση σύνδεση
- 3.21 ο αριθμός πρωτοκόλλου του OSPFv3 είναι 89, ο ίδιος δηλαδή με εκείνον του OSPFv2
- 3.22 ping6 fe00:1::a00:27ff:fe6c:4b9f  
ναι
- 3.23 no interface em0 area 0.0.0.0  
no interface em1 area 0.0.0.0
- 3.24 service frr restart
- 3.25 router-id 1.1.1.1  
router bgp 65010
- 3.26 no bgp ebgp-requires-policy
- 3.27 no bgp default ipv4-unicast
- 3.28 neighbor fd00:3::2 remote-as 65020
- 3.29 address-family ipv6
- 3.30 network fd00:1::/64
- 3.31 neighbor fd00:3::2 activate
- 3.32 router-id 2.2.2.2  
router bgp 65020  
no bgp ebgp-requires-policy  
no bgp default ipv4-unicast  
neighbor fd00:3::1 remote-as 65010  
address-family ipv6  
network fd00:2::/64  
neighbor fd00:3::1 activate
- 3.33 show ipv6 route bgp  
στον πίνακα δρομολόγησης εμφανίζεται μία μόνο δυναμική εγγραφή για το δίκτυο LAN2
- 3.34 η διεύθυνση του επόμενου κόμβου είναι η fe80::a00:27ff:fe91:6f3c, η οποία είναι η link-local διεύθυνση του R2 στη ζεύξη του στο WAN1
- 3.35 tcpdump -i em1 -nnv
- 3.36 παρατηρούνται μηνύματα BGP keepalive  
το πρωτόκολλο μεταφοράς που χρησιμοποιείται είναι το TCP σε συνδυασμό με τη θύρα 179, όπως δηλαδή και τα αντίστοιχα για το IPv4
- 3.37 το hop limit έχει τιμή 1, καθώς γίνεται ανταλλαγή μηνυμάτων μόνο με δρομολογητές που είναι απευθείας συνδεδεμένοι
- 3.38 ping6 fd00:2::a00:27ff:fee9:5091  
ναι
- 3.39 vtysh  
interface em0  
ipv6 address fd00:1::2/64
- 3.40 router-id 1.1.0.0  
router bgp 65010

- 3.41 no bgp default ipv4-unicast
- 3.42 neighbor fd00:1::1 remote-as 65010
- 3.43 address-family ipv6  
neighbor fd00:1::1 activate
- 3.44 neighbor fd00:1::2 remote-as 65010
- 3.45 address-family ipv6  
neighbor fd00:1::2 activate  
neighbor fd00:1::2 next-hop-self
- 3.46 show bgp neighbors fd00:1::2
- 3.47 show ipv6 route bgp  
στον πίνακα δρομολόγησης εμφανίζονται 2 εγγραφές
- 3.48 η διαδρομή προς το δίκτυο fd00:1::/64 δεν είναι επιλεγμένη διότι προτιμάται η άμεση σύνδεση με το δίκτυο αφού έχει μικρότερη διαχειριστική απόσταση
- 3.49 η διεύθυνση του επόμενου κόμβου για το δίκτυο fd00:2::/64 είναι η fd00:1::1, η οποία είναι η διεύθυνση IPv6 του R1 στη διεπαφή LAN1 την οποία βλέπει ως γείτονα το PC1  
η διεύθυνση αυτή είναι ψευδοτυχαία μοναδική τοπική διεύθυνση
- 3.50 ping6 fd00:1::2  
ναι

#### Άσκηση 4

- 4.1 interface em0 -> ip address 192.168.1.1/24
- 4.2 interface em0 -> ip address 192.168.2.1/24
- 4.3 interface em0 -> ip address 192.168.1.2/24  
ip route 0.0.0.0/0 192.168.1.1
- 4.4 interface em0 -> ip address 192.168.2.2/24  
ip route 0.0.0.0/0 192.168.2.1
- 4.5 echo 'firewall\_enable="YES"' >> /etc/rc.conf  
echo 'firewall\_nat64\_enable="YES"' >> /etc/rc.conf  
echo 'firewall\_type="open"' >> /etc/rc.conf  
echo 'firewall\_logif="YES"' >> /etc/rc.conf
- 4.6 service ipfw start
- 4.7 ipfw show  
το τείχος προστασίας περιέχει 12 κανόνες
- 4.8 ping6 fd00:2::a00:27ff:fee9:5091  
το ping είναι επιτυχές
- 4.9 ipfw nat64clat nat64 create clat\_prefix fd00:3:1::/96 plat\_prefix 64:ff9b::/96  
allow\_private log
- 4.10 ipfw add 2000 nat64clat nat64 ip4 from any to not me recv em0
- 4.11 ipfw add 3000 nat64clat nat64 ip6 from 64:ff9b::/96 to fd00:3:1::/96 recv em1
- 4.12 ip6 route 64:ff9b::/96 fd00:3::2
- 4.13 vi /etc/rc.conf  
service ipfw start
- 4.14 ipfw nat64lsn nat64 create prefix4 2.2.2.0/24 prefix6 64:ff9b::/96 allow\_private log
- 4.15 ipfw add 2000 nat64lsn nat64 ip6 from fd00:3:1::/96 to 64:ff9b::/96 recv em1
- 4.16 ipfw add 3000 nat64lsn nat64 ip4 from any to 2.2.2.0/24 recv em0
- 4.17 ipv6 route fd00:3:1::/96 fd00:3::1
- 4.18 ip route 0.0.0.0/0 192.168.2.2
- 4.19 ping 192.168.1.1

- ping 192.168.2.2  
και τα δύο ping είναι επιτυχή
- 4.20 ifconfig ipfwlog0 create  
ifconfig ipfwlog0 up promisc  
tcpdump -i ipfwlog0
- 4.21 ifconfig ipfwlog0 create  
ifconfig ipfwlog0 up promisc  
tcpdump -i ipfwlog0
- 4.22 πρώτα παρατηρούμε το ICMP echo request πακέτο από τη διεύθυνση 129.168.1.2 στην 192.168.2.2 στην καταγραφή του R1  
στη συνέχεια στην ίδια καταγραφή βλέπουμε το μεταφρασμένο σε IPv6 ICMP6 echo request από το fd00:3:1::c0a8:102 στο 64:ff9b::c0a8:202  
το ίδιο πακέτο παρατηρείται και στην καταγραφή του R2  
έπειτα στην καταγραφή του R2 μεταφράζεται το ICMP6 σε ICMP από τη διεύθυνση 2.2.2.167 με προορισμό την 192.168.2.2  
στην ίδια καταγραφή έχουμε την απάντηση ICMP echo reply η οποία αντίστοιχα μεταφράζεται στις IPv6 διευθύνσεις που είδαμε παραπάνω  
το μήνυμα αυτό μεταφέρεται στον R1 και εμφανίζεται και σε αυτή την καταγραφή και εκεί μεταφράζεται σε διευθύνσεις IPv4, με διεύθυνση πηγής την 192.168.2.2 και προορισμού την 192.168.1.2
- 4.23 interface em0  
ip address 172.17.17.2/24  
ip address 10.0.0.2/24
- 4.24 το ping είναι επιτυχές και προς τις δύο διευθύνσεις
- 4.25 ipfw nat64ln nat64 show states  
στην κατάσταση του πίνακα εμφανίζονται 3 εγγραφές, μία για κάθε διεύθυνση IPv4 στην οποία κάναμε ping από το PC1
- 4.26 ping 10.0.0.2  
ping 172.17.17.2  
παρατηρούμε πως οι εγγραφές του nat64ln δεν ανανεώνονται αλλά προστίθενται νέες εγγραφές  
οι εγγραφές διαγράφονται από τον πίνακα μετά από περίπου 1 λεπτό

## Άσκηση 5

- 5.1 dhclient em0  
ping www.google.com  
τα μηχανήματα έχουν πρόσβαση στο Internet
- 5.2 pkg update  
pkg install miredo
- 5.3 echo 'miredo\_enable="YES"' >> /etc/rc.conf
- 5.4 service miredo start
- 5.5 ifconfig  
παρατηρούμε πως δημιουργήθηκε η διεπαφή *teredo* με διεύθυνση IPv6 2001:0:c38c:c38c:1413:7119:4dc4:1679
- 5.6 tcpdump -i em0 -n
- 5.7 η διεύθυνση του εξυπηρετητή Teredo είναι 195.140.195.140
- 5.8 χρησιμοποιείται το πρωτόκολλο μεταφοράς UDP και η θύρα 3544
- 5.9 τα μηνύματα που παρατηρούνται στην καταγραφή είναι πρωτοκόλλου IPv6
- 5.10 μπορούμε να κάνουμε ping6 στη διεύθυνση www.ibm.com
- 5.11 ping6 www.ibm.com

- 5.12 στην καταγραφή παρατηρούνται πακέτα IPv4 πρωτοκόλλου UDP
- 5.13 δεν παρατηρούνται μηνύματα τύπου ICMPv6 Echo request/reply στην καταγραφή
- 5.14 το πρωτόκολλο ανώτερου στρώματος που παρατηρείται στην καταγραφή στο PC1 είναι το UDP με τη θύρα που αντιστοιχεί στον αναμεταδότη teredo να είναι η 3545
- 5.15 tcpdump -i teredo -n
- 5.16 στην καταγραφή βλέπουμε πακέτα IPv6 που περιέχουν ICMP6 Echo request/reply μηνύματα
- 5.17 ping6 2001:0:c38c:c38c:18bf:5013:4dc4:1679  
το ping αποτυγχάνει
- 5.18 δεν παράγονται πακέτα στη διεπαφή teredo
- 5.19 tcpdump -i em0  
δεν παρατηρήθηκαν πακέτα ICMP6 στο προηγούμενο ερώτημα
- 5.20 ping6 -c 1 www.hp.com  
ping6 -c 1 www.f5.com  
για το πρώτο ping επιλέγεται ο teredo relay 185.218.193.138  
για το δεύτερο ο 216.66.86.178
- 5.21 παρατηρούμε πως ο teredo relay που επιλέχθηκε έχει την ίδια διεύθυνση IPv4 με τον teredo server