ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΛΟΠΟΝΝΗΣΟΥ

ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ

ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ:

Υλοποίηση πρακτικών IPv6

ΑΣΠΡΟΥΛΟΠΟΥΛΟΣ ΓΕΩΡΓΙΟΣ ΑΜ:1878

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ:ΒΑΣΙΛΗΣ ΤΡΙΑΝΤΑΦΥΛΟΥ

ΠΑΤΡΑ 2021

ΠΕΡΙΛΗΨΗ

Το διαδίκτυο είναι το μεγαλύτερο παγκόσμιο δίκτυο . Λόγω των ανησυχιών για την επικείμενη εξάντληση των διαθέσιμων IP διευθύνσεων του διαδικτύου και κάποιων προβλημάτων λειτουργικότητας στις νέες συσκευές , μπήκαμε από πολύ παλιά στο στάδιο μιας βελτιωμένης έκδοσης όπου εγκριθηκε το 1994. Αυτή η έκδοση ονομάστηκε IPv6 όπου επιλέει όλα τα λειτουργικά προβλήματα που έχουν ανακύψει από την χρήση του IPv4. Αυτή η πτυχιακή εργασία έχει σκοπό να συγκρίνει το IPv4 με το IPv6 και αναλύσει διεξοδικά τη λειτουργία του IPv6. Ακομα αποσαφηνίζονται οι τύπους διευθύνσεων: Unicast (μονοεκπομπή),Multicast (πολυεκπομπή).Anycast (επιλεκτική εκπομπή). Επίσης παρουσιάζει το πρωτόκολλο ανακαλύψεις γειτόνων (ICMPv6) που χρησιμοποιείται για την ανταλλαγή μηνυμάτων.
Επιπλέον περιέχει υποδικτύωση κι άλλες έννοιες που είναι χρήσιμες για να κατανοήσουμε τη δομή και τη συμπεριφορά του IPv6. Αυτό δεν επιτυγχάνεται μόνο σε θεωρητικό επίπεδο , αλλά θα χρησιμοποιήθει το πρόγραμμα Cisco packet Tracer που είναι ένα πρόγραμμα προσομοίωσης δικτύων, για να γινει κατανοητό πώς γίνεται υποδικτυωση σε ένα δίκτυο IPv4 και σε ένα IPv6.

ABSTRACT

The Internet is the largest global network. Due to concerns about the imminent depletion of available Internet IP addresses and some functionality issues on new devices, it has been long since will have entered the stage of an improved version which was approved in 1994. This version was named IPv6 which solves all operating problems that have arisen from the use of IPv4. This dissertation aims to compare IPv4 with IPv6 and thoroughly analyze the operation of IPv6.
Additionally the types of addresses such us Unicast (single broadcast), Multicast (multicast), Anycast (selective broadcast) are being clarified. Moreover, it presented the protocol (ICMPv6), which is used for exchanging messages.

It also contains subnetting and other concepts that are useful to understand the structure and behavior of IPv6. This will not only be achieved in theory, but also Cisco packet Tracer, a network simulation program, will be used to understand how subnetting is done on an IPv4 network and an IPv6 network.

Εισαγωγή

Η μεγαλη εξέλιξη της τεχνολογίας στον τομέα των ηλεκτρονικών συσκευων,δημιούργησε την ανάγκη αντικατάστασης του πρωτοκόλλου IPv4. Το 1980 πραγματοποιήθηκε η πρώτη έκδοση IPv4. Το 1985 άρχισε το διαδίκτυο να σπάει σε δίκτυα, ενω το 1990 ξεκινησε η προσπάθεια αντικαταστασης του IPv4. Το 1994 εγκριθηκε το IPv6 και ανακοινώθηκε απο το Internet Engineering Task Force (IETF) εναν χρόνο αργότερα.
Το νέο αυτό πρωτόκολλο δίνει λύση σε πολλά από τα προβλήματα του προκατόχου του, εκμεταλλεύεται σε μεγάλο βαθμό τις νέες εφαρμογές και γενικά προσφέρει μια άλλη δυναμική στο Internet και στις δικτυακές επικοινωνίες γενικότερα.

Ο κύριος λόγος δημιουργίας του IPv6 ηταν η διαφαινόμενη έλλειψη διευθύνσεων. Μόνο τα τελευταία 20 χρόνια, οι χρήσεις του υπολογίζεται περίπου στα 5 εκατομμύρια και η διάδοση του στο 63,2 του πληθυσμό της γη, οποίο σημειώνει αύξηση πού λογίζεται στο 1,271%.Ένας άλλος λόγος ηταν ότι έχει καλύτερες επιδόσεις ταχύτητες και στα σύγχρονα λειτουργικά συστήματα(Windows ,Mac)υποστηρίζουν μόνο το πρωτόκολλο IPv6 πλεον.Ακομα πολλές περιοχές υποστηρίζουν μόνο IPv6. Σε θέμα ασφάλειας το IPv4 χρησιμοποιεί ipsec 1 το ipv6 χρησιμοποιεί κρυπτογράφηση από άκρη σε άκρη και το ipsec είναι προαιρετικό.

Στο IPv4 καθε διεύθυνση αποτελείται από 32 bits.Τα 32 bits χωρίζονται σε 8x4 που καθένα bits έχει διαφορετική βαρύτητα.Μία διεύθυνση IPv6 αποτελείται από 128 bit ,οπου ταξινομούνται με βάση τις μεθόδους διευθυνσιοδότησης και δρομολόγησης που συνηθίζονται στα δίκτυα και γιαυτό χρησιμοποιούν διευθύνσεις unicast(μονοεκπομπή), διευθύνσεις multicast(πολυεκπομπή) και διευθύνσεις anycast (επιλεκτική εκπομπή).

Οι κύριες βραχυπρόθεσμες λύσεις στην επέκταση διευθύνσεων είναι η αταξική διατονική δρομολόγηση (CIDR) και η μεταφορά διευθύνσεων δυκτίου(NAT).Το CIDR γενικεύει την έννοια των διευθύνσεων των υποδικτύου τα 32 bit διευθύνσεων χωρίζεται πάλι σε δύο μέρη και έχουν τη μορφή a.b.c.d/x. Το NAT είναι η τεχνική IP μεταμφιέσης όπου ένα πλήρες διαστημά διευθύνσεων συνήθως ιδιωτικό βρίσκεται πίσω από μία μεμονωμένη IP σε ένα άλλο συνήθως δημόσιο τμήμα. Η συγκεκριμένη διεύθυνση αλλάζει σε μία απλή IP, το εξερχόμενο πακέτο και έτσι εμφανίζεται να προέρχεται, από τη συσκευή δρομολόγησης και όχι από την τερματική συσκευή. Επειδη NAT παραβιάζει την αρχική σχεδίαση του δικτύου γίνεται καθυστέρηση στη μετάβαση της στο IPv6.

Η βασική επικεφαλίδα του ipv6 συμπεριλαμβάνει την εκδοση, το μηκος επικεφαλίδες IP, την κλάση κυκλοφορίας, την ετικέτα ροής, το μήκος ωφέλιμου φορτίου, το πεδίο επομένης επικεφαλίδας, το όριο άλματος, την διεύθυνση πηγής και διεύθυνση προορισμού. Οι περισσότερο βασικές επικεφαλίδες υπάρχουν και στο IPv4 είναι πολύ μικρές διαφορές.

Μία σημαντική προσθήκη στο IPv6 είναι οι επικεφαλίδες επέκτασης οι οποίες είναι προαιρετικές και ακολουθούν την κυρία επικεφαλίδα του IPv6.Ανάλογα με τα νούμερα που έχουν δίπλα έχουν και διαφορετικό αποτέλεσμα. Η επικεφαλίδα επέκτασης *Επιλογές Hop-by-Hop* χρησιμοποιείται για να παρέχει προαιρετική πληροφορία.Η επικεφαλίδα επέκτασης Δρομολόγηση επιτρέπει στην πηγή του πακέτου να ορίσει την διαδρομή προς τον προορισμό. Η επικεφαλίδα επέκτασης Τεμάχιο χρησιμοποιείται όταν η πηγή του πακέτου IPv6 πρέπει να κατακερματισει το πακέτο σε τεμάχια και να στείλει κάθε τεμάχιο ως ξεχωριστό πακέτο.Οι επικεφαλίδα επέκτασης Ενσωματωμένα Δεδομένα Ασφάλειας και Αυθεντικοποίησης χρησιμοποιούνται για την εφαρμογή δύο βασικών πρωτοκόλλον ασφαλείας στην διανομή των πακέτων στα IP δίκτυα .Ακομα η Ενθυλακωμένη Ασφάλεια Payload (ESP)παρέχει αυθεντικοποίηση, ακεραιότητα και κρυπτογράφηση.

Υπάχουν 3 τύποι διευθύνσεων Unicast (μονοεκπομπή),Multicast (πολυεκπομπή),Anycast (επιλεκτική εκπομπή).Μία unicast διεύθυνση είναι η πιο κοινή μορφή διεύθυνσης και προσδιορίζει μοναδικά μια διεπαφή σε μία συσκευή που τρέχει το πρωτόκολλο IPv6.Η Multicast αφορά την τεχνική κατά την οποία μία συσκευή στέλνει ένα πακέτο προς πολλαπλούς προορισμούς ταυτόχρονα

ενω η anycast διεύθυνση είναι μια IPv6 διεύθυνση που μπορεί να εκχωρηθεί επιλεκτικά σε περισσότερες από μία διεπαφές.
Μία από τις μεγαλύτερες καινοτομίες είναι το πρωτόκολλο ανακάλυψης γειτόνων (ICMPv6),Που περιλαμβάνει μηνύματα δρομολογητη προς συσκευή και συσκευή προς συσκευη.
Όπως καταλαβαίνουμε το ipv6 δεν έχει μόνο διόρθωσει προβλήματα του ipv4, αλλά έχει καινοτομήσει ώστε να λυθούν προβλήματα που μπορεί να δημιουργηθούν στο μέλλον. Στη συγκεκριμένη πτυχιακή, αναλύονται εκτος απο θεωρητικά και συστήματα πάνω στο Cisco packet Tracer ώστε να μας βοηθήσουν να καταλάβουμε και στην πράξη πώς το διαδίκτυο μπορεί να βελτιωθεί με τη χρήση του IPv6.

Θα ήθελα να ευχαριστήσω ιδιαίτερα τον επιβλέποντα την πτυχιακή μου εργασίας, Καθηγητή κ. Βασίλης Τριανταφύλλου για την δυνατότητα που μου προσέφερε να ασχοληθώ με αυτό το ενδιαφέρον και σύγχρονο θέμα, όπως και για την πολύτιμη βοήθεια που μου παρείχε καθ' όλη την διάρκεια εκπόνησης της διπλωματικής

Περιεχόμενα

Κατάλογος Εικόνων

Κατάλογος Πινάκων

Ακρωνύμια

ARP	Address Resolution Protocol
CIDR	Classless Inter-Domain Routing
CPU	Central Processing Unit
DAD	Duplicate Address Detection
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
EUI	Extended Unique Identifier
IANA	Internet Assigned Numbers Authority
ICAAN	Internet Corporation for Assigned Names and Numbers
ICMP	Internet Control Message Protocol
IETF	Internet Engineering Task Force
IoT	Internet of Things
IP	Internet Protocol
IPsec	Internet Protocol Security
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISOC	Internet Society
ISP	Internet Service Provider

GUA Global Unicast Address

LLA Link Local Address

MTU Maximum Transmission Unit

NAT Network Address Translation

NDP Network Discovery Protocol

NUD Neighbor Unreachability Detection

RFC Request for Comments

RIR Regional Internet Registry

SLAAC StateLess Address AutoConfiguration

TCP Transmission Control Protocol

UDP User Datagram Protocol

ULA Unique Local Address

Λεξικό

anycast – επιλεκτική εκπομπή (?)

bandwidth - εύρος ζώνης

broadcast - ευρεία εκπομπή

datagram - αυτοδύναμο πακέτο

delay – καθυστέρηση

flag – σημαία/δυαδικός ενδείκτης

header – επικεφαλίδα

hop - άλμα

host - τερματική συσκευή

interface - διεπαφή

jitter - διακύμανση καθυστέρησης

label - ετικέτα

latency - καθυστέρηση μεταφοράς

link - σύνδεσμος

loopback - ανατροφοδότηση

mode – κατάσταση λειτουργίας

multicast - πολλαπλή εκπομπή ή πολυεκπομπή

padding – γέμισμα/παραγέμισμα

payload – ωφέλιμο φορτίο

plug-and-play – σύνδεση και άμεση λειτουργία

prefix - πρόθεμα

router – δρομολογητής

solicited-node – προσέγγιση κόμβου

stateful - με επίβλεψη κατάστασης, με καταστάσεις

stateless – χωρίς καταστάσεις

switch – μεταγωγέας

throughtput - ρυθμαπόδοση

unicast - μονοεκπομπή ή μοναδική εκπομπή

Κεφάλαιο 1: Η αναγκαιότητα μετάβασης στο IPv6

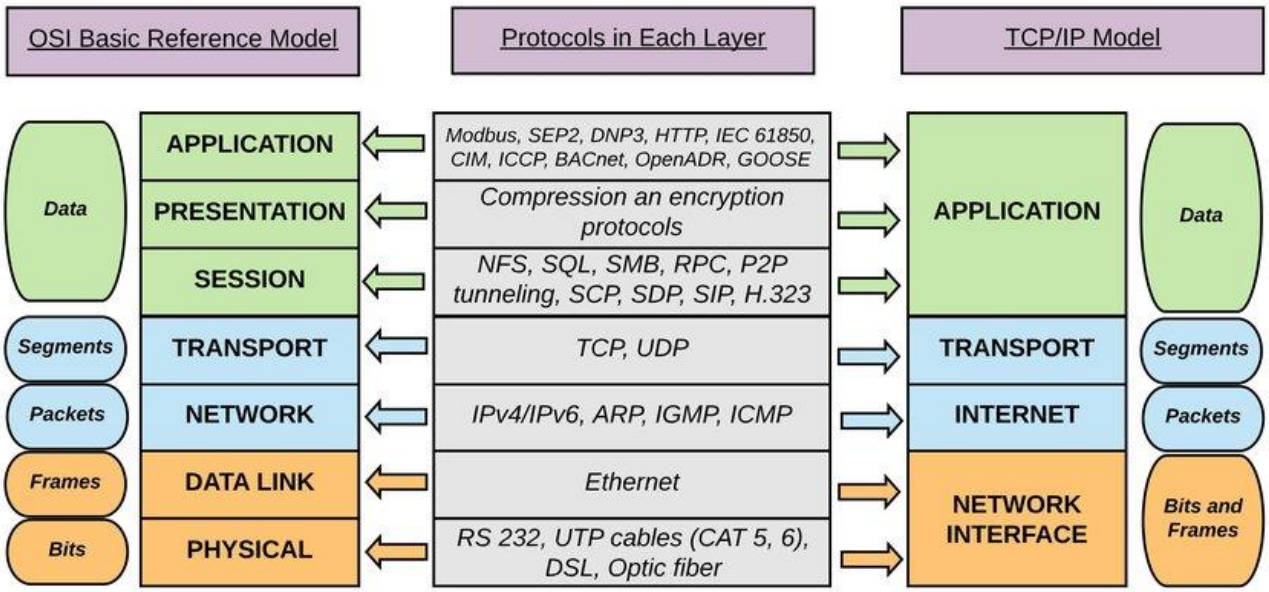
1.1 Το Διαδίκτυο και το Πρωτόκολλο Δικτύωσης

Το Διαδίκτυο (Internet) είναι το μεγαλύτερο παγκόσμιο δίκτυο που διασύνδεει εκατομμύρια υπολογιστικών συσκευών. Γενικότερα, ως διαδίκτυο ορίζεται το δίκτυο από δίκτυα. Την τελευταία δεκαετία οι διασυνδεμένες υπολογιστικές συσκευές του Διαδικτύου δεν είναι μόνο οι παραδοσιακοί υπολογιστές και οι εξυπηρετητές για την πρόσβαση σε ιστοσελίδες και την παροχή υπηρεσιών ηλεκτρονικού ταχυδρομείου. Είναι επιπλέον οι φορητοί υπολογιστές και τα κινητά έξυπνα κινητά τηλέφωνα, οι έξυπνες συσκευές που συνιστούν το Διαδίκτυο των Πραγμάτων (Internet of Things – IoT), όπως για παράδειγμα οι φορετές συσκευές (wearables), τηλεοράσεις, παιχνιδομηχανές κλπ. (Kurose *et al.*, 2017)

Κάθε μία από τις συνδεμένες συσκευές στο Διαδίκτυο ονομάζεται τερματικό σύστημα (end system) και στη γλώσσα του Διαδικτύου host. Οι τερματικές συσκευές που τρέχουν τις διαδικτυακές εφαρμογές συνδέονται με τηλεπικοινωνιακές ασύρματες ή ενσύρματες ζεύξεις μέσω μεταγωγέων-κόμβων για την αποστολή και λήψη πακέτων (packets), δηλαδή τμημάτων δεδομένων. Οι μεταγωγείς είναι συσκευές που αναλαμβάνουν την μεταγωγή των πακέτων επιλέγοντας κάθε φορά μία από τις διαθέσιμες γειτονικές συσκευές του δικτύου, δημιουργώντας έτσι μια διαδρομή για τη δρομολόγηση των πακέτων ανάμεσα στις τερματικές συσκευές, η οποία δεν είναι προκαθορισμένη, αλλά προσαρμόζεται δυναμικά. Οι κυριότεροι τύποι συσκευών μεταγωγής πακέτων του Διαδικτύου είναι οι δρομολογητές-routers και οι μεταγωγείς επιπέδου ζεύξης - link-layer switches (Kurose *et al.*, 2017) .

Οι τερματικές συσκευές έχουν πρόσβαση στο Διαδίκτυο μέσω των παρόχων υπηρεσιών Διαδικτύου (Internet Service Providers -ISPs). Ως ISPs θεωρούνται όσοι παρέχουν υπηρεσίες τηλεπικοινωνιακών ζεύξεων, όπως για παράδειγμα οι εταιρίες τηλεπικοινωνιών και τα μεγάλα πανεπιστήμια, και οι πάροχοι περιεχομένου ιστοσελίδων. Κάθε πάροχος διαθέτει το δικό του δίκτυο

μεταγωγέων πακέτων και τηλεπικοινωνιακών ζεύξεων και οι πάροχοι συνδέονται μεταξύ τους, σχηματίζοντας έτσι το παγκόσμιο δίκτυο των δικτύων (Kurose *et al.*, 2017). Η ανταλλαγή της πληροφορίας μεταξύ των συνιστωσών του Διαδικτύου, πραγματοποιείται μέσω προκαθορισμένων συνόλων κανόνων για την επικοινωνία, δηλαδή των πρωτόκολλων. Κάθε δραστηριότητα που πραγματοποιείται στο Διαδίκτυο στην οποία λαμβάνουν μέρος δύο ή περισσότερες συνιστώσες ορίζεται από ένα πρωτόκολλο. Το σύνολο των πρωτοκόλλων του Διαδικτύου είναι η στοίβα πρωτοκόλλων TCP/IP. Ονομάζεται έτσι διότι, το Πρωτόκολλο Δικτύωσης (Internet Protocol – IP) που αντιστοιχεί επίπεδο δικτύου του μοντέλου αναφοράς για τη στοίβα των πρωτοκόλλων δικτύων OSI (Open Systems Interconnection model) και το Πρωτόκολλο Ελέγχου Μετάδοσης (Transmission Control Protocol – TCP) που αντιστοιχεί στο μεταφοράς του OSI (Εικόνα 1), είναι τα γνωστότερα πρωτόκολλα της στοίβας (Kurose *et al.*, 2017). Το TCP/IP προτάθηκε αρχικά το 1974 από τους Kahn και Cerf γενικότερα ως πρωτόκολλο για δίκτυα μεταγωγής πακέτων (Cerf and Kahn, 1974). Υιοθετήθηκε αργότερα ως πρότυπο από το πρώτο δίκτυο μεταγωγής πακέτων ευρείας περιοχής με κατανεμημένο έλεγχο, το Advanced Research Projects Agency Network (ARPANET) του υπουργείου Άμυνας των ΗΠΑ, στο οποίο και εφαρμόστηκε για πρώτη φορά η στοίβα των πρωτόκολλων TCP/IP, πάνω στην οποία βασίζεται το σημερινό Διαδίκτυο (Wikipedia the free encyclopedia, 2021c). Στην επόμενη παράγραφο θα παρουσιάσουμε αναλυτικότερα το πρωτόκολλο IP που ανήκει στο επίπεδο του διαδικτύου (Internet layer).



Εικόνα 1. Η λογική αντιστοίχιση μεταξύ του μοντέλου αναφοράς OSI και της στοίβας πρωτοκόλλων TCP/IP.

Πηγή: https://www.researchgate.net/publication/327483011/figure/fig2/AS:668030367436802@1536282259885/The-logical-mapping-between-OSI-basic-reference-model-and-the-TCP-IP-stack.jpg

Με δεδομένη τη σημασία των πρωτόκολλων στο Διαδίκτυο, είναι πολύ σημαντικό να υπάρχει συμφωνία για το τι είναι κάθε πρωτόκολλο και το τί κάνει, έτσι ώστε να διασφαλίζεται η διαλειτουργικότητα μεταξύ των ετερογενών συστημάτων και προϊόντων και αυτό επιτυγχάνεται μέσω των προτύπων (standards). Τα πρότυπα του Διαδικτύου αναπτύσσονται από τον επιχειρησιακή ομάδα τεχνολογίας του Διαδικτύου, την Internet Engineering Task Force – IETF (*Internet Engineering Task Force*, 2021). Τα πρότυπα της IETF είναι έγγραφα, που ονομάζονται αιτήματα για σχόλια (Requests For Comments -RFCs), και είναι διαθέσιμα στη διεύθυνση https://www.rfc-editor.org/. Τα RFCs περιέχουν αναλυτικά τις προτάσεις για τις τεχνικές λεπτομέρειες για τη σχεδίαση των δικτύων και των πρωτόκολλων και υλοποιούνται ανάλογα με τη σπουδαιότητά τους και την αποδοχή τους (Kurose *et al.*, 2017).

1.1.1 Το Πρωτόκολλο Δικτύωσης (Internet Protocol - IP)

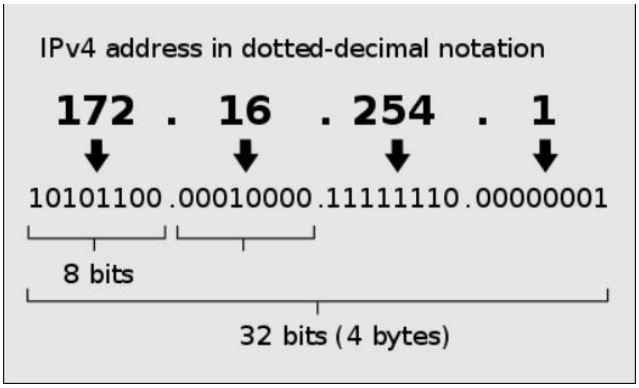
Τα πρωτόκολλα στο επίπεδο Διαδικτύου (Internet layer), το οποίο είναι το τρίτο επίπεδο του μοντέλου αναφοράς OSI και το δεύτερο του TCP/IP, περιγράφουν πως αποστέλλονται και λαμβάνονται τα δεδομένα. Το IP πρωτόκολλο δικτύου, είναι το κυριότερο εργαλείο για την ανάπτυξη ετερογενών δικτύων για τα οποία δεν θέλουμε να υπάρχουν περιορισμοί στο μέγεθός τους. Η κύρια λειτουργία του είναι η διανομή αυτοδύναμων πακέτων (datagrams) μεταξύ των τερματικών συσκευών του δικτύου. Χαρακτηρίζεται ως πρωτόκολλο χωρίς καταστάσεις (stateless)[1]. Επιπρόσθετα, το IP παρέχει τον κατακερματισμό και την επανασύνθεση των πακέτων στον τελικό προορισμό. Η παράδοση των πακέτων βασίζεται στην αρχή της «καλύτερης προσπάθειας» (best effort), πράγμα που σημαίνει ότι, τα πακέτα μπορεί να επαναληφθούν, να χαθούν ή να σπάσουν. Είναι ένα πρωτόκολλο χωρίς σύνδεση (connectionless), πράγμα που σημαίνει ότι, η παράδοση δεν είναι εγγυημένη. Τα προβλήματα που τυχόν δημιουργούνται κατά τη μεταφορά επιλύονται από άλλα πρωτόκολλα του δικτύου. Αυτό γιατί, η πρόθεση των σχεδιαστών του IP ήταν να κρατήσουν τους μεταγωγείς των πακέτων, δηλαδή τους δρομολογητές, όσο το δυνατόν πιο απλούς. Αυτή η απλότητα είναι ένα από τα βασικά πλεονεκτήματα του IP, γιατί του προσδίδει τη δυνατότητα λειτουργίας πάνω από οποιαδήποτε τεχνολογία δικτύωσης. Κάθε IP πακέτο αποτελείται από δύο τμήματα: την επικεφαλίδα (header) η οποία περιέχει όλη την απαιτούμενη πληροφορία για τον έλεγχο του πακέτου και τα δεδομένα (data/payload) του πακέτου (Kurose *et al.*, 2017).

Η πρώτη σημαντική έκδοση του IP είναι η τέταρτη έκδοση, το IPv4. Η πρώτη περιγραφή του IPv4 χρονολογείται το 1980 από RFC 760, το οποίο στη συνέχεια καταργήθηκε από το RFC 791 (Postel, 1981), όπου και προσδιορίζεται με ακρίβεια. Δεν θα αναφέρουμε τις λεπτομέρειες για τα πακέτα του IPv4, αλλά προς το παρόν θα αναφέρουμε τα απαραίτητα στοιχεία για τη διευθυνσιοδότηση των συνιστωσών ενός δικτύου μεταγωγής πακέτων. Πρώτα όμως θα περιγράψουμε τι συμβαίνει με τη σύνδεση των τερματικών συσκευών και των δρομολογητών στο Διαδίκτυο.

[1] Τα πρωτόκολλα χωρίς καταστάσεις (stateless) είναι τα πρωτόκολλα επικοινωνίας στο οποίο δεν τηρούνται πληροφορίες συνόδου από τον παραλήπτη. Το αντίθετο συμβαίνει σε πρωτόκολλα με καταστάσεις (stateful).

Ένας host τυπικά έχει ένα και μοναδικό σύνδεσμο μέσα στο δίκτυο. Όταν το IP που τρέχει ο host θέλει να στείλει ένα αυτοδύναμο πακέτο το κάνει μέσω αυτού του συνδέσμου. Το όριο μεταξύ του host και των φυσικών συνδέσμων ονομάζεται διεπαφή (interface). Ο δρομολογητής έχει ως βασική λειτουργία την λήψη του αυτοδύναμου πακέτου και την προώθησή του σε άλλο σύνδεσμο (ο δρομολογητής συνδέεται με δύο ή περισσότερους συνδέσμους του δικτύου μεταγωγής) σύμφωνα με πληροφορίες που διατηρεί σε ένα πίνακα, τον πίνακα δρομολόγησης (routing table). Το όριο μεταξύ του δρομολογητή και οπουδήποτε από τους συνδέσμους του, ονομάζεται επίσης διεπαφή. Ο δρομολογητής έχει πολλαπλές διεπαφές, μία για κάθε σύνδεσμό του. Επειδή ο κάθε host και ο κάθε δρομολογητής μπορούν να στέλνουν και να λαμβάνουν αυτοδύναμα πακέτα, το πρωτόκολλο IP απαιτεί η κάθε διεπαφή να έχει την δική της IP διεύθυνση, δηλαδή την ταυτότητά της. Η IP διεύθυνση είναι αυτή που δίνει τη δυνατότητα να επικοινωνούν όλοι οι host και οι συσκευές του Διαδικτύου μεταξύ τους. Οι κανόνες με τους οποίους προσδιορίζεται αυτή η ταυτότητα ορίζεται από το σχήμα διευθυνσιοδότησης (Kurose *et al.*, 2017).

Σύμφωνα με το IPv4, κάθε διεύθυνση έχει μήκος 32 bits, κάτι που πρακτικά σημαίνει ότι μπορεί να καλύψει 2^{32} ή 4.294.967.296 διαφορετικές διευθύνσεις. Τα 32 bits ομαδοποιούνται σε τμήματα των 8 bits που χωρίζονται μεταξύ τους με μία τελεία (dotted-decimal notation) και γράφονται στο δεκαδικό σύστημα αρίθμησης. ‘Ετσι, για παράδειγμα, η IP διεύθυνση 172.16.254.1 αντιστοιχεί στην δυαδική αναπαράσταση 10101100 00100000 11111110 00000001, όπως φαίνεται στην Εικόνα 1.



Εικόνα 2. Η μορφή της IPv4 διεύθυνσης.

Πηγή: (Wikipedia the free encyclopedia, 2021c)

Στο αρχικό σχήμα διευθυνσιοδότησης του IP οι διευθύνσεις χωρίζονται σε 5 κατηγορίες ή κλάσεις, τις A, B, C, D και E. Η διάθεση των διευθύνσεων γίνεται μόνο με τη χρήση μιας από τις κλάσεις: A, B, C που ονομάζονται κύριες κλάσεις.

Πίνακας 1. Οι κύριες κλάσεις των IPv4 διευθύνσεων.

Κλάση Διεύθυνσης	**Τιμές των πρώτων bits**	**Περιοχή διευθύνσεων**	**Αριθμός πιθανών δικτύων**	**Αριθμός hosts ανά δίκτυο**
Class A	0	1.0.0.0 έως 126.0.0.0	126 (2^7 -2)	16.777.214 (2^{24}-2)
Class B	1, 0	128.0.0.0 έως 191.255.0.0	16.384 (2^{14})	65.534 (2^{16}-2)
Class C	1, 1, 0	192.0.0.0 έως 223.255.255.0	2.097.152 (2^{21})	254 (2^8-2)

Η κατηγορία που ανήκει μια διεύθυνση και το εύρος των διευθύνσεων, προσδιορίζεται από τα πρώτα bits της διεύθυνσης και ο αριθμός των δικτύων και των hosts από τα επόμενα ψηφία. ‘Ετσι, για παράδειγμα, για την A κλάση διατίθενται τα πρώτα 8 bits, όπως φαίνεται στον Πίνακα 1.

Από την κλάση Α έχει δεσμευθεί η διεύθυνση 0.0.0.0 για τη δήλωση της προκαθορισμένης διαδρομής (default route) και η διεύθυνση 127.0.0.0 για τη λειτουργία του βρόχου επιστροφής (loopback). Για τον υπολογισμό των μέγιστων κόμβων ανά δίκτυο λαμβάνεται υπόψη ότι, εάν ένας κόμβος έχει όλα τα bits του ίσα με 1, η διεύθυνση αυτή δεσμεύεται ως η διεύθυνση ευρείας εκπομπής (broadcast address), ενώ εάν έχει όλα τα bits ίσα με 0 τότε η αντίστοιχη IP προσδιορίζει το δίκτυο συνολικά (Kurose *et al.*, 2017).

Ο αριθμός των bits που χρησιμοποιούνται για τον ορισμό του αριθμού δικτύων δηλώνεται με έναν λογικό αριθμό 32 bits, τη μάσκα υποδικτύου (subnet mask) και συμβολίζεται με την κάθετο «/» ακολουθούμενη από τον αριθμό των bits. Οι προκαθορισμένες μάσκες υποδικτύου είναι:

- Class A: 255.0.0.0 → /8
- Class B: 255.255.0.0 → /16
- Class C: 255.255.255.0 → /24

Η πρότυπη διαδικασία για τον διαμοιρασμό ενός δικτύου σε μικρότερα δίκτυα, τα ονομαζόμενα υποδίκτυα (subnets), περιγράφεται από το RFC 950 (‘Internet Standard Subnetting Procedure’, 1985). Το νόημα της υποδικτύωσης είναι η σύνδεση στο Διαδίκτυο των επιμέρους τερματικών συσκευών των ανεξάρτητων τοπικών δικτύων ενός οργανισμού. Εάν δεν υπήρχε αυτή η δυνατότητα διαμοιρασμού, ένας οργανισμός θα έπρεπε να δεσμεύει τόσες IP διευθύνσεις όσα τα τοπικά του δίκτυα. Ο τρόπος ορισμού των υποδικτύων βασίζεται στον διαμοιρασμό του αριθμού των κόμβων μιας IP διεύθυνσης σε δύο τμήματα που το ένα αντιστοιχεί στον αριθμό του υποδικτύου και το άλλο στον αριθμό του κόμβου μέσα στο υποδίκτυο (Kurose *et al.*, 2017).

Η διαχείριση των IP διευθύνσεων είναι στην αρμοδιότητα του Σώματος του Διαδικτύου για την εκχώρηση ονομάτων και αριθμών (Internet Corporation for Assigned Names and Numbers-ICANN), και βασίζεται στις κατευθυντήριες γραμμές του RFC 7020. Ο ρόλος του μη κερδοσκοπικού οργανισμού της ICANN δεν περιορίζεται μόνο στην εκχώρηση διευθύνσεων, αλλά και τη διαχείριση των εξυπηρετητών του συστήματος ονομασίας περιοχών (Domain Name System - DNS). Η ICANN εκχωρεί τις διευθύνσεις στους οργανισμούς των περιφερειακών μητρών

διαδικτύου, Regional Internet Registries- RIRs πού είναι οι εξής πέντε: African Network Information Center (AFRINIC) για την Αφρική, American Registry for Internet Numbers (ARIN) για την Ανταρκτική, τον Καναδά, τμήμα της Καραϊβικής και τις ΗΠΑ, Asia-Pacific Network Information Centre (APNIC) για μέρος της Ασίας και την Ωκεανία, Latin America and Caribbean Network Information Centre (LACNIC) για την υπόλοιπη Καραϊβική και την Λατινική Αμερική και Réseaux IP Européens Network Coordination Centre (RIPE NCC) για την Ευρώπη και την υπόλοιπη Ασία. Οι RIRs εκχωρούν τις διευθύνσεις στους ISPs. Η Αρχή του Διαδικτύου για την εκχώρηση αριθμών (Internet Assigned Numbers Authority- IANA), είναι ο οργανισμός προτύπων που επιβλέπει παγκόσμια την εκχώρηση των IP διευθύνσεων, τη διαχείριση των ζωνών στο DNS, καθώς και άλλων συμβόλων σχετικών με το IP πρωτόκολλο και αριθμών σχετικών με το διαδίκτυο (Kurose *et al.*, 2017).

Η IETF άρχισε την προσπάθεια για τη δημιουργία του διάδοχου πρωτόκολλου του IPv4 στις αρχές της δεκαετίας του 1990, τότε που άρχισε η ραγδαία εξάπλωση του Διαδικτύου και υπήρξε η εκτίμηση ότι το υπάρχον πρωτόκολλο θα μπορεί να υποστηρίξει τον αριθμό των συνδεμένων συσκευών μέχρι το 1994. Οι διάφορες προσπάθειες για την αντιμετώπιση της εξάντλησης των διευθύνσεων και την προσθήκη επιπλέον λειτουργιών άρχισαν να αναπτύσσονται παράλληλα, με στόχο τον επανασχεδιασμό του IP και την βελτίωση πρωτόκολλων. Το 1994 εγκρίθηκε το RFC 1883 με τίτλο "Internet Protocol, Version 6 (IPv6) Specification" και δημοσιεύτηκε το 1995. Η ομάδα των IPv6 πρωτόκολλων καθιερώθηκε ως πρότυπο από την IEFT το 1998 με το RFC2373 2460 (Deering and Hinden, 1998), καταργώντας το RFC 1883 (Graziani, 2017). Το πρωτόκολλο IPv6, θα το παρουσιάσουμε αναλυτικά στα επόμενα κεφάλαια. Προς το παρόν, αναφέρουμε ότι, στο IPv6 κάθε διεύθυνση έχει μήκος 128 bits, κάτι που πρακτικά σημαίνει ότι έχει τη δυνατότητα να καλύψει 2^{128} ή αλλιώς τον αστρονομικό αριθμό 340.282.366.920.938.463.463.374.607.431.768.211.456 διευθύνσεων. Οι IPv6 διευθύνσεις παριστάνονται ως οκτώ ομάδες τεσσάρων δεκαεξαδικών ψηφίων, διαχωρισμένες με την άνω-κάτω τελεία «:» (colon). Η πλήρης αναπαράσταση μπορεί να συντομευτεί. Για παράδειγμα, η διεύθυνση 2001:0db8:0000:0000:0000:8a2e:0370:7334 μπορεί να γραφεί ως 2001:db8::8a2e:370:7334 (Wikipedia the free encyclopedia, 2021e).

1.1.2 Οι κύριοι λόγοι μετάβασης στο IPv6

Το 1981 που καθιερώθηκε το IPv6, το τότε Διαδίκτυο, δηλαδή το ARPANET που είχε αναπτυχθεί μόνο στις ΗΠΑ, το αποτελούσαν μόνο 600 τερματικές συσκευές (Graziani, 2017). Κανείς τότε δεν μπορούσε να φανταστεί την ανάπτυξη και την εξάπλωση που θα έχει το Διαδίκτυο ούτε τις αλλαγές που θα έφερνε ο παγκόσμιος ιστός (World Wide Web - WWW), καθώς και άλλες τεχνολογίες, όπως για παράδειγμα το Διαδίκτυο των Πραγμάτων (Internet of Things – IoT) και ο κινητός υπολογισμός (mobile computing). Το σημερινό Διαδίκτυο και οι εφαρμογές που υποστηρίζονται δεν συγκρίνονται με το Διαδίκτυο του 1981. Ενδεικτικά, αναφέρουμε ότι, τα τέλη του 2020 οι χρήστες του Διαδικτύου ήταν περίπου 5 εκατομμύρια και η διείσδυση του Διαδικτύου στον παγκόσμιο πληθυσμό ήταν 63,2 %, η δε αύξηση του ποσοστού των χρηστών από το 2000 έως τα τέλη του 2020 ήταν της τάξης του 1.271 % (Miniwatts Marketing Group, 2021). Για το 2023 προβλέπεται ότι, οι χρήστες θα πλησιάσουν τα 5,3 εκατομμύρια και η διείσδυση του Διαδικτύου θα είναι περίπου 67%. Ο αριθμός των συσκευών που θα είναι συνδεμένες σε IP δίκτυα προβλέπεται να είναι περισσότερο από το τριπλάσιο του πληθυσμού της Γης, κάτι που αντιστοιχεί σε 3,6 συσκευές ανά κεφαλή και αριθμητικά σε 29,3 εκατομμύρια συσκευές. Οι μισές και πλέον συσκευές θα αφορούν 14,7 εκατομμύρια συνδέσεις στο IoT ή αλλιώς συνδέσεις Μηχανή με Μηχανή (Machine to Machine -M2M). Ο αριθμός των κινητών συνδέσεων αναμένεται να είναι 5,3 εκατομμύρια (Cisco, 2020).

Με δεδομένη την τρέχουσα κατάσταση και μορφή του Διαδικτύου και τις μελλοντικές προβλέψεις, συνυπολογίζοντας ότι η βασική απαίτηση για κάθε συσκευή του Διαδικτύου είναι να έχει μία και μοναδική διεύθυνση, γίνεται άμεσα αντιληπτή η αναγκαιότητα της μετάβασης από το IPv4 στο IPv6. Η αναγκαιότητα της μετάβασης στο IPv6 οφείλεται κύρια στην εξάντληση των διαθέσιμων IP διευθύνσεων (Graziani, 2017; Kurose *et al.*, 2017), αλλά υπάρχουν και άλλοι λόγοι που καθιστούν επιβεβλημένη αυτή τη μετάβαση. Όπως υποστηρίζει ο Graziani (2017), η μετάβαση κρίνεται απαραίτητη για τους παρακάτω επιπλέον λόγους:

- Υπάρχουν πλέον πολλά μέρη όπου χρησιμοποιείται μόνο το IPv6. Αν και υπάρχουν μηχανισμοί μετάφρασης που δίνουν τη δυνατότητα επικοινωνίας ανάμεσα σε δίκτυα που

υποστηρίζουν μόνο το IPv4 ή μόνο το IPv6, αυτοί οι μηχανισμοί δεν είναι αξιόπιστοι, ούτε μπορούν να αποδώσουν ικανοποιητικά.

- Τα δίκτυα που υποστηρίζουν μόνο το IPv6 έχουν καλύτερες επιδόσεις, σύμφωνα με τα στοιχεία που παρέχουν διάφοροι ISPs. Για παράδειγμα, το Facebook αναφέρει 20% έως 40% καλύτερες επιδόσεις στην τροφοδοσία των ειδήσεων.
- Όλα τα σύγχρονα λειτουργικά συστήματα (Windows, Mac OS, Linux, iOS και Android) εδώ και χρόνια υποστηρίζουν εξ'ορισμού το IPv6, συνεπώς είναι κρίσιμο για τους διαχειριστές των δικτύων να γνωρίζουν το IPv6. Τα δίκτυα πρέπει να προστατεύονται από κακόβουλες επιθέσεις, και όπως λαμβάνονται μέτρα για την ασφάλεια του IPv4, πρέπει να λαμβάνονται τα αντίστοιχα μέτρα και για το IPv6.

Στη συνέχεια θα παρουσιάσουμε συνοπτικά τους κυριότερους περιορισμούς που θέτει το IPv4 για την αντιμετώπιση των σημερινών απαιτήσεων του Διαδικτύου και τις καινοτομίες που εισάγει το IPv6 για να βοηθήσει στην αντιμετώπιση αυτών των περιορισμών.

1.2 Οι Περιορισμοί του IPv4 και οι Καινοτομίες του IPv6

Το βασικό κίνητρο για τον σχεδιασμό του IPv6 ήταν η διαφαινόμενη εξάντληση των IP διευθύνσεων. Όμως, το πρωτόκολλο IPv6 σχεδιάστηκε με την προοπτική να καλυφθούν οι αδυναμίες του IPv4 και οι περιορισμοί που θέτει, καθώς και τη βελτίωση των υπόλοιπων σχετικών πρωτόκολλων. Στις επόμενες παραγράφους παρουσιάζουμε θεματικά τους βασικούς περιορισμούς του IPv4 και που βοηθά το IPv6 για την αντιμετώπιση αυτών των περιορισμών.

1.2.1 Διαθεσιμότητα Διευθύνσεων

Βασική προϋπόθεση για την σύνδεση μιας συσκευής σε ένα δίκτυο, είναι η καταχώρηση της μιας και μοναδικής διεύθυνσης που την προσδιορίζει. Το IPv4 υποστηρίζει περίπου 4,3 εκατομμύρια διευθύνσεις, αριθμός που φαινόταν τεράστιος το 1981, αλλά λόγω της ραγδαίας ανάπτυξης του Διαδικτύου, οι διευθύνσεις αυτές εξαντλήθηκαν οριστικά από όλους τους RIRs στις 31 Ιανουαρίου

του 2011, παρόλο που από το 1999 είχε αρχίσει η εκχώρηση των IPv6 διευθύνσεων (Wikipedia the free encyclopedia, 2021d).

Το IPv6 υποστηρίζει περίπου $3,4x10^{38}$ διαφορετικές διευθύνσεις, που είναι ένας ασύλληπτος αριθμός και ικανός να καλύψει τις μελλοντικές απαιτήσεις, ανεξάρτητα από την περαιτέρω ανάπτυξη του Διαδικτύου.

1.2.2 Επέκταση Διευθύνσεων

Οι κύριες βραχυπρόθεσμες λύσεις για την αντιμετώπιση της διαθεσιμότητας των διευθύνσεων που παρουσιάστηκαν από την IETF είναι δύο: η Αταξική Διατομεακή Δρομολόγηση (Classless Inter-Domain Routing - CIDR) και η Μετάφραση Διευθύνσεων Δικτύου (Network Address Translation - NAT), τις οποίες παρουσιάζουμε συνοπτικά παρακάτω.

α) CIRD

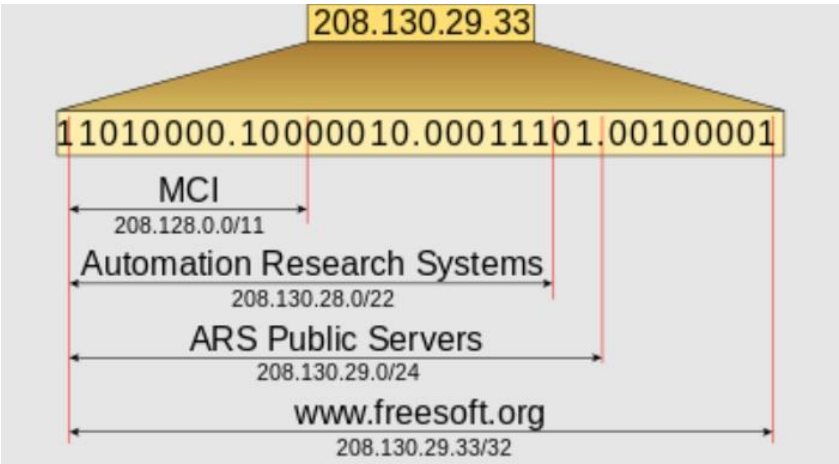
Το 1992 η IEFT αντικατέστησε τη μέθοδο διάθεσης των διευθύνσεων με τη μέθοδο της Αταξικής Διατομεακής Δρομολόγησης (Classless Inter-Domain Routing - CIRD) που προτάθηκε αρχικά στο RFC 1338, το οποίο καταργήθηκε το 1993 από το RFC 1519 (Fuller *et al.*, 1993). Το RFC 1519 καταργήθηκε κι αυτό με τη σειρά του το 2006 από το από το RFC 4632 (Fuller and Li, 2006). Το CIRD γενικεύει την έννοια της διευθυνσιοδότησης των υποδικτύων. Η 32-bit IP διεύθυνση χωρίζεται πάλι σε δύο μέρη και διατηρεί την ίδια μορφή a.b.c.d/x, όπου το x υποδεικνύει τον αριθμό των bits στο πρώτο μέρος της διεύθυνσης. Τα x πιο σημαντικά bits μιας διεύθυνσης της μορφής a.b.c.d/x, συνιστούν το τμήμα του δικτύου της IP διεύθυνσης και αναφέρονται ως πρόθεμα (prefix) της διεύθυνσης. Σε έναν οργανισμό τυπικά διατίθεται ένα τμήμα (block) από συνεχόμενες (όμορες) διευθύνσεις με ένα κοινό πρόθεμα. Σε αυτή την περίπτωση, οι IP διευθύνσεις των συσκευών μέσα στον οργανισμό, μοιράζονται το κοινό πρόθεμα. (Kurose *et al.*, 2017; Wikipedia the free encyclopedia, 2021e).

Παράδειγμα CIDR στο IPv4:

- 192.168.100.14/24 αναπαριστά την IPv4 διεύθυνση 192.168.100.14 και συνδέεται με το πρόθεμα 192.168.100.0, ή ισοδύναμα η μάσκα υποδικτύου είναι 255.255.255.0, που ξεκινά από 24 bits με τιμή 1.
- Το IPv4 τμήμα 192.168.100.0/22 αναπαριστά τις 1024 IPv4 διευθύνσεις από την 192.168.100.0 μέχρι την 192.168.103.255.

Ο πλήρης κατάλογος των IPv4 CIDR τμημάτων, δίνεται στην Wikipedia (Wikipedia the free encyclopedia, 2021a).

Τα πρόσθετα μήκη διευθύνσεων έδωσαν μεγαλύτερη ευελιξία στην IANA για τη διάθεση διευθύνσεων στους RIRs και έκαναν πιο αποτελεσματική την τη διανομή του περιορισμένου εύρους διευθύνσεων του IPv4. Η IANA παραχωρεί στους RIRs μεγάλα, μικρού-προθέματος CIDR τμήματα. Για παράδειγμα τη διεύθυνση, 62.0.0.0/8 (16 εκατομμύρια διευθύνσεις) διαχειρίζεται η RIPE NCC. Οι RIRs υποδιαιρούν αυτά τα τμήματα και εκχωρούν τις διευθύνσεις στους οργανισμούς των τοπικών μητρών διαδικτύου (Local Internet Registries -LIRs) οποίοι με τη σειρά τους μπορούν να προχωρήσουν σε αντίστοιχες υποδιαιρέσεις. Οι τελικοί χρήστες λαμβάνουν υποδίκτυα ανάλογα με τις βραχυπρόθεσμες ανάγκες τους (Wikipedia the free encyclopedia, 2021a). Ένα παράδειγμα για την CIDR δίνεται στην Εικόνα 2.



Εικόνα 3. Παράδειγμα διάθεσης διευθύνσεων με βάση την CIRD.

Πηγή: (Wikipedia the free encyclopedia, 2021a)

Στο IPv6 υπάρχει μια διεύθυνση (η παγκόσμια διεύθυνση μονοεκπομπής – global unicast address) που συμπεριλαμβάνει ένα πεδίο, το Subnet ID, το οποίο μπορεί να οριστεί από ένα οργανισμό, και έτσι δεν υπάρχει η ανάγκη για τον «δανεισμό» των ψηφίων από το τμήμα των ψηφίων του host για τη δημιουργία υποδικτύων. Ο οργανισμός μπορεί να σχεδιάσει και να διαχειρίζεται τα υποδίκτυά του σύμφωνα με τις ανάγκες του (Graziani, 2017).

Παρόλα αυτά, η CIDR μπορεί επίσης να εφαρμοστεί για τις IPv6 διευθύνσεις και το συντακτικό είναι σημασιολογικά παρόμοιο. Το μήκος του προθέματος έχει εύρος από 0 to 128 (Wikipedia the free encyclopedia, 2021a).

Παράδειγμα CIDR στο IPv6:

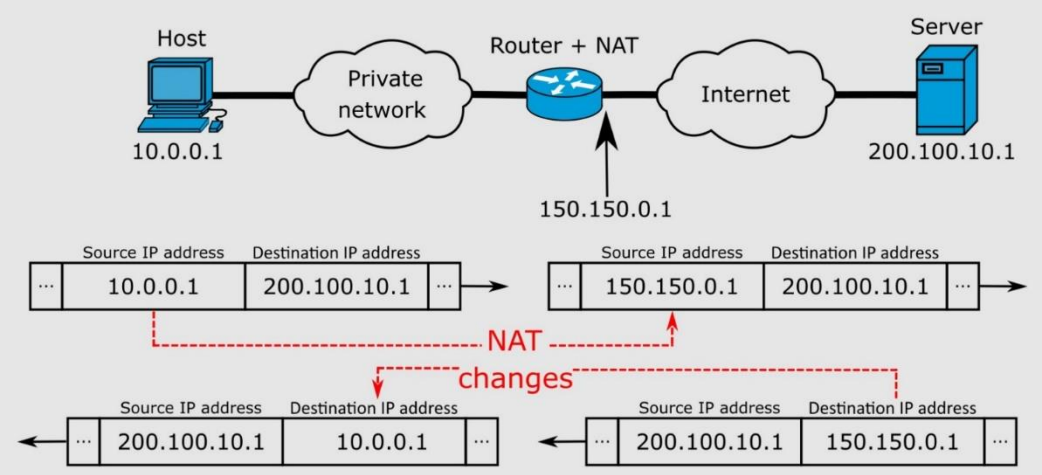
- το IPv6 τμήμα 2001:db8::/48 αναπαριστά το τμήμα των IPv6 διευθύνσεων από το 2001:db8:0:0:0:0:0:0 μέχρι το 2001:db8:0:ffff:ffff:ffff:ffff:ffff.

Ο πλήρης κατάλογος των IPv6 CIDR τμημάτων, δίνεται στην Wikipedia (Wikipedia the free encyclopedia, 2021a).

β) NAT

Το 1994 με το RFC 1631 παρουσιάστηκε για πρώτη φορά η Μετάφραση Διευθύνσεων Δικτύου (Network Address Translation - NAT) (Egevang and Francis, 1994), που είναι μια μέθοδος επανα-αντιστοίχισης (remapping) ενός διαστήματος IP διευθύνσεων σε άλλη μέσω της τροποποίησης της πληροφορίας για την διεύθυνση δικτύου στην επικεφαλίδα των πακέτων που μεταφέρονται διαμέσου μιας συσκευής δρομολόγησης της κυκλοφορίας, που συνήθως είναι ο οριακός δρομολογητής ενός υποδικτύου. Με την NAT εισάγεται η τεχνική της “IP μεταμφίεσης” (IP masquerading) όπου ένα πλήρες διάστημα διευθύνσεων, συνήθως ιδιωτικό, κρύβεται πίσω από μια μεμονωμένη IP σε ένα άλλο, συνήθως δημόσιο διάστημα διευθύνσεων. Οι κρυμμένες διευθύνσεις αλλάζουν σε μια απλή IP ως η πηγαία διεύθυνση (source address) των εξερχόμενων πακέτων κι έτσι εμφανίζονται σαν να προέρχονται από τη συσκευή δρομολόγησης και όχι από την τερματική συσκευή, όπως φαίνεται

στην Εικόνα 4 (Wikipedia the free encyclopedia, 2021f). Το RFC 1631 αντικαταστάθηκε από το RFC 3022 (Egevang and Srisuresh, 2001).



Εικόνα 4. NAT μεταξύ ενός ιδιωτικού δικτύου και του Διαδικτύου.

Πηγή: (Wikipedia the free encyclopedia, 2021f)

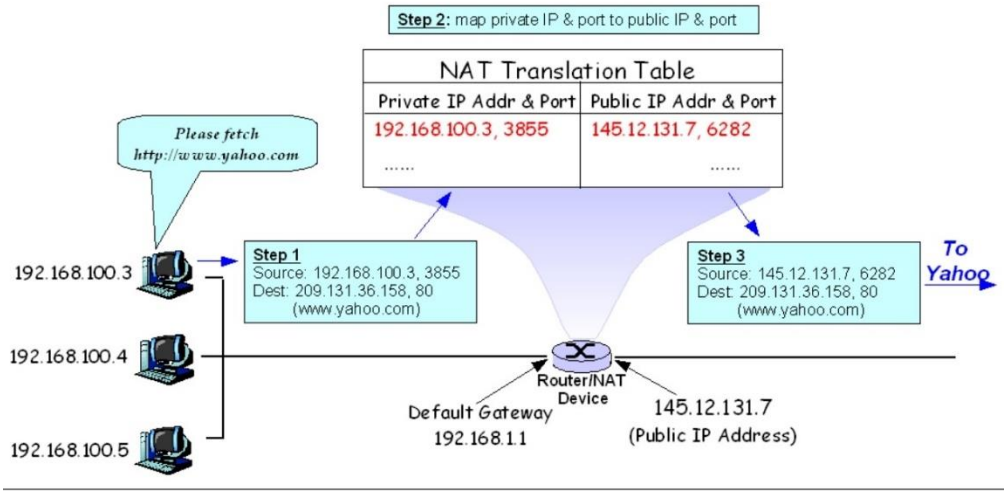
Ο απλούστερος τύπος NAT, που αναφέρεται ως βασικό NAT στο RFC 2663 (Holdrege and Srisuresh, 1999), παρέχει μία-προς-μία μετάφραση των IP διευθύνσεων και χρησιμοποιείται για τη διασύνδεση δύο IP δικτύων που έχουν ασύμβατη διευθυνσιοδότηση.

Η πλειοψηφία των μεταφραστών των διευθύνσεων δικτύων αντιστοιχίζουν πολλαπλές ιδιωτικές τερματικές συσκευές σε μια δημόσια διεύθυνση. Σε μια τυπική προσαρμογή ρυθμίσεων, ένα τοπικό δίκτυο χρησιμοποιεί ένα τμήμα από το διάστημα των ιδιωτικών διευθύνσεων, οι οποίες ορίζονται από το RFC 1918 (Moskowitz *et al.*, 1996) ως εξής:

- 10.0.0.0–10.255.255.255 (10.0.0.0/8)
- 172.16.0.0–172.31.255.255 (172.16.0.0/12)
- 192.168.0.0–192.168.255.255 (192.168.0.0/16)

Με το RFC 6598, η IANA εκχωρεί ακόμη ένα διάστημα ιδιωτικών διευθύνσεων, το 100.64.0.0/10, το οποίο προορίζεται αποκλειστικά για παρόχους υπηρεσιών δικτύου. Ο δρομολογητής συνδέεται

στο Διαδίκτυο με μια δημόσια διεύθυνση, που εκχωρείται από τον ISP. Καθώς η κυκλοφορία περνά από το τοπικό δίκτυο στο Διαδίκτυο, σε κάθε πακέτο η ιδιωτική διεύθυνση μεταφράζεται εν κινήσει (on the fly) από ιδιωτική σε δημόσια διεύθυνση. Όλα τα IP πακέτα έχουν μια διεύθυνση πηγής (source) και μια διεύθυνση προορισμού (destination). Τυπικά, στα πακέτα που περνούν από το ιδιωτικό δίκτυο προς το δημόσιο η διεύθυνση πηγής τροποποιείται. Για να μην υπάρχει ασάφεια για το πως μεταφράζονται οι απαντήσεις, χρειάζονται επιπλέον τροποποιήσεις στα πακέτα. Λόγω του ότι η συντριπτική μεταφορά των πακέτων στο επίπεδο μεταφοράς γίνεται με τα πρωτόκολλα TCP (Transmission Control Protocol) και UDP (User Datagram Protocol), στα οποία ο αριθμός της θύρας (port) αλλάζει, θα πρέπει στα πακέτα να αλλάζει και ο αριθμός της θύρας. Ένα παράδειγμα της μετάφρασης των διευθύνσεων φαίνεται στην Εικόνα 5. Στο RFC 2663 χρησιμοποιείται ο όρος μετάφραση δικτύου και θύρας (Network Address and Port Translation -NAPT) για αυτόν τον τύπο του NAT. Άλλοι όροι που χρησιμοποιούνται είναι ο όρος μετάφραση διεύθυνσης θύρας (Port Address Translation -PAT), IP masquerading, υπερφορτωμένο (NAT overload) και πολλά προς ένα (many-to-one NAT). Ο τύπος αυτός είναι ο συχνότερα χρησιμοποιούμενος και συνήθως είναι συνώνυμος με τον όρο NAT (Wikipedia the free encyclopedia, 2021e).



Εικόνα 5. Η μετάφραση των διευθύνσεων στο NAT

Πηγή: (Wikipedia the free encyclopedia, 2021f)

Το NAT παραβιάζει μία από τις βασικές αρχές σχεδίασης του Διαδικτύου, την άκρο-προς-άκρο συνδεσιμότητα δικτύου (end-to-end network connectivity) και θεωρείται ο κυριότερος λόγος για τον οποίο καθυστέρησε η μετάβαση στο IPv6. Ένας από τους βασικούς στόχους σχεδίασης του IPv6 ήταν η διατήρηση αυτής της αρχής (Graziani, 2017; Kurose *et al.*, 2017). Αυτό θεωρείται και το κυριότερο μειονέκτημα του NAT. Παρακάτω παραθέτουμε κάποια από τα πλεονεκτήματα και τα μειονεκτήματα του NAT.

Πλεονεκτήματα του NAT

- Το NAT διατηρεί νομικά καταχωρημένες διευθύνσεις IP.
- Παρέχει ιδιωτικότητα (privacy) καθώς η IP διεύθυνση της συσκευής που αποστέλλει και παραλαμβάνει την κυκλοφορία παραμένει κρυμμένη.
- Κατά την εξέλιξη ενός δικτύου, εξαλείφει την επανα-αρίθμηση των διευθύνσεων.

Μειονεκτήματα του NAT

- Η μετάφραση έχει ως αποτέλεσμα την καθυστέρηση στη διαδρομή μεταγωγής.
- Κάποιες εφαρμογές δεν λειτουργούν όταν είναι ενεργοποιημένο το NAT.
- Καθιστά πιο σύνθετη την παράλληλη εφαρμογή κάποιων πρωτόκολλων, όπως για παράδειγμα το IPsec (θα το παρουσιάζουμε στη συνέχεια).

Λόγω αριθμού των διαθέσιμων διευθύνσεων στο IPv6, η χρήση του NAT καθίσταται περιττή. Παρόλα αυτά, το NAT χρησιμοποιείται σε μηχανισμούς μετάβασης από το IPv4 στο IPv6 (Graziani, 2017).

1.2.3 Απλοποίηση Διαχείρισης Δικτύων και Ρυθμίσεων

Για τη σύνδεση μιας συσκευής σε δίκτυο που υποστηρίζει το IPv4, η καταχώρηση της μοναδικής IP διεύθυνσης μπορεί να γίνει είτε στατικά, δηλαδή με χειροκίνητη προσαρμογή των ρυθμίσεων (manual configuration), είτε δυναμικά με τη χρήση του Πρωτόκολλου Δυναμικής Καταχώρησης Κόμβου (Dynamic Host Configuration Protocol – DHCP), όπου ένας εξυπηρετητής (DHCP server)

αναλαμβάνει να αποδώσει τις IP διευθύνσεις στις τερματικές συσκευές του δικτύου, τους πελάτες (clients). Οι πελάτες ζητούν από τον DHCP εξυπηρετητή τη δυναμική εκχώρηση IP διευθύνσεων πριν τη σύνδεση στο δίκτυο. Το IPv6 συμπεριλαμβάνει έναν μηχανισμό σύνδεσης και άμεσης λειτουργίας (plug-and-play) που διευκολύνει τη σύνδεση του εξοπλισμού στο δίκτυο. Η απαιτούμενη προσαρμογή ρυθμίσεων είναι αυτόματη. Το χαρακτηριστικό αυτό ονομάζεται αυτόματη προσαρμογή ρυθμίσεων διευθύνσεων χωρίς καταστάσεις (StateLess Address AutoConfiguration - SLAAC) και επιταχύνει τη συνδεσιμότητα στο δίκτυο γιατί οι συσκευές μπορούν να αποκτήσουν μια μοναδική και παγκόσμια διεύθυνση δρομολόγησης χωρίς τις υπηρεσίες ενός DHCPv6 εξυπηρετητή, κάτι που είναι πολύ σημαντικό ειδικά σε μεγάλα IPv6 δίκτυα, όπως τα δίκτυα του IoT. Επίσης, το DHCPv6 προβλέπει λειτουργία stateless και λειτουργία stateful, κάτι που προδίδει σε μια συσκευή αρκετές επιλογές για να αποκτήσει μέρος ή όλη την πληροφορία διευθυνσιοδότησης (Graziani, 2017).

Όπως ήδη έχουμε αναφέρει, το IP δεν εγγυάται την παράδοση των αυτοδύναμων πακέτων στον τελικό προορισμό και αυτή η λειτουργία εκτελείται από άλλα πρωτόκολλα. Για να γίνει αυτό, θα πρέπει να υπάρχει ένας μηχανισμός αναφοράς σφαλμάτων και αυτός είναι το πρωτόκολλο μηνύματος ελέγχου διαδικτύου (Internet Control Message Protocol – ICMP), το οποίο χρησιμοποιείται και για τη διακίνηση πληροφοριών ελέγχου, δηλαδή για παράδειγμα, να ελέγξει την το εάν ο ένας προορισμός είναι προσιτός, να επιλέξει την αναδρομολόγηση πακέτων κ.α. (Kurose *et al.*, 2017).

Το ICMPv6 πρωτόκολλο ανακάλυψης γειτόνων (Network Discovery Protocol – NDP), χρησιμοποιείται από τους IPv6 δρομολογητές για την αποστολή μηνυμάτων υποδεικνύοντας πως μια συσκευή μπορεί να λάβει δυναμικά την IPv6 πληροφορία διευθυνσιοδότησης. Το ICMPv6 χρησιμοποιείται στο επίπεδο δικτύου για τον για την αντιστοίχιση της IP διεύθυνσης προορισμού με την φυσική διεύθυνση της συσκευής, αντί του πρωτόκολλου προσδιορισμού διεύθυνσης (Address Resolution Protocol – ARP) (Graziani, 2017).

Επίσης, το IPv6 παρέχει τη δυνατότητα στις συσκευές να ανήκουν σε πολλά ταυτόχρονα, με μια μοναδική διεύθυνση σε κάθε δίκτυο, καθώς και τη δυνατότητα του συνδυασμού πολλαπλών επιχειρησιακών δικτύων χωρίς να χρειάζεται επανα-διευθυνσιοδότηση (Graziani, 2017).

1.2.4 Ποιότητα Υπηρεσιών

Η μεγάλη διάδοση των πολυμεσικών εφαρμογών στο Διαδίκτυο, καθώς και των υπηρεσιών πραγματικού χρόνου υπάρχει η ανάγκη για την ανάπτυξη δικτύων εγγυημένης ποιότητας εξυπηρέτησης (Quality of Service – QoS). Οι μετρικές που έχουν προταθεί για τη μέτρηση της ποιότητας υπηρεσιών είναι αρκετές και διαφορετικές μεταξύ τους και περιλαμβάνουν μεταβλητές όπως το εύρος ζώνης (bandwidth), η διαμετακομιστική ικανότητα ή ρυθμαπόδοση (throughput) που αντιπροσωπεύει τα δεδομένα που μεταφέρονται στη μονάδα του χρόνου, η καθυστέρηση (delay), η διακύμανση της καθυστέρησης (jitter), το κόστος και πιθανότητα απώλειας πακέτων (Parra, Rios and Lopez Rubio, 2011). Όταν θέλουμε να συγκρίνουμε την ποιότητα των υπηρεσιών ανάμεσα στο IPv4 και το IPv6, οι κυριότερες μετρικές είναι η καθυστέρηση, η διακύμανση καθυστέρησης και η ρυθμαπόδοση (Hassan and Jabbar, 2017).

Η υποστήριξη της κυκλοφορίας των δεδομένων πραγματικού χρόνου στο IPv4 βασίζεται σε ένα πεδίο μήκους 8 bit της επικεφαλίδας του, το Type of Service (TOS), το οποίο έχει περιορισμένη λειτουργικότητα και δεν μπορεί να γίνει ο διαχωρισμός των πακέτων όπου τα δεδομένα είναι ευαίσθητα στον χρόνο (time- sensitive), όπως για παράδειγμα είναι τα δεδομένα του video streaming, ή όχι, όπως για παράδειγμα τα δεδομένα της μεταφοράς των αρχείων (Graziani, 2017; Kurose *et al.*, 2017).

Στο IPv6, υπάρχουν μηχανισμοί για την υποστήριξη της κυκλοφορίας δεδομένων με διαφορετικές απαιτήσεις ανάλογα με το είδος της ροής των δεδομένων. Μέσω αυτών των μηχανισμών, οι δρομολογητές αναγνωρίζουν το είδος της ροής των δεδομένων των πακέτων και η ποιότητα υπηρεσιών μπορεί να υποστηριχθεί αποτελεσματικά (Graziani, 2017).

Το IPv6 υποστηρίζει την διευθυνσιοδότηση κατά την πολυεκπομπή (multicast addressing), η οποία επιτρέπει στις ροές πακέτων που είναι ευαίσθητες στην ρυθμαπόδοση, όπως για παράδειγμα οι ροές πολυμέσων, να αποστέλλονται σε πολλαπλούς προορισμούς ταυτόχρονα, μειώνοντας έτσι το εύρος ζώνης (bandwidth) του δικτύου (Graziani, 2017).

Περισσότερα για τους μηχανισμούς οι οποίοι συμβάλλουν στην ποιότητα υπηρεσιών του IPv6 θα έχουμε τη δυνατότητα να εξετάσουμε σε επόμενα κεφάλαια.

1.2.5 Υποστήριξη Κινητών Χρηστών

Ο πιο προφανής λόγος για την αδυναμία υποστήριξης των κινητών χρηστών από το IPv4, είναι ο αριθμός των κινητών συνδέσεων, ο οποίος το 2018 ήταν 5,1 εκατομμύρια και αναμένεται το 2023 να πλησιάσει τα 5,3 εκατομμύρια, κάτι που αντιστοιχεί στο 70% περίπου του παγκόσμιου πληθυσμού (Cisco, 2020). Τέτοιο θέμα δεν υπάρχει με το IPv6, λόγω του ότι μπορεί να καλύψει την ανάγκη της μοναδικής IP για κάθε συσκευή. Όπως αναφέρει ο Graziani (2017), οι περισσότεροι πάροχοι κινητών υπηρεσιών παγκόσμια υποστηρίζουν ήδη το IPv6 στην ανάπτυξη των δικτύων τους και είναι πρωτοπόροι στην εφαρμογή του. Η υιοθέτηση του προτύπου στην Ευρώπη και την Ασία, οφείλεται κατά κύριο λόγο στην ανάπτυξη της κινητής τηλεφωνίας. Η παροχή ασύρματων υπηρεσιών αναμένεται να προωθήσει το IPv6 λόγω των αυξανόμενου αριθμού των συσκευών που συνδέονται στο Διαδίκτυο.

Η υποστήριξη της κινητικότητας στο IPv4 προστέθηκε πολλά χρόνια μετά την καθιέρωση του IP με το RFC 3344 και το πρωτόκολλο “IP Mobility Support for IPv4” (Perkins, 2002), το οποίο αναφέρεται συνοπτικά ως Mobile IPv4. Λόγω της έλλειψης επεκτασιμότητας, κάποια στοιχεία του πρωτόκολλου τοποθετήθηκαν σε άλλα επίπεδα της στοίβας TCP/IP. Για παράδειγμα, στο Mobile IPv4 η καταχώρηση (registration) των μηνυμάτων αίτησης/απάντησης (request/reply) μεταφέρονται μέσω του πρωτόκολλου UDP, κάτι που επίσης παραβιάζει την αρχή της άκρο- προς- άκρο συνδεσιμότητας (*Mobility support*, 2021).

Βασικά, το Mobile IPv4 βασίζεται σε ένα μηχανισμό επανακατεύθυνσης της κυκλοφορίας των δεδομένων όταν η τερματική συσκευή-πελάτης κινείται και εξυπηρετείται ανάλογα με τη θέση του από κάποιον σταθμό- εξυπηρετητή (Cisco, no date). Δεν θα εισέλθουμε σε περισσότερες λεπτομέρειες (οι οποίες παρέχονται από την προαναφερθείσα πηγή και το αντίστοιχο RFC), παραμόνο θα αναφέρουμε ότι, ο μηχανισμός αυτός βασίζεται σε τριγωνική δρομολόγηση. Επίσης, το Mobile IPv4 δεν προσφέρει λύση για πολυεκπομπή (Cisco, no date).

Η IETF όρισε με το RFC 3775 το πρωτόκολλο "Mobility Support in IPv6" (Perkins, Arkko and Johnson, 2004), όπου ορίζεται η υποστήριξη της κινητικότητας στο IPv6 και αναφέρεται απλά ως Mobile IPv6. Το Mobile IPv6 πηγαίνει ένα βήμα παραπάνω όσον αφορά την IPv4 υποστήριξη κινητικότητας και παρέχει βέλτιστες διαδρομές για τα δεδομένα μεταξύ πελάτη και εξυπηρετητή. Η διαδικασία στο IPv6 είναι παρόμοια με αυτήν του IPv4 με κάποιες επιπλέον προσθήκες που αφορούν τη διαδρομή δρομολόγησης, η οποία πλέον δεν είναι τριγωνική, αλλά γίνεται απευθείας μεταξύ πελάτη- εξυπηρετητή και συνεπώς καθίσταται απλούστερη. Για να επιτευχθεί όμως αυτό, απαιτείται οι κινητές τερματικές συσκευές να είναι όλες συμβατές με το IPv6 (Cisco, no date).

1.2.6 Ασφάλεια

Τα δίκτυα των υπολογιστών, και κατ' επέκταση το Διαδίκτυο, χαρακτηρίζονται ως ασφαλή μέσα επικοινωνίας εάν υποστηρίζουν τουλάχιστον τρεις βασικές μη λειτουργικές απαιτήσεις: την εμπιστευτικότητα (Confidentiality), την ακεραιότητα (Integrity) και τη διαθεσιμότητα (Avialiability) των δεδομένων που διακινούνται. Αυτοί είναι οι τρεις βασικοί στόχοι για όλα τα επίπεδα, καθώς και για το επίπεδο δικτύου και για την επίτευξή τους προτάθηκε από την IETF η σειρά των πρωτόκολλων από ασφάλειας (IP Security - IPSec), η οποία είναι πολύπλοκη και περιγράφεται από πολλά RFCs. Τα βασικότερα είναι το RFC 2011 (Atkinson and Kent, 1998) όπου περιγράφεται η αρχιτεκτονική του IPSec, και το RFC 2411 (Doraswamy, Glenn and Thayer, 1998) όπου δίνεται μια συνοπτική περιγραφή των επιμέρους πρωτόκολλων που συνθέτουν την οικογένεια των IPSec (Kurose *et al.*, 2017). Ο σχεδιασμός του IPSec είναι τέτοιος ώστε να είναι δυνατή η πλήρης ενσωμάτωσή του στο IPv4, στο οποίο δεν υπήρχε αρχικά η πρόβλεψη για μηχανισμούς ασφάλειας.

Σε αντίθεση με το IPv4, στο IPv6 υπάρχουν μηχανισμοί ασφάλειας για τη διασφάλιση της πληροφορίας των πακέτων που βρίσκονται σε πεδία της επικεφαλίδας του, όπως θα δούμε σε επόμενα κεφάλαια, γιατί ένας ακόμη στόχος στον αρχικό σχεδιασμό του IPv6 ήταν η από άκρο σε άκρο κρυπτογράφηση. Αρχικά, η εφαρμογή του IPSec ήταν υποχρεωτική για το IPv6, αλλά έγινε προαιρετική με το RFC 6434, το οποίο αντικαταστάθηκε από το RFC 8504 (Chown, Loughney and Winters, 2019) όπου η εφαρμογή του IPSec παραμένει προαιρετική και είναι στην αρμοδιότητα του εκάστοτε ISP. Όμως, η αλήθεια είναι ότι το IPv4 μπορεί να είναι εξίσου ασφαλές με την παράλληλη χρήση του IPSec, απορρίπτοντας τον μύθο ότι το IPv6 είναι περισσότερο ασφαλές από το IPv4 (Graziani, 2017). Μια ενδιαφέρουσα τοποθέτηση για αυτόν τον μύθο, δίνεται στο blog της APNIC (Holder, 2019) και παραπέμπουμε τον αναγνώστη στην πηγή για περισσότερες λεπτομέρειες.

1.2.7 Σύστημα Ονοματοδοσίας

Η αριθμητική απεικόνιση των IP διευθύνσεων καθιστά δύσκολη την ανάγνωσή τους και τη χρήση τους. Είναι πολύ δύσκολο κάποιος να θυμάται έναν αριθμό που αντιστοιχεί σε μια διεύθυνση, όπως για παράδειγμα τον 172.16.254.1 του IPv4, πόσο μάλλον τον 2001:0db8:0000:0000:0000:8a2e:0370:7334 ή έστω τον 2001:db8::8a2e:370:7334 του IPv6. Για τον λόγο αυτό αναπτύχθηκε από τα πρώτα χρόνια του Διαδικτύου το Σύστημα Ονομασίας Περιοχών (Domain Name System- DNS), για την αντιστοίχιση της αριθμητικής απεικόνιση της IP διεύθυνσης σε μια ισοδύναμη αλφαριθμητική απεικόνιση το οποίο είναι ένα ιεραρχικό σύστημα ονοματοδοσίας για τα δίκτυα που χρησιμοποιούν το IP πρωτόκολλο. Η διαχείριση του DNS είναι στην αρμοδιότητα της IANA. Περισσότερες πληροφορίες για το DNS δίνονται από τους Kurose κ.ά. (2017).

Το DNS βοηθά τους χρήστες μεταφράζοντας τα αλφαριθμητικά ονόματα των τερματικών συσκευών σε IP διευθύνσεις. Ο DNS επιλυτής (DNS Resolver) είναι μια συνιστώσα λογισμικού που αποτελεί μέρος των λειτουργικών συστημάτων, των δρομολογητών και των υπηρεσιών του δικτύου, όπου δέχεται το όνομα ενός host, για παράδειγμα “www.example.com” και είναι υπεύθυνος για την εύρεση της σωστής IP διεύθυνσης του ονόματος του host. Κατά την μετάβαση του IPv4 προς το

IPv6, η ονοματοδοσία για τους hosts παραμένει η ίδια, καθώς και η αρμοδιότητες για την ονοματοδοσία (Kurose *et al.*, 2017).

Κεφάλαιο 2: Εισαγωγή στο IPv6

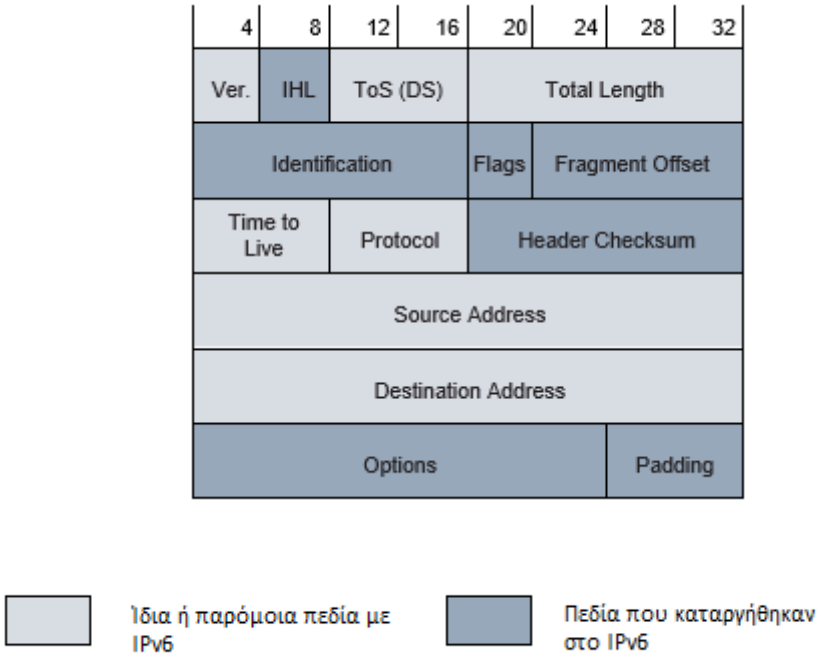
Στο Κεφάλαιο αυτό γίνεται η παρουσίαση της δομής της επικεφαλίδας του πρωτοκόλλου IPv6, καθώς και οι διαφορές της από την επικεφαλίδα του πρωτοκόλλου IPv4. Στη συνέχεια παρουσιάζονται τα πεδία της επικεφαλίδας του IPv6 και γίνεται ειδική μνεία για τα πεδία που διαφέρουν από το IPv4. Τέλος, γίνεται η αναλυτική παρουσίαση της λειτουργίας των επικεφαλίδων των IPv6.

2.1 Επισκόπηση των Αλλαγών της Επικεφαλίδας

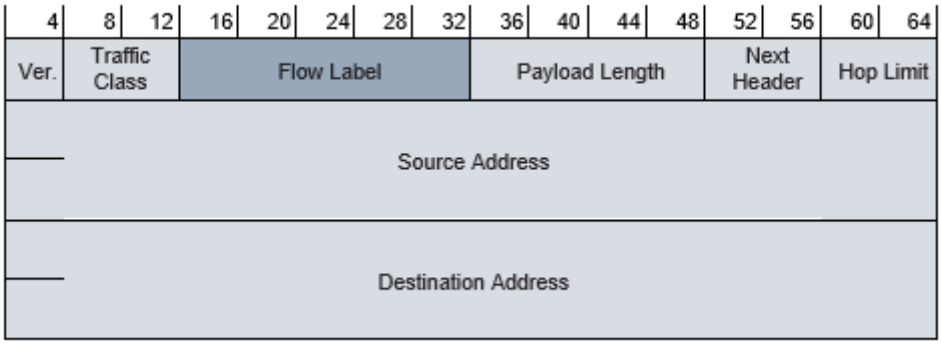
Οι δύο κύριες λειτουργίες του IP πρωτόκολλου δικτύου, όπως αναφέρθηκε στο προηγούμενο κεφάλαιο, είναι η προώθηση και διανομή αυτοδύναμων πακέτων μεταξύ των τερματικών συσκευών του δικτύου, και η κατάτμηση και συναρμολόγηση αυτών των πακέτων. Κάθε πακέτο αποτελείται από την επικεφαλίδα και τα δεδομένα. Ανάλογα με τον τύπο του δικτύου το μέγιστο μήκος των δεδομένων σε bytes που μπορεί να ενθυλακωθεί (encapsulate) μέσα σε ένα πακέτο είναι προκαθορισμένο και ονομάζεται Μέγιστη Μονάδα Μετάδοσης (Maximum Transmission Unit - MTU). Γενικά, η κατανόηση των πεδίων της επικεφαλίδας των πακέτων του IP πρωτόκολλων είναι σημαντική για την κατανόηση της λειτουργίας του επιπέδου δικτύου της στοίβας των πρωτόκολλων του TCP/IP, γιατί γίνονται κατανοητά τα χαρακτηριστικά της από άκρο σε άκρο επικοινωνίας των πακέτων μεταξύ των hosts της πηγής και του προορισμού (Kurose *et al.*, 2017)

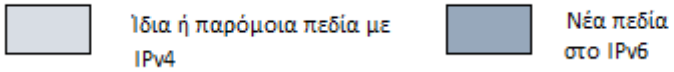
Η δομή της επικεφαλίδας του IPv4 ορίζεται από το RFC 791 (Postel, 1981). Όπως ήδη έχουμε αναφέρει, ο κύριος λόγος επανασχεδίασης του IP ήταν η διαφαινόμενη εξάντληση των διευθύνσεων, αλλά παράλληλα υπήρξε η πρόθεση βελτίωσης των χαρακτηριστικών του IPv6. Η δομή της επικεφαλίδας του IPv6 ορίζεται από το RFC 2460 (Deering and Hinden, 1998) και συνήθως αναφέρεται ως *κύρια επικεφαλίδα IPv6 (main IPv6 header)*. Αυτό συμβαίνει γιατί η κύρια επικεφαλίδα μπορεί να δείχνει σε μία ή περισσότερες επικεφαλίδες, τις επικεφαλίδες επέκτασης (extension headers), τις οποίες θα δούμε αναλυτικά σε επόμενη παράγραφο και οι οποίες αποτελούν μια από τις πιο σημαντικές προσθήκες στο IPv6.

Οι επικεφαλίδες του IPv4 και IPv6 φαίνονται στην Εικόνα 6α και 6β, αντίστοιχα και θα προχωρήσουμε σε μια πρώτη σύγκριση μεταξύ τους για να εντοπίσουμε τις αλλαγές. Όπως βλέπουμε, υπάρχουν πεδία τα οποία είτε καταργήθηκαν στο IPv6, είτε είναι ίδια ή παρόμοια και επίσης στο IPv6 έγινε προσθήκη νέων πεδίων.



(α) Η επικεφαλίδα του IPv4





(b) Η επικεφαλίδα του IPv4

Εικόνα 6. Οι επικεφαλίδες των IPv4 και IPv6

Πηγή: (Graziani, 2017)

Οι πιο σημαντικές αλλαγές που εισάγονται στο IPv6 είναι προφανείς από τη μορφή του αυτοδύναμου πακέτου και πιο συγκεκριμένα από τις αλλαγές στην επικεφαλίδα του (Graziani, 2017; Kurose *et al.*, 2017). Με μια πρώτη ματιά, διαπιστώνουμε ότι η επικεφαλίδα του IPv6 είναι απλούστερη, βελτιστοποιημένη και περιέχει λιγότερα πεδία. Το μήκος της επικεφαλίδας από 32 bit στο IPv4 είναι 64 bit στο IPv6, γιατί ένας από τους βασικούς στόχους των σχεδιαστών του IPv6 ήταν, μεταξύ των άλλων, η βελτίωση του IP πρωτόκολλου για τις συσκευές που διαθέτουν 64-bit κεντρικές μονάδες επεξεργασίας (Central Processing Units – CPUs). Έτσι, όλα τα πεδία του IPv6 ξεκινούν με 64-bit ομοιόμορφο όριο ή πολλαπλάσιο του 64, χωρίς αυτό να δημιουργεί πρόβλημα στις CPU των 32 bits, γιατί το 64-bit όριο είναι επίσης ένα 32-bit όριο που είναι το όριο του IPv4. Το μήκος της επικεφαλίδας του IPv6 είναι προκαθορισμένο στα 40 bytes, με αποτέλεσμα η επεξεργασία των πακέτων στους δρομολογητές να είναι πιο γρήγορη, ενώ στο IPv4 είναι μεταβλητό. Επίσης, μια άλλη προφανής αλλαγή είναι η αλλαγή του μήκους της διεύθυνσης πηγής και προορισμού από τα 32 bits στα 128 bits, η οποία ήταν και ο κύριος λόγος επανασχεδιασμού του IP πρωτοκόλλου λόγω της διαφαινόμενης εξάντλησης των διευθύνσεων. Στην επόμενη παράγραφο παρουσιάζουμε αναλυτικά τη βασική επικεφαλίδα του IPv6.

2.2 Η Βασική Επικεφαλίδα του IPv6

Με βάση την Εικόνα 6, θα εξετάσουμε αναλυτικά την βασική επικεφαλίδα του IPv6, αναφέροντας παράλληλα τις κύριες διαφορές με αυτή του IPv4 και τα πεδία του IPv4 που καταργήθηκαν, έχοντας ως αναφορά την επικεφαλίδα του IPv6, σύμφωνα με τον Graziani (2017).

Το πεδίο ***Έκδοση (Version)*** δηλώνει την έκδοση του πακέτου που χρησιμοποιείται στο αυτοδύναμο πακέτο και είναι κοινή και στα δύο πρωτόκολλα. Έχει μήκος 4 bits. Βάσει αυτού του πεδίου, ο δρομολογητής μπορεί να προσδιορίσει πως θα διερμηνευτεί το υπόλοιπο τμήμα του πακέτου. Προφανώς, η τιμή είναι 4 στο IPv4 και 6 στο IPv6.

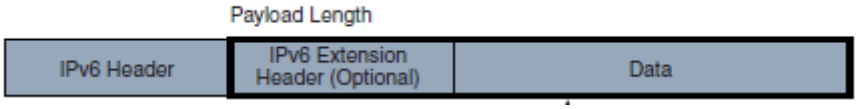
Το πεδίο *Μήκος επικεφαλίδας IP (IP Header Length – IHL)* του IPv4 καταργήθηκε στο IPv6, γιατί το μήκος της επικεφαλίδας του IPv6 είναι προκαθορισμένο. Στο IPv4 καθορίζει το μήκος της επικεφαλίδας και έχει μήκος 4 bits. Επειδή ένα IPv4 πακέτο μπορεί να έχει διαφορετικό αριθμό επιλογών (options) τα bits αυτά χρειάζονται και να ορίσουν σε ποιο σημείο ξεκινά το τμήμα των δεδομένων (για παράδειγμα μπορεί να ενθυλακώνεται ένα τμήμα από το επίπεδο μεταφοράς).

Το πεδίο ***Κλάση κυκλοφορίας (Traffic Class)*** του IPv6 και *Τύπος Υπηρεσίας (Type of service – TOS)* του IPv4 είναι παρόμοια. Μέσω αυτών των πεδίων καθορίζεται ο τρόπος χειρισμού του πακέτου από τους δρομολογητές. Η πληροφορία που δίνει το πεδίο είναι άμεσα συσχετισμένη με την ποιότητα υπηρεσιών, γιατί ορίζονται οι προτεραιότητες προώθησης των πακέτων. Όταν υπάρχουν πολλά πακέτα προς μεταφορά σε μια διεπαφή, η τιμή αυτού του πεδίου χρησιμοποιείται για να οριστεί μεταξύ των άλλων και η σειρά με την οποία θα δρομολογηθούν τα πακέτα. Είναι χρήσιμο για τον διαχωρισμό των πακέτων πραγματικού χρόνου από αυτά του μη -πραγματικού χρόνου. Με το RFC 2474 (Baker *et al.*, 1998), ορίστηκε από την IETF η τεχνική των διαφοροποιημένων υπηρεσιών (Differentiated Services – DS) που χρησιμοποιείται και στα δύο πρωτόκολλα. Στο IPv6 ειδικότερα διατίθενται 6 bits που χαρακτηρίζονται ως σημείο κωδικού διαφοροποιημένων υπηρεσιών (Differentiated Services Code Point - DSCP). Ο τρόπος που χρησιμοποιούνται τα 6 bits στο DSCP δίνει τη δυνατότητα για 64 διαφορετικές σημάνσεις για την κλάση κυκλοφορίας. Έτσι, στο IPv6 παρέχεται μεγαλύτερη ευελιξία για την επιλογή της προτεραιότητας κατά την προώθηση των πακέτων.

Το επόμενο πεδίο ***Ετικέτα Ροής (Flow Label)*** είναι ένα νέο πεδίο που προστέθηκε στο IPv6 και χρησιμοποιείται για την τοποθέτηση ετικετών (tags) σε μια ακολουθία ή ροή IPv6 πακέτων που αποστέλλονται από την πηγή προς τον προορισμό. Αυτή η ροή μπορεί να χρησιμοποιηθεί για να

βάλει ετικέτες στα πακέτα όπου υπάρχει απαίτηση για διαφορετική διαχείριση από τους δρομολογητές, όπως για παράδειγμα για δεδομένα που αφορούν υπηρεσίες πραγματικού χρόνου. Το πεδίο χρησιμοποιείται για την αναγνώριση όλων των πακέτων της ίδιας ροή για να διασφαλιστεί ότι θα έχουν τον ίδιο τρόπο διαχείρισης από τον δρομολογητή. Η χρήση των ετικετών ροής περιγράφεται στο RFC 6437 (Amante *et al.*, 2011). Προς το παρόν, δεν υπάρχουν πολλές εφαρμογές που εξετάζουν την ετικέτα ροής. Έχουν οριστεί δύο περιπτώσεις χρήσεις: η Πολύ-Διαδρομή Ίσου Κόστους (Equal Cost Multi-Path -ECMP) η οποία ορίζεται στο RFC 6438 (Amante and Carpenter, 2011) , και η Εξισορρόπηση Φορτίου Εξυπηρετητή (Server Load Balancing - SLB) η οποία ορίζεται στο RFC 7098 (Carpenter, Jiang and Tarreau, 2014). Πολλά συστήματα θέτουν την Ετικέτα Ροής στα πακέτα που ανήκουν σε διαφορετικές TCP συνόδους. Όταν στην Ετικέτα Ροής τίθεται η τιμή 0, σημαίνει ότι η κυκλοφορία δεν συνδέεται με καμία ροή.

Το πεδίο ***Μήκος Ωφέλιμου Φορτίου (Payload Length)*** του IPv6 που αφορά τα δεδομένα και έχει μήκος 16 bits, είναι παρόμοιο με το πεδίο *Μήκος Πακέτου (Total Length)* του IPv4 εκτός από μία ουσιαστική διαφορά: το πεδίο Μήκος Πακέτου του IPv4 προσδιορίζει το συνολικό μήκος του πακέτου ενώ το πεδίο Μήκος Ωφέλιμου Φορτίου του IPv6 ορίζει μόνο τον αριθμό των bytes του ωφέλιμου φορτίου των δεδομένων (payload) του πακέτου και δεν περιλαμβάνει το μήκος της κύριας επικεφαλίδας του IPv6, όπως φαίνεται στην Εικόνα 7. Εάν το IPv6 πακέτο έχει μία ή περισσότερες επικεφαλίδες επέκτασης, αυτές περιλαμβάνονται σε αυτό το πεδίο και θεωρούνται μέρος του payload.

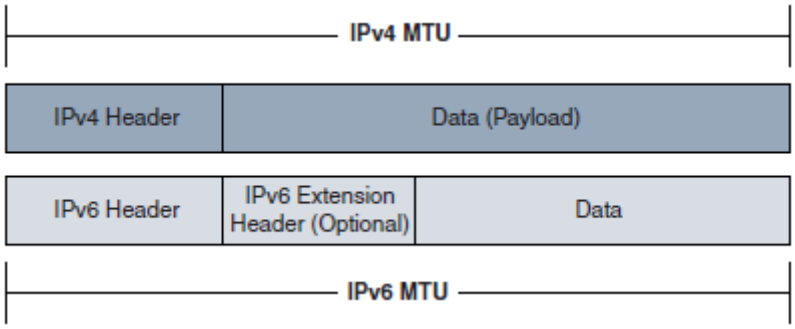


Εικόνα 7. Το πεδίο μήκος δεδομένων (Payload Length) του IPv6

Πηγή: (Graziani, 2017)

Στο IPv4 το μέγιστο θεωρητικά μέγεθος του πακέτου είναι 65.635 bytes. Πρακτικά, τα πακέτα είναι μικρότερα σε μέγεθος εξαιτίας του MTU, δηλαδή του μέγιστης μονάδας μεταφοράς που υποστηρίζει

ο κάθε σύνδεσμος. Και στα δύο πρωτόκολλα το MTU είναι το συνολικό μήκος του πακέτου, όπως φαίνεται στην Εικόνα 8. Το IPv6 έχει τη δυνατότητα να μεταφέρει περισσότερα δεδομένα. Αυτός ο τύπος των πακέτων ονομάζεται jumbograms και περιγράφεται στο RFC 2675 (Borman, Deering and Hinden, 1999). Ένα jumbogram με τη βοήθεια μιας επιλογής, της Jumbo Payload σε μία από τις επικεφαλίδες επέκτασης -την Hop-by-Hop που θα δούμε στην επόμενη παράγραφο, μπορεί να έχει μέγεθος από 65.635 μέχρι 4.294.967.295 (2^{32}−1) bytes.

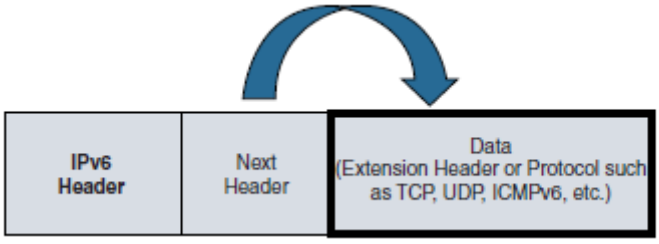


Εικόνα 8. Τα MTU του IPv4 και του IPv6

Πηγή: (Graziani, 2017)

Τα πεδία *Αναγνώριση Ταυτότητας (Identification), Δυαδικοί δείκτες (Flags), Μετατόπιση Τεμαχίου (Fragment Offset)* του IPv4 που αφορούν πληροφορίες για την κατάτμηση των IP πακέτων, δεν υπάρχουν στο IPv6. Αυτό γιατί ο τρόπος κατάτμησης των πακέτων είναι διαφορετικός. Το IPv4 απαιτεί από κάθε κόμβο να μπορεί να προωθήσει πακέτα 68 bytes χωρίς περαιτέρω κατάτμηση. Αυτό συμβαίνει γιατί η επικεφαλίδα του IPv6 μπορεί να καταλάβει μέχρι 60 bytes, κάτι που σημαίνει ότι τα δεδομένα μπορεί να καταλαμβάνουν 8 bytes. Το IPv6 απαιτεί από κάθε σύνδεσμο να έχει ένα ελάχιστο MTU 1280 bytes, με συνιστώμενο μέγεθος 1500 bytes, σε σύγκριση με τα 68 bytes του IPv4. Η σχεδίαση του IPv4 προβλέπει κατακερματισμό τον πακέτων στην πηγή ή σε οποιοδήποτε σύνδεσμο της διαδρομής προς τον προορισμό, σε αντίθεση με το IPv6, όπου ο κατακερματισμός των πακέτων γίνεται μόνο στην πηγή με τη βοήθεια επικεφαλίδων επέκτασης,, όπως θα δούμε παρακάτω.

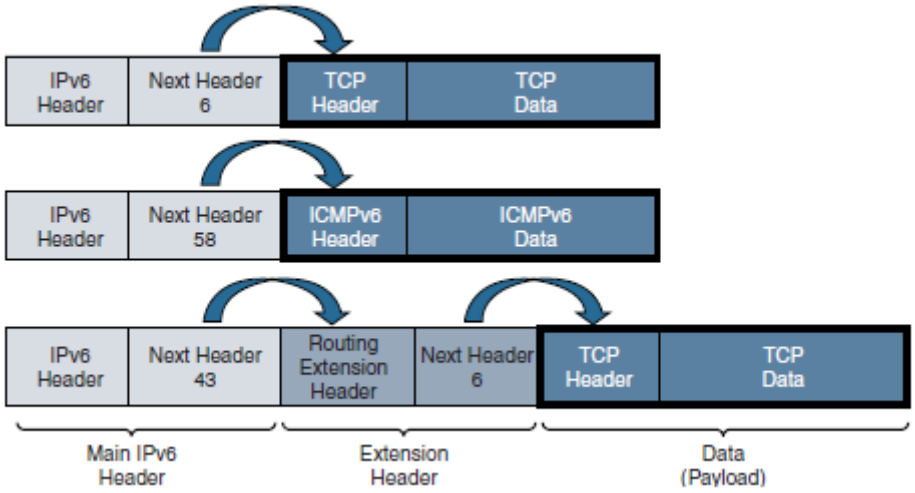
Το πεδίο ***Επόμενη Επικεφαλίδα (Next Header)*** του IPv6 έχει παρόμοια λειτουργία με το πεδίο *Πρωτόκολλο (Protocol)* του IPv4, ορίζει τον τύπο της επικεφαλίδας που αναμένεται μετά την κύρια επικεφαλίδα, αλλά υπάρχει και μία πρόσθετη επιλογή σε σχέση με το IPv4. Το πεδίο Πρωτόκολλο του IPv4 χρησιμοποιείται όταν ένα IP πακέτο πλησιάζει στον προορισμό του και προσδιορίζει το πρωτόκολλο του επιπέδου μεταφοράς στο οποίο θα διαβιβαστεί η πληροφορία του IP πακέτου. Οι τιμές των διάφορων πρωτόκολλων ορίζονται στο RFC 1700 (Reynolds and Postel, 1994). 'Ετσι, εάν πρόκειται το πακέτο να περάσει στο TPC η τιμή αυτή έχει προκαθοριστεί να είναι ίση με 6, ενώ για το UDP είναι 17. Σε περίπτωση που σε ένα πακέτο IPv6 δεν υπάρχουν επικεφαλίδες επέκτασης, το πεδίο Επόμενη Ετικέτα λειτουργεί όπως το πεδίο Πρωτόκολλο του IPv4. Το πεδίο Επόμενη Επικεφαλίδα φαίνεται πως δείχνει σε μια επικεφαλίδα επέκτασης στην Εικόνα 9.



Εικόνα 9. Το πεδίο Επόμενη Επικεφαλίδα (Next Header) του IPv6.

Πηγή: (Graziani, 2017)

Το πεδίο Επόμενη Επικεφαλίδα παίρνει διάφορες τιμές και κάθε μία αντιστοιχεί και σε μία διαφορετική λειτουργία. Συνήθως, η πληροφορία που ακολουθεί μετά την κύρια επικεφαλίδα είναι τα δεδομένα του πακέτου, όπως για παράδειγμα ένα TCP τμήμα (segment) εφόσον η επόμενη επικεφαλίδα έχει την τιμή 6. Για διάφορες άλλες τιμές, μπορεί να «δείχνει» (point) σε μια επικεφαλίδα επέκτασης και να ακολουθούν άλλες λειτουργίες, όπως για παράδειγμα φαίνεται στην Εικόνα 10. Οι σημαντικότερες διαφορετικές τιμές που παίρνει το πεδίο δίνονται από τον Graziani (2017). Περισσότερα για αυτό το πεδίο, παρουσιάζονται στην επόμενη παράγραφο.



Εικόνα 10. Παραδείγματα Επόμενης Επικεφαλίδας (Next Header) του IPv6

Πηγή: (Graziani, 2017)

Το πεδίο ***Όριο Άλματος (Hop Limit)*** του IPv6 και το πεδίο *Χρόνος Ζωής Πακέτου (Time to Live – TTL)* του IPv4 διασφαλίζουν ότι ένα πακέτο δεν θα «περιφέρεται» επ'αόριστον μέσα στο δίκτυο σε περίπτωση που δημιουργηθεί ένας βρόγχος στον δρομολογητή. Το πεδίο αυτό είναι στην ουσία ένας απαριθμητής που παίρνει μια αρχική τιμή, η οποία μειώνεται κατά 1 κάθε φορά που ένας δρομολογητής λαμβάνει το πακέτο. Όταν η τιμή γίνει 0, τότε το πακέτο καταστρέφεται.

Το πεδίο *'Άθροισμα Ελέγχου Επικεφαλίδας (Header Checksum)* του IPv4 καταργήθηκε από στο IPv6. Οι σχεδιαστές του IPv6 έκριναν περιττή την ύπαρξη αυτού του πεδίου, γιατί ο έλεγχος ορθότητας πραγματοποιείται στα πρωτόκολλα του επιπέδου μεταφοράς (πχ TCP ή UDP) και συνδέσμου (πχ Ethernet) της στοίβας πρωτοκόλλων TCP/IP. Το IP είναι ένα πρωτόκολλο «καλύτερης προσπάθειας», οπότε αυτή η λειτουργικότητα πρέπει να υπάρχει σε άλλα πρωτόκολλα. Ο έλεγχος ορθότητας στο IPv6 περιγράφεται στο RFC 2460 (Deering and Hinden, 1998).

Τα πεδία ***Διεύθυνση Πηγής (Source Address)*** και ***Διεύθυνση Προορισμού (Destination Address)*** υπάρχουν και στις δύο εκδόσεις, αλλά με μια σημαντική διαφορά: την επέκταση της διεύθυνσης από τα 32 bits στο IPv4 στα 128 bits στο IPv6. Η λειτουργικότητα παραμένει η ίδια.

Το πεδίο *Επιλογές (Options)* του IPv4 δεν είναι πλέον μέρος της IPv6 επικεφαλίδας, γιατί η λειτουργικότητά του μεταφέρθηκε κατά κάποιο τρόπο στο πεδίο επόμενη επικεφαλίδα, κάτι που είχε ως αποτέλεσμα την σταθερού μήκους 40 bytes επικεφαλίδα του IPv6.

Στην επόμενη παράγραφο παρουσιάζονται οι επικεφαλίδες επέκτασης του IPv6.

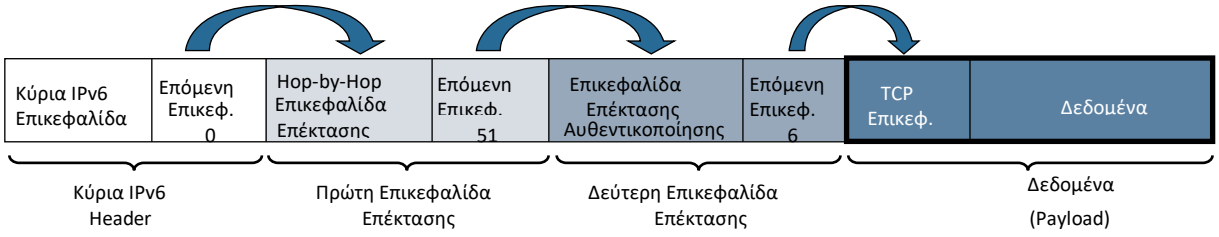
2.2 Οι επικεφαλίδες επέκτασης του IPv6

Μια σημαντική προσθήκη στο IPv6 αποτελούν οι ***επικεφαλίδες επέκτασης (extension headers)*** οι οποίες είναι προαιρετικές και ακολουθούν την κύρια επικεφαλίδα του IPv6. Προσθέτουν ευελιξία γιατί βοηθούν σε μελλοντικές επεκτάσεις του πρωτοκόλλου χωρίς να χρειαστεί επανασχεδιασμός ολόκληρου του πρωτοκόλλου. Το πεδίο Επόμενη Επικεφαλίδα (Next Header), όπως ήδη αναφέρθηκε, εξυπηρετεί δύο σκοπούς. Ο πρώτος αφορά την αναγνώριση του πρωτόκολλου που φέρει το τμήμα δεδομένων του πακέτου, όπου κάτι παρόμοιο υπάρχει στο πεδίο Πρωτόκολλο (Protocol) του IPv4. Ο δεύτερος σκοπός αφορά μία από τις σημαντικότερες προσθήκες που υπάρχουν στη επικεφαλίδα του IPv6: το πεδίο επόμενη επικεφαλίδα δείχνει στο πεδίο των επικεφαλίδων επέκτασης (Extension Headers), το οποίο είναι προαιρετικό, ακολουθεί την υποχρεωτική κύρια επικεφαλίδα του IPv6 και μπορεί να περιλαμβάνει από μηδέν έως αρκετές επικεφαλίδες επέκτασης. Ένα κοινό πεδίο σε όλες τις επικεφαλίδες επέκτασης είναι ένα άλλο πεδίο, το πεδίο Επόμενης Ετικέτας (Next Header), το οποίο υποδεικνύει εάν ακολουθεί μια άλλη επικεφαλίδα επέκτασης ή εάν ακολουθεί το πρωτόκολλο του payload, όπως για παράδειγμα ένα TCP τμήμα, όπως φαίνεται στην Εικόνα 10. Έτσι, η τελευταία επικεφαλίδα επέκτασης καθορίζει συνήθως ποιο πρωτόκολλο ενθυλακώνεται ως δεδομένα ή payload, όπως ισχύει για το πεδίο πρωτόκολλο (Protocol) του IPv4 (Graziani, 2017).

Όπως ήδη αναφέραμε, οι σχεδιαστές του IPv6 είχαν, μεταξύ των άλλων, ως σκοπό τη βελτίωση του IP πρωτόκολλου για τις συσκευές που διαθέτουν 64-bit CPUs. Όπως συμβαίνει με την κύρια επικεφαλίδα του IPv6, έτσι και οι επικεφαλίδες επέκτασης είναι προκαθορισμένου μήκους και πολλαπλάσια των 64 bits. Σε περίπτωση που το μήκος είναι μικρότερο από τα 64 bits, τότε γίνεται το παραγέμισμα (padding) (Graziani, 2017).

Στον Πίνακα 2 συνοψίζονται οι επικεφαλίδες επέκτασης, έτσι όπως ορίζονται στο RFC 2460. Δεν περιλαμβάνεται η επικεφαλίδα επέκτασης No Next Header με δεκαδική τιμή 59, γιατί είναι η μοναδική επικεφαλίδα επέκτασης που δεν δείχνει σε κάποιο πρωτόκολλο ή σε μια άλλη επικεφαλίδα επέκτασης.

Στο RFC 2460 συνιστάται, εφόσον στο ίδιο πακέτο χρησιμοποιούνται περισσότερες από μία επικεφαλίδες επέκτασης, να μπαίνουν σε συγκεκριμένη σειρά όπως αναφέρονται στον Πίνακα 2, και τελευταία να μπαίνει η επικεφαλίδα που ορίζει το πρωτόκολλο. Δηλαδή, εάν για παράδειγμα υπάρχουν οι επικεφαλίδες επέκτασης Hop-by-Hop και η επικεφαλίδα αυθεντικοποίησης (AH) και το πρωτόκολλο μεταφοράς είναι το TCP, τότε θα μπει πρώτα η επικεφαλίδα επέκτασης Hop-by-Hop, θα ακολουθήσει η επικεφαλίδα επέκτασης AH και τέλος θα μπει το πρωτόκολλο μεταφοράς. Αυτό το παράδειγμα φαίνεται στην Εικόνα 11, όπου βλέπουμε ότι πρώτα μπαίνει η κύρια επικεφαλίδα του IPv6 η οποία περιέχει όλα τα πεδία που περιγράψαμε. Στο πεδίο Επόμενη Επικεφαλίδα υπάρχει η τιμή 0, πράγμα που σημαίνει ότι μετά την κύρια επικεφαλίδα θα ακολουθήσει η επικεφαλίδα επέκτασης Hop-by-Hop, η οποία με τη σειρά της περιλαμβάνει το δικό της πεδίο Επόμενη Επικεφαλίδα με την τιμή 51, πράγμα που σημαίνει ότι θα ακολουθήσει η επικεφαλίδα επέκτασης Αυθεντικοποίησης. Στο πεδίο Επόμενη Επικεφαλίδα της Αυθεντικοποίησης υπάρχει τη τιμή 6, πράγμα που σημαίνει ότι ακολουθεί μια TCP ανωτέρου επιπέδου επικεφαλίδα και δεν υπάρχουν άλλες επικεφαλίδες επέκτασης (Graziani, 2017).



Εικόνα 11. Παράδειγμα IPv6 πακέτου με δύο επικεφαλίδες επέκτασης

Πίνακας 2. Οι επικεφαλίδες επέκτασης του IPv6

Τιμή επόμενης επικεφαλίδας (Δεκαδική)	Ονομασία επικεφαλίδας επέκτασης	Μήκος επικεφαλίδας επέκτασης (Bytes)	Χρήση Επιλογών Μεταβλητού Μήκους (TLV)	Περιγραφή επικεφαλίδας επέκτασης
0	Επιλογές Hop-by-Hop (Hop-by-Hop Options)	Μεταβλητό	Ναι	Χρησιμοποιείται για τη μεταφορά προαιρετικής πληροφορίας, η οποία πρέπει να εξεταστεί από κάθε δρομολογητή κατά τη διαδρομή του πακέτου
43	Δρομολόγηση (Routing)	Μεταβλητό	Όχι	Επιτρέπει την πηγή του πακέτου να προσδιορίσει τη διαδρομή προς τον προορισμό
44	Τεμάχιο (Fragment)	8	Όχι	Χρησιμοποιείται για την κατάτμηση των IPv6 πακέτων
50	Ενσωματωμένα Δεδομένα Ασφάλειας (Encapsulating Security Payload -ESP)	Μεταβλητό	Όχι	Χρησιμοποιείται για να παρέχει αυθεντικοποίηση, ακεραιότητα και κρυπτογράφηση
51	Επικεφαλίδα Αυθεντικοποίησης (Authentication Header -AH)	Μεταβλητό	Όχι	Χρησιμοποιείται για να παρέχει αυθεντικοποίηση, ακεραιότητα

Τιμή επόμενης επικεφαλίδας (Δεκαδική)	Ονομασία επικεφαλίδας επέκτασης	Μήκος επικεφαλίδας επέκτασης (Bytes)	Χρήση Επιλογών Μεταβλητού Μήκους (TLV)	Περιγραφή επικεφαλίδας επέκτασης
60	Επιλογές Προορισμού (Destination Options)	Μεταβλητό	Όχι	Χρησιμοποιείται για τη μεταφορά προαιρετικής πληροφορίας που χρειάζεται να εξεταστεί μόνο από τον κόμβο προορισμού του πακέτου

Στη συνέχεια θα αναλύσουμε τις επικεφαλίδες επέκτασης με τη σειρά που εμφανίζονται στον Πίνακα 2.

2.2.1 Η επικεφαλίδα επέκτασης Επιλογές Hop-by-Hop (Hop-by-Hop Options)

Η επικεφαλίδα επέκτασης ***Επιλογές Hop-by-Hop (Hop-by-Hop Options)*** χρησιμοποιείται για να παρέχει προαιρετική πληροφορία η οποία θα πρέπει να εξετάζεται από κάθε δρομολογητή κατά τη διαδρομή του πακέτου από την πηγή προς τον προορισμό. Παλαιότερα ήταν υποχρεωτική, αλλά στη συνέχεια έγινε προαιρετική, οπότε δεν είναι υποχρεωτική αυτή η εξέταση σε κάθε δρομολογητή. Η επικεφαλίδα επέκτασης Επιλογές Hop-by-Hop είναι μία από τις δύο επικεφαλίδες επέκτασης που περιέχουν επιλογές ποικίλου μεγέθους του πεδίου, παρόμοια με το IPv4 (Graziani, 2017). Η άλλη είναι η επικεφαλίδα επέκτασης Επιλογές Προορισμού (Destination Options) την οποία και θα εξετάσουμε ξεχωριστά.

Οι επιλογές παρέχουν ευελιξία, επιτρέποντας στα πακέτα IPv6 να συμπληρώνονται με σύνολα τιμών που δεν ορίζονται στην τυπική ομάδα των επικεφαλίδων επέκτασης. Αυτά τα σύνολα τιμών αναφέρονται επίσης ως το τρίδυμο ***Τύπος-Μήκος-Τιμή (Type-Length-Value -TLV)***.

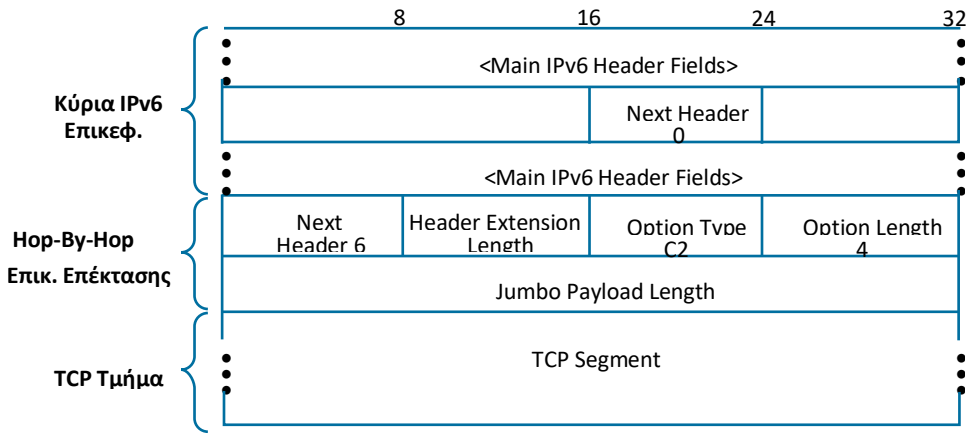
Η επικεφαλίδα επέκτασης Επιλογές Hop-by-Hop υποδεικνύεται στο πεδίο Επόμενη Επικεφαλίδα με τον δεκαδικό αριθμό 0. Περιλαμβάνει ένα πεδίο Επόμενης Επικεφαλίδας (Next Header), ένα πεδίο Μήκους Επικεφαλίδας Επέκτασης (Header Extension Length) και ακολουθούν μία ή περισσότερες ομάδες επιλογών. Κάθε επιλογή περιέχει μια ομάδα από τον Τύπο Επιλογών (Options Type), το Μήκος Επιλογών (Options Length) και πεδία Επιλογών Δεδομένων (Options Data), δηλαδή το τρίδυμο TLV (Graziani, 2017).

Γενικά, η επικεφαλίδα επέκτασης Hop-by-Hop μπορεί να περιέχει τις παρακάτω επιλογές:

- **Pad1**: Παρέχει 1-byte γεμίσματος (padding).
- **PadN**: Χρησιμοποιείται όταν χρειάζονται 2 ή περισσότερα bytes για το γέμισμα.
- **Jumbo Payload Length**: Υποδεικνύει ότι το μέγεθος του IPv6 πακέτου, ένα jumbogram, είναι μεγαλύτερο από 65,535 bytes.
- **Router Alert**: Ενημερώνει τους δρομολογητές για να εξετάσουν προσεκτικά τα περιεχόμενα ενός πακέτου IPv6. Αυτή η επιλογή είναι χρήσιμη για καταστάσεις στις οποίες ένα πακέτο περιέχει πληροφορίες που απαιτούν ειδική επεξεργασία από τους δρομολογητές κατά μήκος της διαδρομής.

Ως παράδειγμα μιας επικεφαλίδας επέκτασης Επιλογές Hop-by-Hop θα παρουσιάσουμε την επικεφαλίδα επέκτασης για την Επιλογή Ωφέλιμου Φορτίου Jumbo (Jumbo Payload Option), που φαίνεται στην Εικόνα 12 (Graziani, 2017).

Η Επιλογή Jumbo Payload χρησιμοποιείται για να υποδείξει ότι το μέγεθος ενός jumbogram πακέτου είναι μεγαλύτερο από 65.535 bytes. Επειδή πρόκειται για μια Επιλογή Hop-by-Hop, αυτή η πληροφορία θα πρέπει να εξεταστεί από κάθε δρομολογητή κατά μήκος της διαδρομής του πακέτου.



Εικόνα 12. Η επικεφαλίδα επέκτασης Hop-by-Hop για την Επιλογή Jumbo Payload

Παρακάτω, περιγράφονται τα πεδία που σχετίζονται με την επικεφαλίδα επέκτασης Hop-by-Hop, όπως φαίνονται στην Εικόνα 12:

- **Η κύρια IPv6 επικεφαλίδα**: Μαζί με άλλες πληροφορίες στην κύρια επικεφαλίδα IPv6, υπάρχει ένα πεδίο Next Header με την τιμή 0. Αυτό δείχνει ότι μια κεφαλίδα επέκτασης Επιλογών Hop-by-Hop ακολουθεί αυτήν την κύρια επικεφαλίδα.
- **Η επικεφαλίδα επέκτασης Hop-by-Hop** που περιέχει τα ακόλουθα:
    - *Επόμενη επιφυλλίδα -8 bits:* Η τιμή 6 στο πεδίο Επόμενη Επικεφαλίδα υποδεικνύει ότι αυτήν την επικεφαλίδα την ακολουθεί μια TCP επικεφαλίδα, οπότε δεν υπάρχουν άλλες επικεφαλίδες επέκτασης.
    - *Μήκος Επικεφαλίδας Επέκτασης (Header Extension Length) -8 bits:* Αυτό είναι το μήκος της επικεφαλίδας Επιλογές Hop-by-Hop. Μπορεί να υπάρχουν πολλαπλές επιλογές και κάθε επιλογή θα αποτελείται από το τρίδυμο TLV.
    - *Τύπος Επιλογής (Option Type) -8 bits:* Αυτός είναι ο τύπος της επιλογής που μεταφέρεται σε αυτή την επικεφαλίδα και έχει την δεκαεξαδική τιμή C2 που υποδεικνύει ότι, πρόκειται για μια Επιλογή Jumbo Payload.

- *Επιλογή Μήκος Δεδομένων (Option Data Length) -8 bits:* Αυτός είναι ο αριθμός των bytes στο πεδίο Επιλογή Δεδομένων. Η τιμή 4 υποδεικνύει ότι το πεδίο έχει μήκος 4 bytes (32 bits).
- *Επιλογή Δεδομένα (Option Data) -μεταβλητού μήκους:* Τα δεδομένα σε αυτό το παράδειγμα είναι το Μήκος του Jumbo Payload (Jumbo Payload Length) το οποίο είναι ένα πεδίο 32-bit που υποδεικνύει το μέγεθος του IPv6 πακέτου σε bytes, εξαιρώντας την IPv6 επικεφαλίδα, αλλά συμπεριλαμβανομένης της επικεφαλίδας επέκτασης Επιλογές Hop-by-Hop και οποιονδήποτε άλλων επικεφαλίδων επέκτασης που υπάρχουν. Το μήκος του Jumbo Payload πρέπει να τουλάχιστον 65.535 bytes και το μέγιστο μήκος είναι 4.294.967.295 bytes.

- **Τμήμα TCP (TCP Segment):** Επειδή υπάρχει μόνο μια επιλογή και δεν υπάρχουν άλλες επικεφαλίδες επέκτασης, ακολουθεί ένα τμήμα TCP, όπως υποδεικνύεται από την τιμή 6 που υπάρχει στο πεδίο Επόμενη Επικεφαλίδα της προηγούμενης επικεφαλίδας επέκτασης Hop-by-Hop. Εάν χρησιμοποιείται μια επικεφαλίδα επέκτασης Hop-by-Hop Options, τότε αυτή πάντα ακολουθεί την κύρια IPv6 επικεφαλίδα.

2.2.2 Η επικεφαλίδα επέκτασης Δρομολόγηση (Routing)

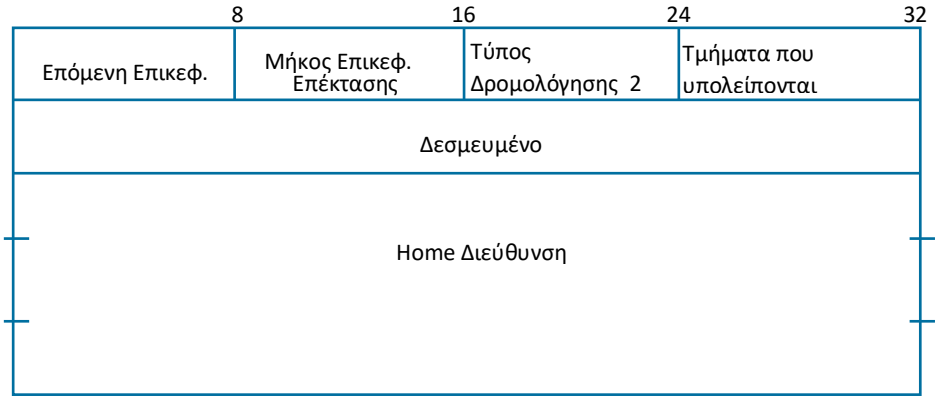
Η επικεφαλίδα επέκτασης ***Δρομολόγηση (Routing)*** επιτρέπει στην πηγή του πακέτου να ορίσει τη διαδρομή προς τον προορισμό. Περιέχει έναν κατάλογο από έναν ή περισσότερους δρομολογητές προς την κατεύθυνση του προορισμού του πακέτου. Η λειτουργία αυτή είναι παρόμοια με μια προαιρετική λειτουργία δρομολόγησης του IPv4, την Loose Source route[2]. Η επικεφαλίδα επέκτασης Δρομολόγηση υποδεικνύεται από τη δεκαδική τιμή 43 στο πεδίο Επόμενη Επικεφαλίδα (Graziani, 2017).

[2] Περισσότερες πληροφορίες για αυτή τη λειτουργία δρομολόγησης δίνονται στην (Wikipedia the free encyclopedia, 2021b)

Υπάρχουν τέσσερις Τύποι (Types) επικεφαλίδων επέκτασης, καθώς και ένας τύπος ο οποίος καταργήθηκε και είναι οι εξής:

- **Τύπος 0:** Καταργήθηκε για λόγους ασφάλειας
- **Τύπος 1:** Χρησιμοποιείται για το Nimrod, ένα έργο που χρηματοδοτείται από την DARPA.
- **Τύπος 2:** Χρησιμοποιείται για το Mobile IPv6.
- **Τύπος 3:** Χρησιμοποιείται για την εκχώρηση του αλγόριθμου δρομολόγησης και των παραμέτρων που εφαρμόζονται σε ένα anycast πακέτο.
- **Τύπος 4:** Χρησιμοποιείται για δρομολόγηση τμημάτων (segment).

Ως παράδειγμα μιας επικεφαλίδας επέκτασης Δρομολόγηση, στην Εικόνα 13 φαίνεται η δομή ενός Τύπου 2 επικεφαλίδας Δρομολόγησης που χρησιμοποιείται για την υποστήριξη της κινητικότητας στο IPv6. Αυτή η επικεφαλίδα επέκτασης, παρέχει την πληροφορία για την τρέχουσα θέση του κινητού κόμβου (Graziani, 2017).



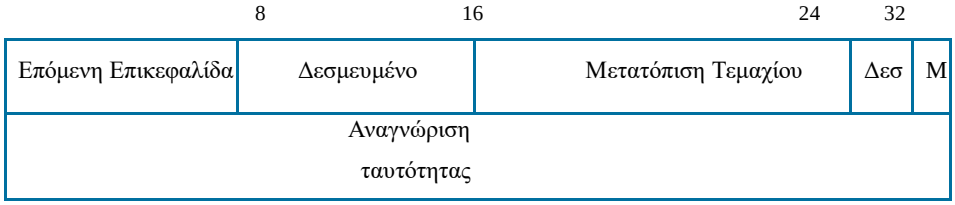
Εικόνα 13.Η Τύπου 2 επικεφαλίδα επέκτασης Δρομολόγησης.

Τα πεδία που σχετίζονται με την επικεφαλίδα επέκτασης Δρομολόγησης Τύπου 2 είναι τα παρακάτω:

- **Επόμενη Επικεφαλίδα (Next Header) -8 bits**: Προσδιορίζει τον τύπο της επικεφαλίδας αμέσως μετά την επικεφαλίδα Δρομολόγησης. Είναι είτε μια άλλη επικεφαλίδα επέκτασης, είτε το πρωτόκολλο του payload.
- **Μήκος Επικεφαλίδας Επέκτασης (Header Extension Length) -8 bits**: Αυτό είναι το μήκος της κεφαλίδας δρομολόγησης σε μονάδες των 8 οκτάδων (octets), εκτός από τις πρώτες 8 οκτάδες.
- **Τύπος Δρομολόγησης (Routing Type) - 8 bits**: Αυτή η τιμή είναι 2.
- **Τμήματα που υπολείπονται (Segments Left) -8 bits**: Αυτή η τιμή είναι 1.
- **Δεσμευμένο (Reserved) -32 bits:** Το πεδίο αυτό είναι δεσμευμένο. Αρχικοποιείται στο 0 για τη μετάδοση και αγνοείται κατά τη λήψη.
- **Home Διεύθυνση (Home Address) -128 bits**: Είναι η home διεύθυνση του προορισμού του κινητού κόμβου. Αυτό το πεδίο είναι συγκεκριμένο για το mobile IPv6 που ορίζεται από το RFC 3775 (Perkins, Arkko and Johnson, 2004).

2.2.3 Η επικεφαλίδα επέκτασης Τεμάχιο (Fragment)

Η επικεφαλίδα επέκτασης ***Τεμάχιο (Fragment),*** όπως φαίνεται στην Εικόνα 14, είναι παρόμοια με τα πεδία που χρησιμοποιούνται στα πεδία της επικεφαλίδας του IPv4 για την κατάτμηση. Η επικεφαλίδα επέκτασης Τεμάχιο υποδεικνύεται από τη δεκαδική τιμή 44 στο πεδίο Επόμενη Επικεφαλίδα. Χρησιμοποιείται όταν η πηγή του πακέτου IPv6 πρέπει να κατακερματίσει το πακέτο σε τεμάχια και να στείλει κάθε τεμάχιο ως ξεχωριστό πακέτο. Ο παραλήπτης του πακέτου συναρμολογεί ξανά τα τεμάχια, το καθένα με τη δική του κύρια επικεφαλίδα IPv6 και μια επικεφαλίδα επέκτασης Τεμάχιο (Graziani, 2017).



Εικόνα 14. Η επικεφαλίδα Τεμάχιο (Fragment Header)

Σε αντίθεση με το IPv4, στο IPv6 ένας δρομολογητής δεν κατακερματίζει ένα πακέτο, εκτός εάν είναι η πηγή του πακέτου. Οι ενδιάμεσοι κόμβοι δεν εκτελούν κατακερματισμό. Μόνο η πηγή του πακέτου μπορεί να πραγματοποιήσει τον κατακερματισμό. Εάν ένας δρομολογητής λάβει ένα πακέτο IPv6 που είναι μεγαλύτερο από το MTU της διεπαφής εξόδου, ο δρομολογητής απορρίπτει το πακέτο και στέλνει ένα μήνυμα σφάλματος του πρωτόκολλου ICMPv6 (πιο συγκεκριμένα το μήνυμα «Packet Too Big») πίσω στην πηγή (Graziani, 2017).

Παρόμοια με το IPv4, στο IPv6 για κάθε πακέτο που θα κατακερματιστεί, η πηγή δημιουργεί ένα μοναδικό αναγνωριστικό (identification). Αυτό το αναγνωριστικό περιλαμβάνεται σε κάθε ένα από τα πακέτα κατακερματισμού και διασφαλίζει ότι, τα τμήματα του αρχικού πακέτου θα συναρμολογούνται σωστά. Εάν η πηγή πρέπει να κατακερματίσει επιπλέον πακέτα μέσα στο ίδιο μήνυμα, χρησιμοποιούνται διαφορετικά αναγνωριστικά (Graziani, 2017).

Αναλυτικά, τα πεδία που αποτελούν την επικεφαλίδα επέκτασης Τεμάχιο, όπως φαίνεται στην Εικόνα 14 και είναι τα παρακάτω (Graziani, 2017):

- **Επόμενη Επικεφαλίδα (Next Header) -8 bits**: Προσδιορίζει τον αριθμό πρωτοκόλλου των δεδομένων, το κατακερματισμένο μέρος του αρχικού πακέτου.
- **Δεσμευμένο (Reserved) -8 bits**: Είναι δεσμευμένο πεδίο και αρχικοποιείται στο 0 για την μετάδοση και αγνοείται κατά την παραλαβή.
- **Μετατόπιση Τεμαχίου (Fragment Offset) -13 bits**: Είναι η σχετική μετατόπιση ή θέση (σε μονάδες 8 οκτάδων) των κατακερματισμένων δεδομένων που ακολουθούν αυτήν την επικεφαλίδα, σε σχέση με το αρχικό πακέτο. Όπως το πεδίο Fragment Offset στο IPv4, το πεδίο αυτό ενημερώνει τον παραλήπτη πού να ευθυγραμμίσει το κατακερματισμένο πακέτο σε σχέση με τα άλλα κατακερματισμένα πακέτα.
- **Δεσμευμένο- Δες (Reserved) -2 bits**: Είναι δεσμευμένο πεδίο και αρχικοποιείται στο 0 για την μετάδοση και αγνοείται κατά την παραλαβή.

- **Μ σημαία (M flag) -1 bit:** Η Μ σημαία (More Fragments flag) χρησιμοποιείται για να υποδείξει εάν αυτό είναι το τελευταίο τμήμα λαμβάνοντας την τιμή 0 ή αν ακολουθούν και άλλα τεμάχια οπότε λαμβάνει την τιμή 1. Το πεδίο αυτό είναι παρόμοιο με τη σημαία More Fragments του IPv4.
- **Αναγνώριση ταυτότητας (Identification) -32 bits**: Είναι παρόμοιο με το πεδίο Identification στην επικεφαλίδα του IPv4. Χρησιμοποιείται για τον μοναδικό προσδιορισμό όλων των κατακερματισμένων πακέτων εντός του ίδιου αρχικού πακέτου. Το πεδίο έχει επεκταθεί στο IPv6 στα 32 bits από τα 16 bit που καταλάμβανε στο IPv4.

2.2.4 Οι επικεφαλίδες επέκτασης Ενσωματωμένα Δεδομένα Ασφάλειας (Encapsulating Security Payload -ESP) και Επικεφαλίδα Αυθεντικοποίησης (Authentication Header -AH)

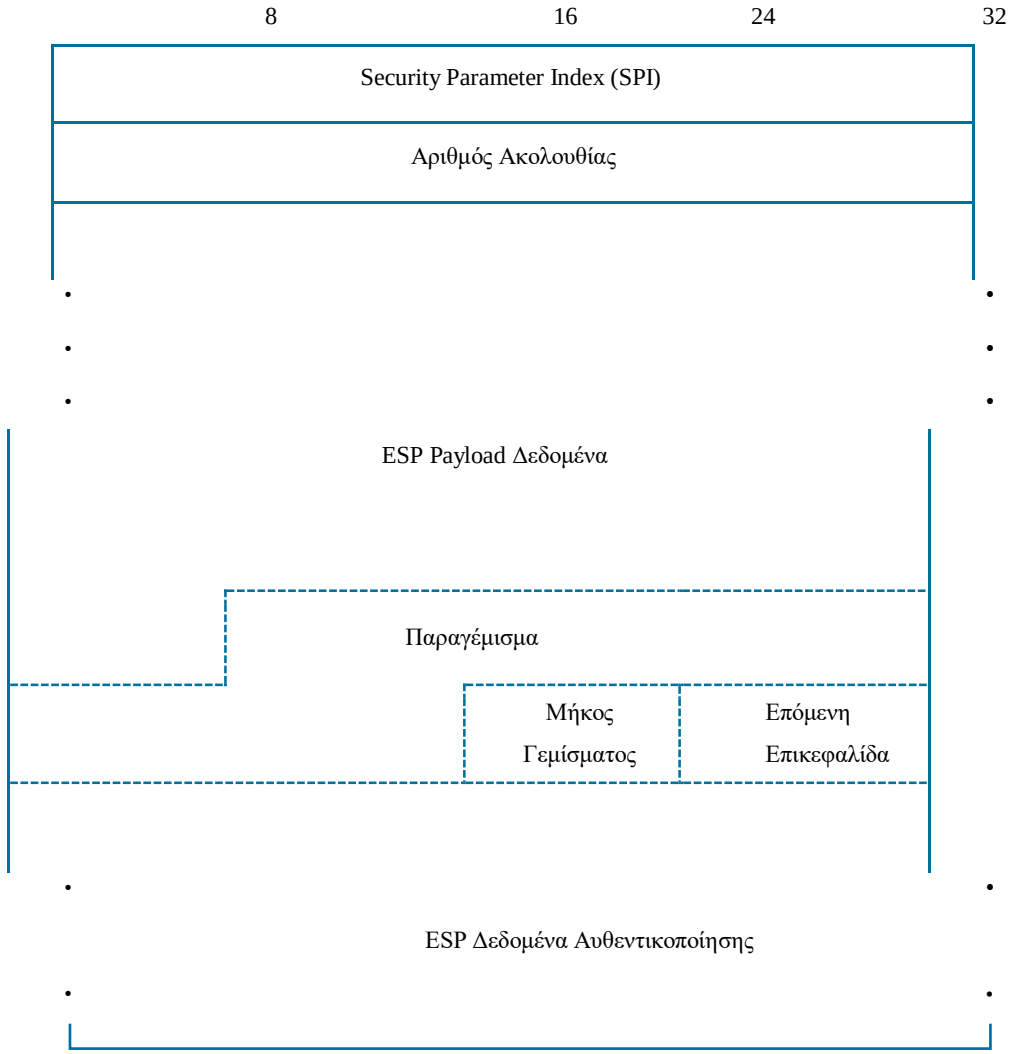
Οι επικεφαλίδες επέκτασης ***Ενσωματωμένα Δεδομένα Ασφάλειας (Encapsulating Security Payload -ESP)*** και ***Επικεφαλίδα Αυθεντικοποίησης (Authentication Header -AH)*** χρησιμοποιούνται για την εφαρμογή δύο βασικών πρωτοκόλλων ασφαλείας στην οικογένεια των πρωτόκολλων του IPsec, η οποία δημιουργήθηκε για την ασφαλή διανομή των πακέτων στα IP δίκτυα.

Η Επικεφαλίδα Αυθεντικοποίησης (AH) χρησιμοποιείται για να εγγυηθεί την αυθεντικοποίηση (authentication) και την ακεραιότητα (integrity) ενός πακέτου. Η αυθεντικοποίηση σημαίνει την επιβεβαίωση ότι ο αποστολέας και ο παραλήπτης του πακέτου είναι πράγματι αυτοί που ισχυρίζονται ότι είναι. Η ακεραιότητα εγγυάται ότι τα δεδομένα δεν αλλοιώνονται κατά τη μεταφορά. Η AH δεν παρέχει κρυπτογράφηση (encryption). Η κρυπτογράφηση είναι η διαδικασία της μετατροπής της πληροφορίας (η οποία είναι συνήθως σε απλό κείμενο - plain text) με τη χρήση ενός κρυπτογραφικού αλγόριθμου σε κρυπτογράφημα (cipher) έτσι ώστε να μην είναι αναγνώσιμη από οποιονδήποτε, παραμόνο από αυτόν που κατέχει μια ειδική πληροφορία (που συνήθως αναφέρεται ως το κλειδί- key) (Graziani, 2017).

Η Ενθυλακωμένη Ασφάλεια Payload (Encapsulating Security Payload -ESP) παρέχει αυθεντικοποίηση, ακεραιότητα και κρυπτογράφηση. Η ESP προστατεύει το πακέτο από την αλλοίωση από άλλες συσκευές, αλλά και την ορατότητα του περιεχομένου του πακέτου. Έχει το δικό της σχήμα αυθεντικοποίησης ή μπορεί να χρησιμοποιηθεί σε συνδυασμό με την AH. Συνοπτικά, η AH παρέχει μόνο αυθεντικοποίηση και ακεραιότητα, ενώ η ESP παρέχει και την κρυπτογράφηση των πακέτων. Ο τρόπος με τον οποίο γίνεται η αυθεντικοποίηση ή η κρυπτογράφηση εξαρτάται από την κατάσταση λειτουργίας (mode) που χρησιμοποιείται το IPsec. Χωρίς να μπούμε προς το παρόν σε άλλες λεπτομέρειες διότι είναι εκτός σκοπού της εργασίας, αναφέρουμε ότι υπάρχουν δύο καταστάσεις λειτουργίας του IPsec: η κατάσταση λειτουργίας μεταφοράς (transport mode) και η κατάσταση λειτουργίας σήραγγας (tunnel mode) (Graziani, 2017).

Η ESP είναι επικεφαλίδα επέκτασης μεταβλητού μήκους και υποδεικνύεται από τη δεκαδική τιμή 50 στο πεδίο Επόμενη Επικεφαλίδα. Όπως φαίνεται στην Εικόνα 15, η επικεφαλίδα επέκτασης ESP χωρίζεται σε τέσσερα μέρη, όπως φαίνεται στην Εικόνα 15 (Graziani, 2017):

- **ESP Επικεφαλίδα:** Περιλαμβάνει τα πεδία SPI και Αριθμός Ακολουθίας (Sequence Number)
- **Ωφέλιμο φορτίο (Payload):** Περιέχει το πεδίο ESP Payload Δεδομένα (ESP Payload Data)
- **ESP ουρά (Trailer):** Περιλαμβάνει τα πεδία Παραγέμισμα (Padding), Μήκος Γεμίσματος (Pad Length), και Επόμενη Επικεφαλίδα (Next Header)
- **ESP Δεδομένα Αυθεντικοποίησης**

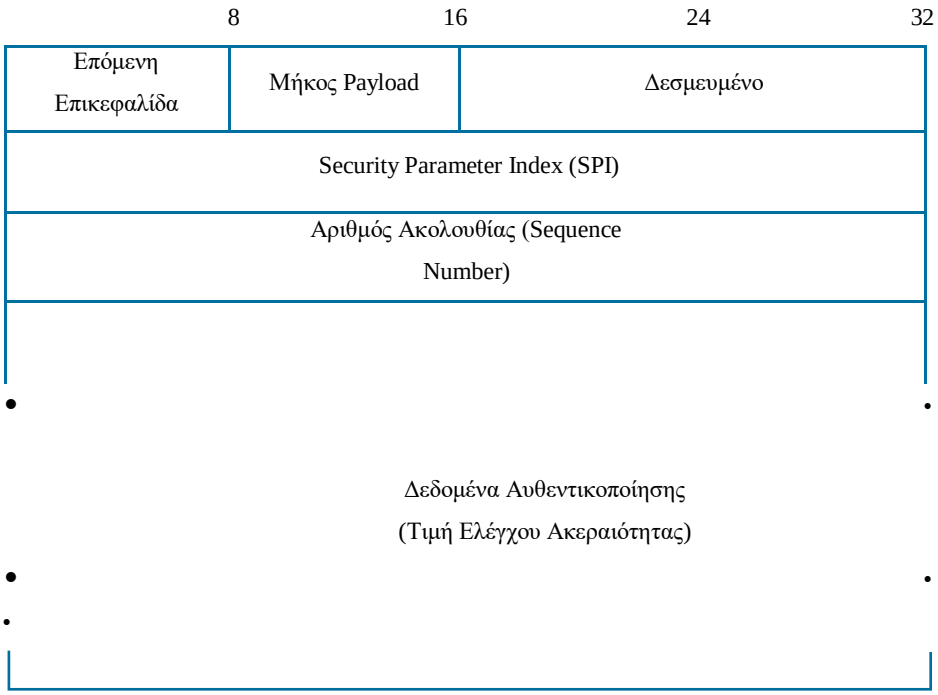


Εικόνα 15. Η επικεφαλίδα επέκτασης ESP

Η επικεφαλίδα επέκτασης ESP θεωρείται ως από άκρο σε άκρο (end-to-end) επικοινωνία. Αυτό πρακτικά σημαίνει ότι, δεν γίνεται καμία επεξεργασία από τους δρομολογητές κατά μήκος της διαδρομής. Ενθυλακώνεται αμέσως μετά την κύρια IPv6 επικεφαλίδα και ακολουθεί τις επικεφαλίδες επέκτασης Hop-by-Hop, Δρομολόγηση και Τεμάχιο. Στο IPv6 η κρυπτογράφηση καλύπτει ολόκληρο το τμήμα του επιπέδου μεταφοράς, καθώς και την ουρά της ESP και την επικεφαλίδα επέκτασης Επιλογές Προορισμού. Η επικεφαλίδα επέκτασης Επιλογές Προορισμού

μπορεί να εμφανίζεται πριν την ESP, μετά την ESP ή και τα δύο. Η ESP και η AH μπορούν να συνδυαστούν με πολλαπλούς τρόπους, οι οποίοι ορίζονται στο RFC 4301 (Fuller and Li, 2006).

Στην Εικόνα 16 φαίνονται τα πεδία της επικεφαλίδας επέκτασης AH. Όπως η ESP, έτσι και AH αντιμετωπίζεται ως επικοινωνία από άκρο σε άκρο. Η επικεφαλίδα επέκτασης AH ενθυλακώνεται μετά την κύρια IPv6 επικεφαλίδα και μετά τις επικεφαλίδες Hop-by-Hop, Δρομολόγηση και Τεμάχιο και υποδεικνύεται από τη δεκαδική τιμή 51 στο πεδίο Επόμενη Επικεφαλίδα.



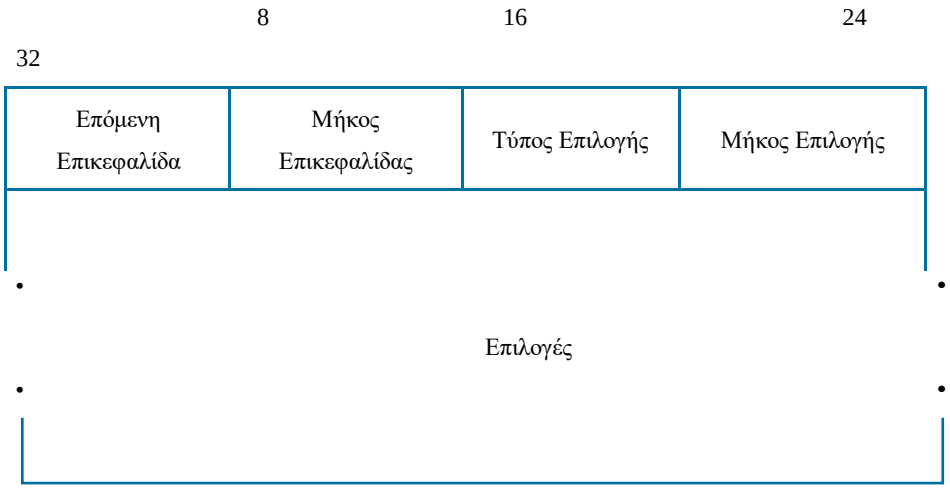
Εικόνα 16. Η επικεφαλίδα επέκτασης Αυθεντικοποίησης (AH)

Περισσότερες λεπτομέρειες και στοιχεία για τις επικεφαλίδες επέκτασης αφορούν την κατανόηση του IPsec και είναι εκτός του σκοπού της παρούσας εργασίας.

2.2.5 Η επικεφαλίδα επέκτασης Επιλογές Προορισμού (Destination Options)

Η επικεφαλίδα επέκτασης Επιλογές Προορισμού (Destination Options) χρησιμοποιείται για να μεταφέρει την προαιρετική πληροφορία που χρειάζεται να εξεταστεί μόνο από τον ή τους κόμβους

προορισμού του πακέτου. Υποδεικνύεται από τη δεκαδική τιμή 60 στο πεδίο Επόμενη Επικεφαλίδα και η μορφή της φαίνεται στην Εικόνα 17. Είναι η δεύτερη επικεφαλίδα που χρησιμοποιεί επιλογές, όπως η Hop-by-Hop επικεφαλίδα επέκτασης (Graziani, 2017).



*Εικόνα 17. Η επικεφαλίδα επέκτασης Επιλογές Προορισμού (*Destination Options)

Η επικεφαλίδα επέκτασης Επιλογές Προορισμού περιέχει τα ακόλουθα, σύμφωνα με την Εικόνα 17:

- **Επόμενη Επικεφαλίδα (Next Header) -8 bits:** Υποδεικνύει τον τύπο της επικεφαλίδας που θα ακολουθήσει μετά και μπορεί να είναι μια άλλη επικεφαλίδα επέκτασης ή το πρωτόκολλο του payload.
- **Μήκος Επικεφαλίδας Επέκτασης (Header Extension Length) - 8 bits:** Είναι το μήκος της επικεφαλίδας επέκτασης Επιλογές Προορισμού σε 8-οκτάδων μονάδες, χωρίς να περιλαμβάνονται οι πρώτες 8 οκτάδες.
- **Επιλογές (Options) – μεταβλητού μήκους:** Το πεδίο περιέχει μία ή περισσότερες TLV-κωδικοποιημένες επιλογές:
    - **Επιλογή Τύπος (Option Type)- 8 bits:** Είναι ο τύπος της επιλογής που μεταφέρεται σε αυτή την επικεφαλίδα.

- **Επιλογή Μήκος Δεδομένων (Option Data Length) -8 bits:** Υποδηλώνει τον αριθμό των bytes του πεδίου Επιλογή Δεδομένων (Option Data).
- **Επιλογή Δεδομένα (Option Data) - μεταβλητού μήκους:** Είναι το περιεχόμενο δεδομένων, ανάλογα με τη χρήση αυτού του πεδίου.

Κεφάλαιο 3: Βασικές αρχές του IPv6

Στο Κεφάλαιο αυτό αρχικά παρουσιάζεται το μοντέλο διευθύνσεων του IPv6, καθώς και ο τρόπος αναπαράστασης των διευθύνσεων. Στη συνέχεια παρουσιάζονται αναλυτικά οι τύποι των διευθύνσεων unicast, anycast και multicast. Τέλος, παρουσιάζεται το ICMPv6 πρωτόκολλο ανακάλυψης γειτόνων (Network Discovery Protocol – NDP) και η δυναμική ανάθεση διευθύνσεων (dynamic address allocation).

3.1 Μοντέλο Διευθύνσεων

Βασική προϋπόθεση για την σύνδεση μιας συσκευής σε ένα δίκτυο, είναι η καταχώρηση της μιας και μοναδικής διεύθυνσης που την προσδιορίζει και οι κανόνες με τους οποίους προσδιορίζεται αυτή η ταυτότητα ορίζεται από το σχήμα διευθυνσιοδότησης, δηλαδή το μοντέλο διευθύνσεων. Ο κύριος λόγος της δημιουργίας του IPv6 ήταν η διαφαινόμενη εξάντληση των διευθύνσεων του IPv4, το οποίο με τη χρήση των 32 bit για την απόδοση διεύθυνσης υποστηρίζει περίπου 4,3 εκατομμύρια διευθύνσεις, ενώ το IPv6 με τη χρήση των 128 bit για την απόδοση διεύθυνσης υποστηρίζει περίπου $3{,}4 \times 10^{38}$ διαφορετικές διευθύνσεις, και παράλληλα έχει σχεδιαστεί έτσι ώστε να υποστηρίζεται την υποδιαίρεση του Διαδικτύου σε ιεραρχικούς τομείς δρομολόγησης. Αυτή είναι μια από τις βασικές διαφορές του IPv6 με το IPv4 (Graziani, 2017).

Ένας host τυπικά έχει ένα και μοναδικό σύνδεσμο (link) μέσα στο δίκτυο. Ο σύνδεσμος υποδεικνύει τη δυνατότητα επικοινωνίας ή ένα μέσο πάνω στο οποίο οι κόμβοι μπορούν να επικοινωνούν στο επίπεδο συνδέσμου (link layer), δηλαδή στο επίπεδο ακριβώς κάτω από το IPv6. Όταν το IP πρωτόκολλο που τρέχει ο host θέλει να στείλει ένα αυτοδύναμο πακέτο το κάνει μέσω αυτού του συνδέσμου. Το όριο μεταξύ του host και των φυσικών συνδέσμων ονομάζεται διεπαφή (interface). Ο δρομολογητής έχει ως βασική λειτουργία την λήψη του αυτοδύναμου πακέτου και την προώθησή του σε άλλο σύνδεσμο (ο δρομολογητής συνδέεται με δύο ή περισσότερους συνδέσμους του δικτύου μεταγωγής) σύμφωνα με πληροφορίες που διατηρεί στον πίνακα δρομολόγησής του. Το όριο μεταξύ

του δρομολογητή και οπουδήποτε από τους συνδέσμους του, ονομάζεται επίσης διεπαφή. Ο δρομολογητής έχει πολλαπλές διεπαφές, μία για κάθε σύνδεσμό του. Επειδή ο κάθε host και ο κάθε δρομολογητής μπορούν να στέλνουν και να λαμβάνουν αυτοδύναμα πακέτα, το πρωτόκολλο IP απαιτεί η κάθε διεπαφή να έχει την δική της IP διεύθυνση, δηλαδή την ταυτότητά της. Η IP διεύθυνση είναι αυτή που δίνει τη δυνατότητα να επικοινωνούν όλοι οι host και οι συσκευές του Διαδικτύου μεταξύ τους (Kurose *et al.*, 2017).

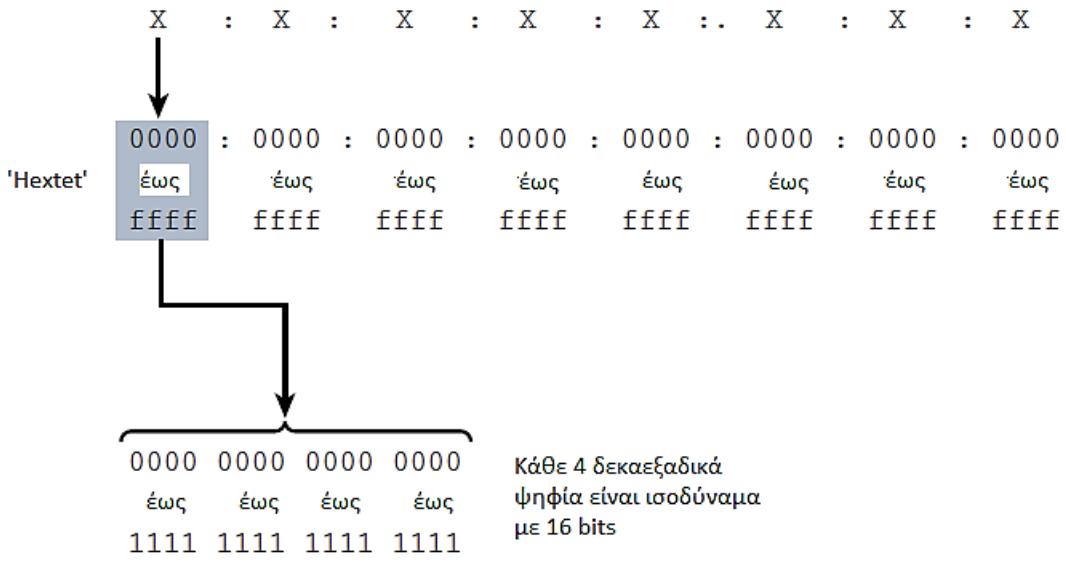
Η μήκους 32 bit IPv4 διεύθυνση αναπαριστάνεται, όπως ήδη αναφέραμε, στο δυαδικό σύστημα σε 4 τμήματα των bits, τα octets, που χωρίζονται μεταξύ τους με τον χαρακτήρα «.». Οι διευθύνσεις του IPv6 αναπαριστάνονται έχουν μήκος 128 bits, και γράφονται στο δεκαεξαδικό σύστημα ως συμβολοσειρά δεκαεξαδικών αριθμών. Όπως είναι γνωστό στο δεκαεξαεδικό σύστημα οι αριθμοί από το 0 έως το 9 αντιπροσωπεύουν τους αντίστοιχους αριθμούς του δεκαδικού συστήματος, ενώ οι αριθμοί από το 10 έως το 15 αντιστοιχούν στους αλφαριθμητικούς χαρακτήρες A έως F (A= 10, B= 11, C= 12, D= 13, E= 14, F= 15). Οι αλφαριθμητικοί χαρακτήρες δεν είναι case sensitive, οπότε τα μικρά και τα κεφαλαία γράμματα είναι ισοδύναμα. Κάθε αριθμός του δεκαεξαδικού συστήματος μπορεί να γραφεί στο δυαδικό σύστημα με 4 bits. Έτσι, για παράδειγμα ο αριθμός 15 του δεκαδικού είναι 15_{10}= f_{16} = 1111_2. Έτσι, για τα 128 bits, κάθε 4 bits μπορούν να αναπαρασταθούν με ένα δεκαεξαδικό ψηφίο (από το 0_{16} [0000_2] μέχρι το f_{16} [1111_2] . Το πρότυπο που ισχύει για το μοντέλο διευθύνσεων του IPv6 ορίζεται στο RFC 4291, *«IP Version 6 Addressing Architecture»* (Deering and Hinden, 2006) και η προτεινόμενη μορφή των IPv6 διευθύνσεων ορίζεται ως x:x:x:x:x:x:x:x. Στο RFC 5952, *"A Recommendation for IPv6 Address Text Representation"* (Kawamura and Kawashima, 2010) συνιστάται η αναπαράσταση των διευθύνσεων να γίνεται με μικρά γράμματα. Κάθε *x* είναι ένα τμήμα των 16 bits, τα hextets, που μπορεί να αναπαρασταθεί χρησιμοποιώντας μέχρι 4 δεκαεξαδικά ψηφία και κάθε τμήμα χωρίζεται με τον χαρακτήρα «:» (colon). Έτσι, προκύπτει ένας αριθμός 128 bits, όπως φαίνεται στην Εικόνα 18και μια συμβολοσειρά 32 δεξαεξαδικών ψηφίων. Αυτή είναι η μεγαλύτερη δυνατή μορφή αναπαράστασης και όπως θα δούμε σε επόμενη παράγραφο, υπάρχει η δυνατότητα διαφορετικής αναπαράστασης, ώστε να μειωθεί το

μήκος των ψηφίων στην αναπαράσταση της διεύθυνσης. Παραδείγματα αναπαραστάσεων μιας IPv6 διεύθυνσης στην μεγαλύτερη μορφή αναπαράστασης είναι τα παρακάτω:

0000:0000:0000:0000:0000:0000:0000:0000

ff02:0000:0000:0000:0000:0000:0000:0001

fe80:0000:0000:0000:a299:9bff:fe18:50d1



Εικόνα 18. Η μορφή της IPv6 διεύθυνσης.

Πριν προχωρήσουμε στις διαφορετικές αναπαραστάσεις μιας IPv6 διεύθυνσης, θα παρουσιάσουμε πρώτα την ιδιαίτερη ορολογία της.

3.1.1 Ορολογία Διευθύνσεων

Η ορολογία των IPv6 διευθύνσεων έχει κάποια κοινά στοιχεία με την ορολογία των IPv4 διευθύνσεων, αλλά και κάποια διαφορετικά. Η IPv4 διεύθυνση, όπως ήδη αναφέρθηκε περιλαμβάνει τρία τμήματα: το τμήμα της κλάσης (A,B,C), το τμήμα του δικτύου και το τμήμα του host. Η IPv6 έχει σχεδιαστεί με διαφορετική λογική, ώστε να υποστηριχθεί μια ιεραρχική δομή δρομολόγησης που να ανταποκρίνεται στην σύγχρονη τοπολογία

του διαδικτύου και κατά αναλογία κάποιοι όροι είναι διαφορετικοί. Πιο συγκεκριμένα, χρησιμοποιούνται οι παρακάτω όροι (Graziani, 2017).

Prefix (πρόθεμα): Το πρόθεμα είναι το τμήμα δικτύου της IPv6 διεύθυνσης. Σε μια IPv4 διεύθυνση, το τμήμα αυτό ονομάζεται τμήμα δικτύου της διεύθυνσης ή πρόθεμα δικτύου.

Prefix length (μήκος προθέματος): Το μήκος προθέματος είναι ο αριθμός των πιο σημαντικών (most-significant) bits, δηλαδή των πρώτων από αριστερά που ορίζουν το πρόθεμα. Αυτό είναι ισοδύναμο με την μάσκα υποδικτύου στο IPv4. Εφόσον οι IPv6 διευθύνσεις έχουν μήκος 128 bits, το πρόθεμα μπορεί να είναι από /0 έως /128.

ID διεπαφής (Interface ID): Το ID (IDentification – ταυτότητα) της διεπαφής είναι ισοδύναμο με το τμήμα του host της IPv4 διεύθυνσης. Στο IPv6 χρησιμοποιείται ο όρος ID διεπαφής γιατί κάθε τύπος συσκευής μπορεί να έχει μια IP διεύθυνση, όχι μόνο ένας host υπολογιστής. Μια συσκευή με ένα IPv6 interface μπορεί να είναι οποιαδήποτε συσκευή, όπως για παράδειγμα μια κάμερα ή ένας αισθητήρας σε ένα σύστημα του IoT ή ένας εξυπηρετητής ή ένας οικιακός υπολογιστής. Ο όρος διεπαφή χρησιμοποιείται γιατί μια IP διεύθυνση, είτε IPv4 είτε IPv6, καταχωρείται στην διεπαφή και μία συσκευή μπορεί να διαθέτει πολλές διεπαφές.

Κόμβος (node) ή συσκευή (device): Ως IPv6 κόμβος ή συσκευή χαρακτηρίζεται οτιδήποτε έχει μια IPv6 διεύθυνση, όπως οι εκτυπωτές και οι συσκευές του IoT. Οι όροι χρησιμοποιούνται εναλλακτικά με την ίδια σημασία.

Όταν, για παράδειγμα, η διεύθυνση γράφεται ως fe80:0000:0000:0000:a299:9bff:fe18:50d1/64, τότε το μήκος του προθέματος αντιστοιχεί στα 64 πρώτα δεκαεξαδικά ψηφία (fe80:0000:0000:0000:) και το ID διεπαφής στα υπόλοιπα a299:9bff:fe18:50d1. Όπως στο IPv4, έτσι και στο IPv6 ο αριθμός των κόμβων σε ένα δίκτυο εξαρτάται από το μήκος του προθέματος.

3.2 Αναπαράσταση Διευθύνσεων

Η αναπαράσταση των IPv6 διευθύνσεων με 32 δεκαεξαδικά ψηφία είναι μεγάλη, δυσανάγνωστη και θα λέγαμε υπερφορτωμένη. Στα RFC 4291 (Deering and Hinden, 2006) και RFC 5952 (Kawamura and Kawashima, 2010) παρέχονται δύο κανόνες για την μείωση του μήκους της αναπαράστασης: ο κανόνας παράλειψης των μπροστινών 0 σε ένα hextet και ο κανόνας παράλειψης ενός hextet που αποτελείται μόνο από μηδενικά χρησιμοποιώντας διπλό colon (::) για την αναπαράσταση μιας

όμορης συμβολοσειράς δύο ή περισσότερων hextet που αποτελούνται μόνο από 0 (Graziani, 2017). ‘Ετσι, για παράδειγμα σύμφωνα με τον πρώτο κανόνα, οι διευθύνσεις

0000:0000:0000:0000:0000:0000:0000:0000

ff02:0000:0000:0000:0000:0000:0000:0001

fe80:0000:0000:0000:a299:9bff:fe18:50d1

μπορούν να γραφούν αντίστοιχα ως

0:0:0:0:0:0:0:0

ff02:0:0:0:0:0:0:1

fe80:0:0:0:a299:9bff:fe18:50d1

και σύμφωνα με τον δεύτερο κανόνα ως

0::

ff02::0001

fe80::a299:9bff:fe18:50d1

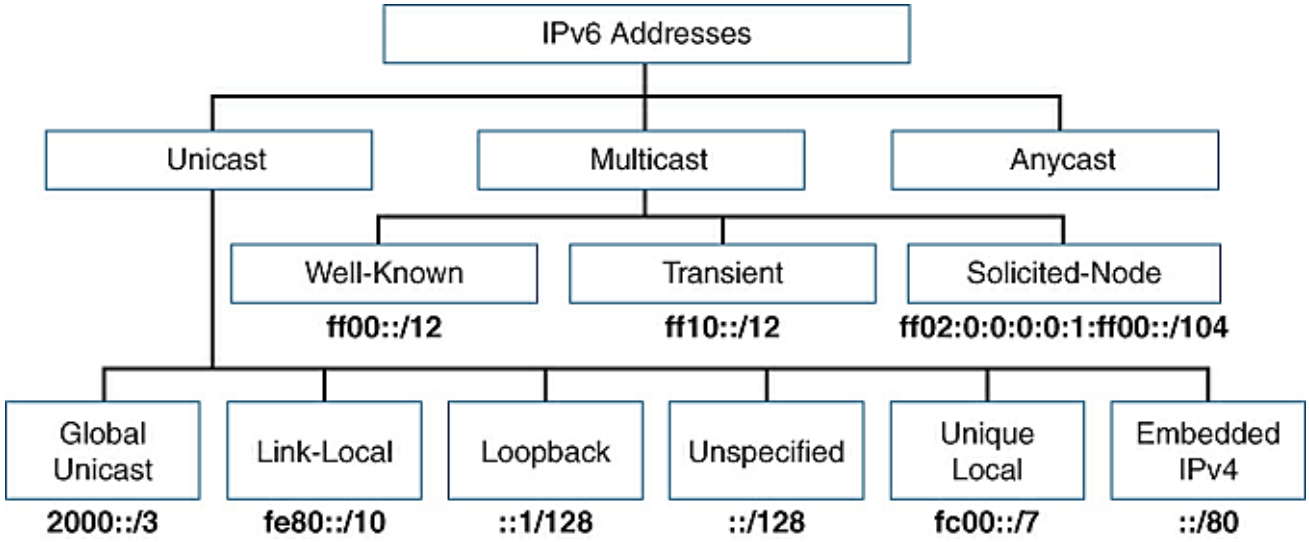
Οι δύο κανόνες μπορούν να συνδυαστούν, οπότε, για παράδειγμα η διεύθυνση ff02:0000:0000:0000:0000:0000:0000:0001 μπορεί να γραφεί ως ff02::1. Για την περίπτωση που μέσα στην συμβολοσειρά υπάρχουν περισσότερα ισάριθμα τμήματα όμορων hextets με 0, το RFC 5952 προβλέπει να γράφεται το πρώτο τμήμα με τον συμβολισμό του δεύτερου κανόνα και το δεύτερο με τον συμβολισμό του πρώτου κανόνα. ‘Ετσι, για παράδειγμα η διεύθυνση 2001:0abd:0000:0000:8abc:0000:0000:2021 γράφεται ως 2001:0abd::8abc:0:0:2021.

3.3 Τύποι Διευθύνσεων

Οι τύποι των IPv6 διευθύνσεων ορίζονται στο RFC 4291 και είναι τρεις: οι διευθύνσεις unicast (μονοεκπομπή), multicast (πολυεκπομπή) και anycast (επιλεκτική εκπομπή). Κάθε διεύθυνση IPv6 έχει καθορισμένο εύρος προσβασιμότητας. Οι τύποι unicast και multicast έχουν υπο-τύπους. Η

εκχώρηση των IPv6 διευθύνσεων γίνεται από την IANA (Graziani, 2017). Ο χώρος των IPv6 διευθύνσεων είναι προφανώς διαφορετικός από ότι από αυτόν των IPv4 διευθύνσεων και απαιτεί τη γνώση όλων των τύπων και των υποτύπων των IPv6 και γίνεται σύμφωνα με τα πρώτα δυαδικά bits του προθέματος.

Όλοι οι τύποι των τύπων και των υποτύπων των IPv6 διευθύνσεων, καθώς και των αντίστοιχων προθεμάτων τους, φαίνονται στην Εικόνα 19 και παρουσιάζονται συνοπτικά ανά τύπο στις επόμενες παραγράφους. Ο χώρος των IPv6 διευθύνσεων με τα αντίστοιχα προθέματα δίνεται αναλυτικά από την IANA στην ιστοσελίδα με τίτλο *«Internet Protocol Version 6 Address Space»* (Internet Assigned Numbers Authority, 2019).



Εικόνα 19. Οι τύποι των IPv6 διευθύνσεων.

Πηγή: (Graziani, 2017)

3.3.1 Διευθύνσεις Unicast

Μία unicast διεύθυνση είναι η πιο κοινή μορφή διεύθυνσης και προσδιορίζει μοναδικά μια διεπαφή σε μία συσκευή που τρέχει το πρωτόκολλο IPv6, δηλαδή αφορά εκπομπή ένας-προς-έναν (one-to-

one). Ένα πακέτο που αποστέλλεται σε μια unicast διεύθυνση λαμβάνεται από μία διεπαφή στην οποία έχει εκχωρηθεί αυτή η διεύθυνση. Οι τύποι των unicast διευθύνσεων είναι συνολικά έξι:

- Global unicast (παγκόσμια μονοεκπομπή)
- Link-Local (τοπικού συνδέσμου)
- Loopback (ανατροφοδότησης)
- Unspecified (απροσδιόριστη)
- Unique local (μοναδικά τοπική)
- Embedded IPv4 (ενσωμάτωση IPv4)

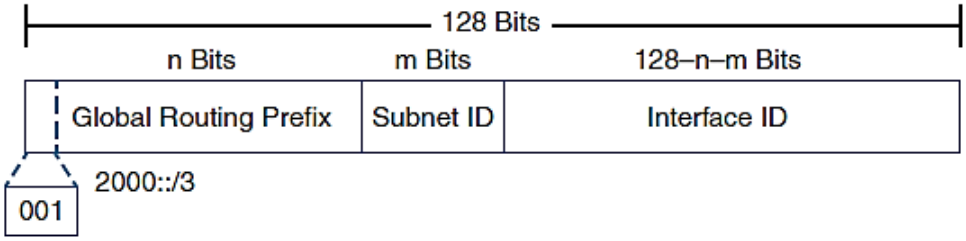
Οι πιο σημαντικοί τύποι unicast διευθύνσεων είναι οι global, οι οποίες είναι ισοδύναμες με τις δημόσιες (public) IPv4 διευθύνσεις και οι link-local που χρησιμοποιούνται για την επικοινωνία των συσκευών στον ίδιο τοπικό σύνδεσμο (Graziani, 2017).

Global unicast διευθύνσεις (διευθύνσεις παγκόσμιας μονοεκπομπής)

Οι Global unicast διευθύνσεις (Global Unicast Addresses – GUAs), γνωστές και ως συγκεντρωτικές (aggregatable) global unicast διευθύνσεις, είναι μοναδικές διευθύνσεις παγκόσμιας δρομολόγησης και πρόσβασης στο IPv6 Διαδίκτυο. Είναι ισοδύναμες με τις δημόσιες (public) IPv4 διευθύνσεις και παίζουν έναν σημαντικό ρόλο στην αρχιτεκτονική της IPv6 διευθυνσιοδότησης. Η γενική δομή της GUA περιλαμβάνει τρία πεδία, όπως φαίνεται στην Εικόνα 20 (Graziani, 2017):

- **Global Routing Prefix** (Παγκόσμιο Πρόθεμα Δρομολόγησης): Είναι το πρόθεμα ή το τμήμα δικτύου της διεύθυνσης που εκχωρείται από τους παρόχους, όπως για παράδειγμα ένας ISP, στον ιστότοπο του πελάτη. Τα τρία πρώτα bits αρχίζουν με τη δυαδική τιμή 001, πράγμα που σημαίνει ότι, το πρώτο δεκαεξαδικό ψηφίο είναι το 2 ή το 3. Το εύρος του πρώτου hextet είναι από το 2000 έως το 3fff.
- **Subnet ID** (ID υποδικτύου): Είναι ένα ξεχωριστό πεδίο για την εκχώρηση των υποδικτύων του ιστότοπου. Σε αντίθεση με το IPv4, για τη δημιουργία υποδικτύων, δεν είναι απαραίτητος ο δανεισμός bits από Interface ID, (δηλαδή το τμήμα του host), και έτσι η υποδικτύωση γίνεται πιο απλή.

- **Interface ID** (ID διεπαφής): Προσδιορίζει τη διεπαφή σε ένα υποδίκτυο και είναι ισοδύναμο με το τμήμα του host σε μια IPv4 διεύθυνση και στις περισσότερες περιπτώσεις έχει μήκος 64 bits.



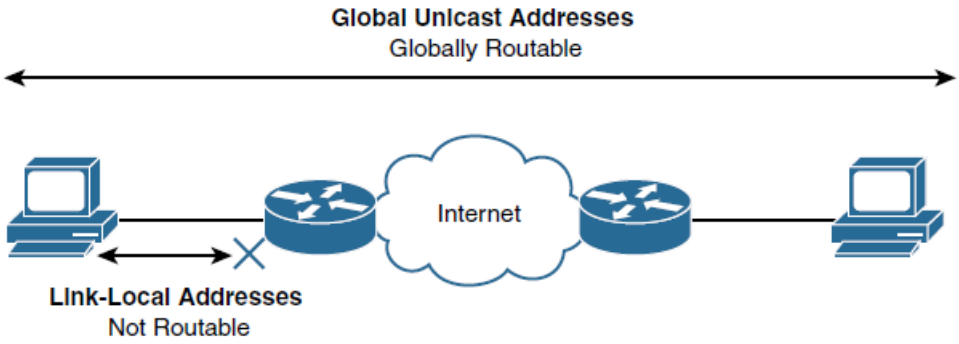
Εικόνα 20. Η δομή της GUA unicast διεύθυνσης

Πηγή: (Graziani, 2017)

Link-Local διευθύνσεις (διευθύνσεις τοπικού συνδέσμου)

Οι link-local διευθύνσεις (Link Local Adddress – LLA) είναι τοπικές διευθύνσεις ενός συνδέσμου (link), όπου ως σύνδεσμος εννοείται ένα λογικό τμήμα δικτύου ή υποδικτύου. Μια LLA περιορίζεται στο συγκεκριμένο σύνδεσμο (υποδίκτυο) και πρέπει να είναι μοναδική στον σύνδεσμο και δεν απαιτείται να είναι μοναδική πέρα από τον σύνδεσμο. Επομένως, οι δρομολογητές δεν προωθούν τα πακέτα με μια link-local διεύθυνση.

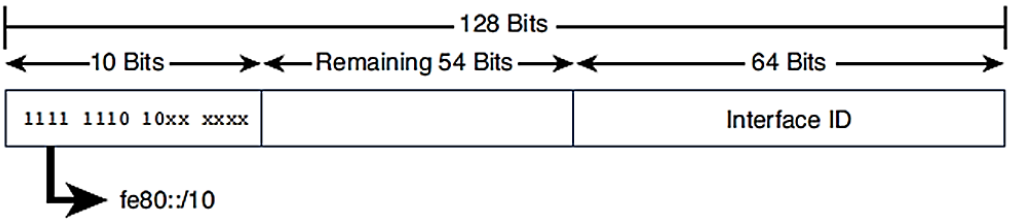
Στην Εικόνα 21 φαίνεται η σύγκριση μεταξύ των διευθύνσεων GUAs και των LLAs.



Εικόνα 21.Σύγκριση μεταξύ GUA και link-local unicast διευθύνσεων

Πηγή: (Graziani, 2017)

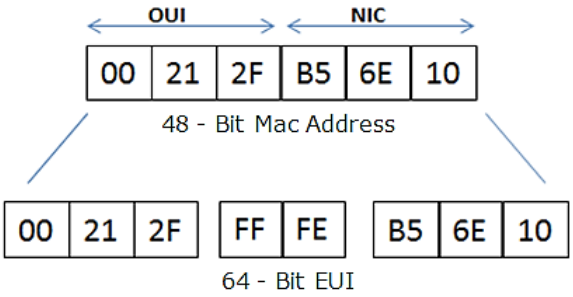
Η link-local διεύθυνση έχει τη μορφή που φαίνεται στην Εικόνα 22 και είναι στο εύρος fe80::10. Η χρήση αυτού του προθέματος και το μήκος προθέματος των 10bits έχει ως αποτέλεσμα το πρώτο hextet να είναι από fe80 έως febd. Το RFC 4291 δεν δίνει συγκεκριμένες οδηγίες για επόμενα 54 bit πριν από το Interface ID, αλλά είναι η καλύτερη πρακτική για αυτά 54 bits να έχουν την τιμή 0. Τα επόμενα 64 bits είναι το ID της διεπαφής.



Εικόνα 22. Δομή της link-local unicast διεύθυνσης.

Πηγή: (Graziani, 2017)

Η IEEE ορίζει το Extended Unique Identifier (EUI), ή το τροποποιημένο EUI-64, μια διαδικασία κατά την οποία χρησιμοποιείται η μήκους 48-bit Ethernet MAC διεύθυνση της διεπαφής για να δημιουργηθεί το μήκους 64-bit μοναδικό ID της διεπαφής. Όταν χρησιμοποιείται το EUI-64 για τη δημιουργία της LLA, τοποθετείται μπροστά το πρόθεμα fe80::/64 prefix στο EUI-64 για να δημιουργηθεί το Interface ID. Για τη δημιουργία του EUI-64, η διεύθυνση MAC χωρίζεται αρχικά σε δύο 24-bit τμήματα, όπου το ένα είναι το OUI (Organally Unique Identifier) και το άλλο είναι το Network Interface Controller (NIC). Το 16-bit 0xFFFE στη συνέχεια παρεμβάλλεται μεταξύ αυτών των δύο 24-bit για τη διεύθυνση EUI μήκους 64-bit. Το IEEE επέλεξε το FFFE ως δεσμευμένη τιμή που μπορεί να εμφανιστεί μόνο στο EUI-64 που δημιουργήθηκε από τη διεύθυνση EUI-48 MAC. Η δημιουργία του EUI-64 Interface ID για τις IPv6 διευθύνσεις περιγράφεται στο RFC 4291 (Graziani, 2017). Στην Εικόνα 23 φαίνεται ένα παράδειγμα που δείχνει πως χρησιμοποιείται μια διεύθυνση MAC για τη δημιουργία EUI, όπου μεταξύ των bits του OUI και του NIC εισάγονται 16 bits με την τιμή fffe.



Εικόνα 23. Μετατροπή EUI-48 MAC σε EUI-64

Τα κύρια χαρακτηριστικά των LLA είναι (Graziani, 2017):

- Κάθε IPv6 συσκευή πρέπει οπωσδήποτε να έχει μία IPv6 link-local διεύθυνση και δεν είναι αναγκαίο να έχει GUA.
- Οι δρομολογητές δεν προωθούν πακέτα που προέρχονται από link-local διευθύνσεις.
- Οι link-local διευθύνσεις πρέπει να είναι μοναδικές μόνο μέσα στο υποδίκτυο. Αρκετές φορές μπορεί να είναι επιθυμητό για μία συσκευή να χρησιμοποιεί την ίδια link-local διεύθυνση σε διαφορετικές διεπαφές που βρίσκονται σε διαφορετικά υποδίκτυα.
- Υπάρχει μόνο μία link-local διεύθυνση ανά διεπαφή.

Loopback διευθύνσεις (διευθύνσεις ανατροφοδότησης)

Οι loopback διευθύνσεις έχουν την μορφή ::1, δηλαδή όλα τα ψηφία είναι 0, εκτός από το τελευταίο που είναι 1. Είναι ισοδύναμες με το τμήμα 127.0.0.0/8 της IPv4 διεύθυνσης, της οποίου η πιο κοινή είναι η 127.0.0.1 διεύθυνση ανατροφοδότησης. Χρησιμοποιείται από έναν κόμβο για να στείλει ένα IPv6 πακέτο στον εαυτό του, τυπικά για τον έλεγχο της στοίβας του TCP/IP και έχει τα παρακάτω χαρακτηριστικά (Graziani, 2017):

- Μπορεί να καταχωρηθεί μόνο σε μια φυσική διεπαφή
- Ένα πακέτο με μια loopback διεύθυνση δεν αποστέλλεται ποτέ έξω από τη συσκευή
- Ο δρομολογητής ποτέ δεν προωθεί πακέτα των οποίων η διεύθυνση προορισμού είναι μία loopback διεύθυνση

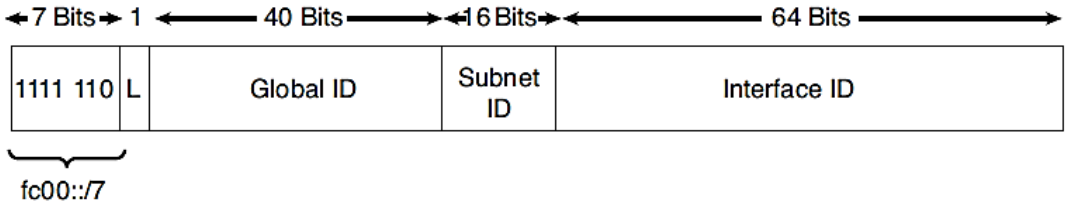
- Η συσκευή απορρίπτει ένα πακέτο που λαμβάνεται σε μία υποδείκνυα διεπαφή εάν η διεύθυνση προορισμού είναι μία loopback διεύθυνση

Unspecified διευθύνσεις (απροσδιόριστες διευθύνσεις)

Μία unspecified διεύθυνση είναι μία διεύθυνση όπου τα ψηφία της είναι όλα 0. Χρησιμοποιείται ως διεύθυνση πηγής για να υποδείξει την έλλειψη διεύθυνσης και δεν μπορεί να καταχωρηθεί σε μία διεπαφή. Ο δρομολογητής ποτέ δεν προωθεί πακέτα με unspecified διεύθυνση (Graziani, 2017).

Unique local διευθύνσεις (μοναδικά τοπικές διευθύνσεις)

Οι Unique local IPv6 διευθύνσεις (Unique Local Address – ULA) είναι οι ισοδύναμες IPv4 ιδιωτικές (private) διευθύνσεις. Είναι γνωστές και ως ιδιωτικές IPv6 διευθύνσεις. Οι ULA διευθύνσεις μπορούν να χρησιμοποιηθούν με παρόμοιο τρόπο όπως οι GUA αλλά μόνο για ιδιωτική χρήση και δεν δρομολογούνται στο Διαδίκτυο. Είναι για συσκευές που δεν έχουν πρόσβαση στο Διαδίκτυο ούτε είναι προσβάσιμες ποτέ από το Διαδίκτυο και χρησιμοποιούνται σε περιορισμένες περιοχές. Είναι ανεξάρτητες από οποιονδήποτε ISP και μπορούν να χρησιμοποιηθούν σε ένα site χωρίς να υπάρχει σύνδεση στο Διαδίκτυο. Οι ULA διευθύνσεις ορίζονται στο RFC 4193 “Unique Local IPv6 Unicast Addresses” (Haberman and Hinden, 2005), και έχουν τη μορφή που φαίνεται στην Εικόνα 24. Το πρόθεμα είναι μήκους 7 bits και είναι fc00::/7, το οποίο έχει ως αποτέλεσμα εύρος από fc00::/7 έως fdff::/7 (Graziani, 2017).



Εικόνα 24. Η δομή της unique local unicast διεύθυνσης.

Πηγή: (Graziani, 2017)

Το πεδίο L (Local) μήκους 1bit είναι flag πεδίο, και μπορεί να πάρει τιμές 1 και 0, πράγμα που σημαίνει ότι, το εύρος των ULA διευθύνσεων χωρίζεται σε δύο μέρη:

- Το fc00::/8 (1111 1100) όπου L=0 και μπορεί η διεύθυνση να οριστεί στο μέλλον.
- Το fd00::/8 (1111 1100) όπου L=1 και η διεύθυνση εκχωρείται τοπικά.

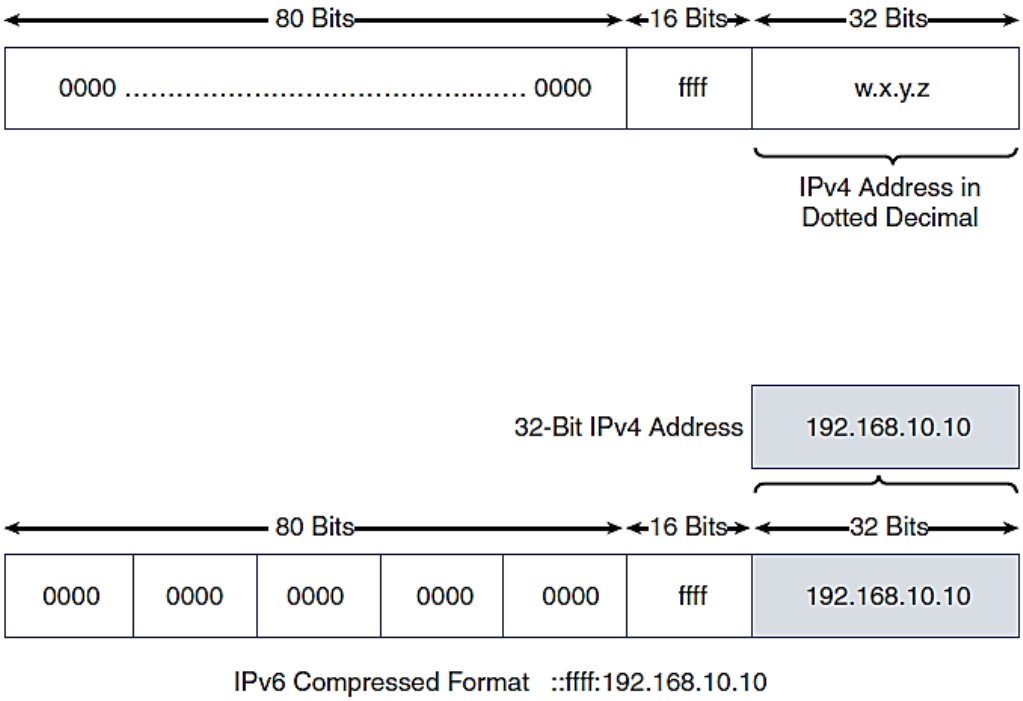
κι έτσι οι έγκυρες ULA διευθύνσεις έχουν το πρόθεμα fd00::/8.

Μια διαφορά με τις IPv4 ιδιωτικές διευθύνσεις είναι ότι, οι ULA διευθύνσεις μπορεί να είναι μοναδικές παγκόσμια. Αυτό είναι χρήσιμο για να διασφαλίζεται ότι, δεν θα υπάρχουν συγκρούσεις, για παράδειγμα όταν οι ULA διευθύνσεις διαρρεύσουν στο Διαδίκτυο.

Embedded IPv4 διευθύνσεις (ενσωμάτωση IPv4 διευθύνσεων)

Η τελευταία κατηγορία των unicast διευθύνσεων είναι αυτές που αφορούν την ενσωμάτωση των IPv4 διευθύνσεων και είναι IPv6 διευθύνσεις που χρησιμοποιούνται για την μετάβαση από το IPv4 στο IPv6. Σε αυτές τις διευθύνσεις, στα 32 τελευταία bits υπάρχει μία IPv4 διεύθυνση ενσωματωμένη στην IPv6 διεύθυνση. Στο RFC 4291 οριζόταν δύο τύποι ενσωμάτωσης IPv4 διευθύνσεων: α) IPv4 αντιστοιχισμένες (IPv4-mapped) IPv6 διευθύνσεις και β) IPv4 συμβατές (IPv4 compatible) IPv6 διευθύνσεις (οι οποίες μετέπειτα καταργήθηκαν).

Οι IPv4-mapped IPv6 διευθύνσεις μπορούν να χρησιμοποιηθούν σε dual-stack συσκευές που χρειάζεται να στείλουν ένα IPv6 πακέτο σε μια συσκευή που τρέχει μόνο το IPv4 και η δομή τους φαίνεται στην Εικόνα 25.



Εικόνα 25. Οι IPv4-mapped IPv6 διευθύνσεις.

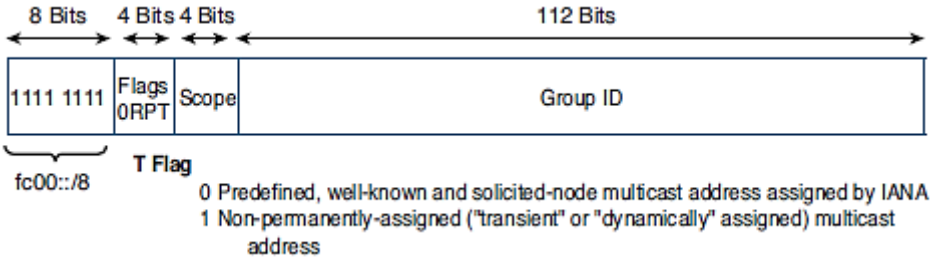
Πηγή: (Graziani, 2017)

Τα πρώτα 80 bits, έχουν όλα την τιμή 0, τα επόμενα 16 bits έχουν όλα την τιμή 1 (ffff) και τα τελευταία 32 bits είναι η ενσωματωμένη IPv6 διεύθυνση, όπου δεν αναπαριστάνεται με την μορφή της IPv4 διεύθυνσης. Οι διευθύνσεις αυτές δεν χρειάζεται να είναι μοναδικές παγκόσμια.

3.3.2 Διευθύνσεις multicast

Η πολυεκπομπή αφορά την τεχνική κατά την οποία μία συσκευή στέλνει ένα πακέτο προς πολλαπλούς προορισμούς ταυτόχρονα, δηλαδή αφορά εκπομπή ένα-προς πολλούς (one-to many). Οι πολλαπλοί προορισμοί ουσιαστικά μπορεί να είναι πολλαπλές διεπαφές στην ίδια συσκευή, αλλά τυπικά είναι διαφορετικές συσκευές. Η IPv6 multicast διεύθυνση ορίζει μια ομάδα συσκευών που ονομάζονται ομάδα πολυεκπομπής (multicast group). Ένα πακέτο που αποστέλλεται από μία ομάδα multicast έχει πάντα ως πηγή μία unicast διεύθυνση. Μια multicast διεύθυνση δεν μπορεί να είναι η

διεύθυνση της πηγής. Σε αντίθεση με το IPv4, δεν υπάρχει η broadcast διεύθυνση. Οι multicast διευθύνσεις χωρίζονται περαιτέρω σε δύο κατηγορίες: τις προκαθορισμένες (predefined) και τις προσωρινές (transient). Οι προκαθορισμένες διευθύνσεις εκχωρούνται από την IANA και είναι δύο τύπων: **well-known** (καλώς ορισμένες ή ευρέως γνωστές) και **solicitated-node** (προσέγγισης κόμβου) (Graziani, 2017).



Εικόνα 26. Η IPv6 multicast διεύθυνση.

Πηγή: (Graziani, 2017)

Η δομή της multicast διεύθυνσης φαίνεται στην Εικόνα 26. Δεν θα αναλύσουμε όλη τη δομή, απλά θα αναφέρουμε τα πιο σημαντικά στοιχεία.

Τα πρώτα 8 bits έχουν την τιμή 1 (ff) και ακολουθούνται από ένα πεδίο μήκους 4 bits (Flags 0RPT) που είναι δεσμευμένα για 4 τιμές flag. Το τελευταίο bit του πεδίου χρησιμοποιείται ως flag για να δηλωθεί εάν η multicast διεύθυνση είναι προκαθορισμένη (τιμή bit=0) ή εάν είναι προσωρινή (τιμή bit=1). Το επόμενο πεδίο μήκους 4 bits (Scope) ορίζει το εύρος στο οποίο οι δρομολογητές μπορούν να προωθήσουν το multicast πακέτο. Το επόμενο πεδίο ορίζει μήκους 112 bits (Group ID) αναπαριστά το ID της ομάδας πολυεκπομπής.

Οι **well-known multicast διευθύνσεις** έχουν το πρόθεμα ff00::12. Είναι προκαθορισμένες ή δεσμευμένες multicast διευθύνσεις για εκχωρημένες ομάδες συσκευών και είναι ισοδύναμες με τις broadcast IPv4 διευθύνσεις στο εύρος από 224.0.0.0 έως 239.255.255.255. Για παράδειγμα, οι διευθύνσεις με πρόθεμα ff02::1: αντιστοιχούν σε όλες τις IPv6 συσκευές και οι διευθύνσεις με πρόθεμα ff02::2: αντιστοιχούν σε όλους τους IPv6 δρομολογητές (Graziani, 2017).

Η solicited-node multicast διεύθυνση είναι κάθε unicast διεύθυνση που καταχωρείται σε μια διεπαφή. Αυτές οι διευθύνσεις δημιουργούνται αυτόματα τοποθετώντας το πρόθεμα της solicited-node πολυεκπομπής ff02:0:0:0:1ff00::/104 στα τελευταία 24 bits της unicast διεύθυνσης. Παρέχουν έναν τρόπο για την προσέγγιση οποιασδήποτε συσκευής στον σύνδεσμο χωρίς να απαιτείται από όλες αυτές τις συσκευές να επεξεργάζονται τα δεδομένα ενός πακέτου. Θεωρούνται ως μια πιο αποτελεσματική προσέγγιση στην broadcast IPv4 διεύθυνση (Graziani, 2017).

3.3.3 Διευθύνσεις anycast

Η IPv6 anycast διεύθυνση είναι μια IPv6 διεύθυνση που μπορεί να εκχωρηθεί επιλεκτικά σε περισσότερες από μία διεπαφές (τυπικά σε πολλές συσκευές). Με άλλα λόγια, πολλές συσκευές μπορούν να έχουν την ίδια anycast διεύθυνση. Όταν ένα πακέτο αποστέλλεται σε μια anycast διεύθυνση δρομολογείται στην εγγύτερη διεπαφή που έχει αυτή τη διεύθυνση, σύμφωνα με τον πίνακα δρομολόγησης του δρομολογητή. Οι anycast διευθύνσεις είναι διαθέσιμες τόσο στο IPv4, και στο IPv6. Ο αρχικός σκοπός των anycast διευθύνσεων ήταν να χρησιμοποιηθούν σε πρωτόκολλα όπως το DNS και το HTTP αλλά ποτέ δεν υλοποιήθηκαν σύμφωνα με τον αρχικό σχεδιασμό. Σε αυτές τις διευθύνσεις δεν υπάρχει προκαθορισμένο πρόθεμα και χρησιμοποιούνται τα προθέματα όπως στις GUAs. Υπάρχουν κάποιες δεσμευμένες μορφές των anycast διευθύνσεων που ορίζονται στα RFC 4291 και RFC 2526, αλλά είναι ακόμα σε πειραματικό στάδιο (Graziani, 2017).

3.4 Το Πρωτόκολλο Ανακάλυψης Γειτόνων (Neighbor Discovery Protocol)

Μία από τις μεγάλες καινοτομίες στο πρωτόκολλο ICMPv6, το οποίο περιγράφεται στο RFC 4443 «Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification» (Gupta and Conta, 2006), είναι η εισαγωγή του πρωτόκολλου ανακάλυψης γειτόνων, του Neighbor Discovery Protocol – NDP, το οποίο προσθέτει στο ICMPv6 μία νέα λειτουργικότητα και περιγράφεται στο RFC 4861 “Neighbor Discovery for IP version 6 (IPv6)” (Simpson *et al.*,

2007). Το NDP χρησιμοποιείται για την ανακάλυψη συσκευών και την ανταλλαγή μηνυμάτων του ίδιου υποδικτύου (on-link).

Το NDP χρησιμοποιεί πέντε τύπους μηνυμάτων του ICMPv6, τα οποία αφορούν:

Α. Μηνύματα δρομολογητή προς συσκευή που χρησιμοποιούνται για δυναμική εκχώρηση διευθύνσεων:

- Router Solicitation – RS (προσέγγιση δρομολογητή) μήνυμα
- Router Advertisement – RA (διαφήμιση δρομολογητή) μήνυμα

Β. Μηνύματα συσκευή προς συσκευή που χρησιμοποιούνται για δυναμική επίλυση διευθύνσεων:

- Neighbor Solicitation – NS (προσέγγιση γείτονα) μήνυμα
- Neighbor Advertisement – NA (διαφήμιση γείτονα) μήνυμα

Γ. Μηνύματα δρομολογητή προς συσκευή που χρησιμοποιούνται για την καλύτερη επιλογή του πρώτου άλματος (hop):

- Redirect messages (ανακατεύθυνση μηνυμάτων)

Οι τέσσερις πρώτοι είναι νέοι τύποι στο πρωτόκολλο ICMPv6. Ο τελευταίος τύπος αποτελεί μέρος και του ICMPv4, αλλά στο ICMPv6 παρέχει επιπλέον λειτουργικότητες. Τα μηνύματα μπορεί να περιλαμβάνουν μία ή περισσότερες επιλογές, κάποιες από τις οποίες μπορεί να εμφανίζονται πολλές φορές μέσα στο ίδιο μήνυμα. Οι επιλογές αυτές βοηθούν στην παροχή πληροφορίας που σχετίζεται με διάφορους σκοπούς της ανακάλυψης γειτόνων. Υπάρχουν πέντε επιλογές:

- Source Link-Layer Address: Περιέχει την επιπέδου 2 διεύθυνση (συνήθως Ethernet) του αποστολέα του πακέτου. Χρησιμοποιείται στα Neighbor Solicitation, Router Solicitation, και Router Advertisement μηνύματα.
- Target Link-Layer Address: Περιέχει την επιπέδου 2 διεύθυνση (συνήθως Ethernet) του στόχου. Χρησιμοποιείται στα Neighbor Advertisement και Redirect μηνύματα.

- Prefix Information: Παρέχει στους host προθέματα και άλλες πληροφορίες. Εμφανίζεται στα Router Advertisement μηνύματα.
- Redirect Header: Χρησιμοποιείται στα Redirect μηνύματα για το περιεχόμενο μέρος ή όλου του πακέτου το οποίο πρόκειται να επανακατευθυνθεί.
- MTU: Χρησιμοποιείται στα Router Advertisement μηνύματα για να βοηθήσει στην εξασφάλιση ότι όλες οι συσκευές του συνδέσμου χρησιμοποιούν το ίδιο MTU.

3.4.1 Δυναμική Επίλυση Διευθύνσεων (Dynamic Address Resolution)

Τα μηνύματα NS και NA χρησιμοποιούνται για την ανταλλαγή μηνυμάτων μεταξύ δύο οποιονδήποτε συσκευών του ίδιου υποδικτύου για τις εξής λειτουργικότητες (Graziani, 2017):

Επίλυση διευθύνσεων (Address resolution): Η επίλυση διευθύνσεων στο IPv6 είναι παρόμοια με το πρωτόκολλο ARP στο IPv4. Μια συσκευή στέλνει ένα Neighbor Solicitation μήνυμα όταν γνωρίζει την IPv6 διεύθυνση προορισμού αλλά χρειάζεται request της διεύθυνσης του κατώτερου 2ου επιπέδου (τυπικά μιας Ethernet διεύθυνσης). Αυτό είναι παρόμοιο με ένα ARP request στο IPv4. Σε απάντηση του Neighbor Solicitation μηνύματος, η συσκευή στόχος στέλνει ένα Neighbor Advertisement μήνυμα, παρόμοιο με ένα ARP reply. Στον Πίνακα 3 δίνεται η σύγκριση IPv4 ARP Request και IPv6 Neighbor Solicitation.

Πίνακας 3. Σύγκριση IPv4 ARP Request και IPv6 Neighbor Solicitation

	IPv4 ARP Request	**IPv6 Neighbor Solicitation**

MAC προορισμού	Broadcast	Multicast
Ενσωμάτωση πάνω στο IP	Όχι	Ναι (IPv6)
IP προορισμού	N/A	Solicited-Node Multicast
Address Resolution Protocol	ARP	ICMPv6

Η επίλυση των διευθύνσεων περιλαμβάνει επίσης την ανίχνευση όμοιας διεύθυνσης (Duplicate Address Detection - DAD), η οποία επαληθεύει την μοναδικότητα μιας διεύθυνσης στον σύνδεσμο. Η συσκευή στέλνει ένα Neighbor Solicitation μήνυμα της δικής της IPv6 διεύθυνσης για να ανιχνεύσει εάν μια άλλη συσκευή στο υποδίκτυο χρησιμοποιεί την ίδια διεύθυνση. Εάν δεν παραληφθεί ένα Neighbor Advertisement μήνυμα, τότε η συσκευή γνωρίζει ότι είναι μοναδική στο υποδίκτυο.

Cache γείτονα (Neighbor Cache) και ανίχνευση μη-προσέγγισης γείτονα (Neighbor Unreachability Detection -NUD): Οι IPv6 συσκευές χρησιμοποιούν NS μηνύματα και τα συσχετισμένα NA μηνύματα για να δημιουργήσουν ένα Neighbor Cache. Το Neighbor Cache περιέχει μια αντιστοίχιση του IPv6 στις Ethernet MAC διευθύνσεις, παρόμοια με το ARP cache του IPv4. Το NUD χρησιμοποιεί NS και NA μηνύματα για να ανιχνεύσει εάν μια άλλη συσκευή messages είναι προσβάσιμη στο υποδίκτυο.

Τα μηνύματα RS και RA χρησιμοποιούνται για την ανταλλαγή μηνυμάτων μεταξύ μιας συσκευής και ενός δρομολογητή στον ίδιο σύνδεσμο (υποδίκτυο) και πιο συγκεκριμένα για τη δυναμική ανάθεση διευθύνσεων που εξετάζουμε στην αμέσως επόμενη παράγραφο.

3.4.2 Δυναμική Ανάθεση Διευθύνσεων (Dynamic Address Allocation)

Όπως στο IPv4, έτσι και στο IPv6, οι καταχωρήσεις μπορούν να γίνουν είτε στατικά, είτε δυναμικά. Ωστόσο, στη δυναμική ανάθεση διευθύνσεων στο IPv6 ακολουθείται μια διαφορετική προσέγγιση. Η δυναμική εκχώρηση IPv6 διευθύνσεων αρχίζει με τα ICMPv6 Router Solicitation (RS) και Router Advertisement (RA) μηνύματα, τα οποία ενσωματώνονται στο IPv6 όπως φαίνεται στην Εικόνα 27.

IPv6 Header	ICMPv6: RS or RA Message

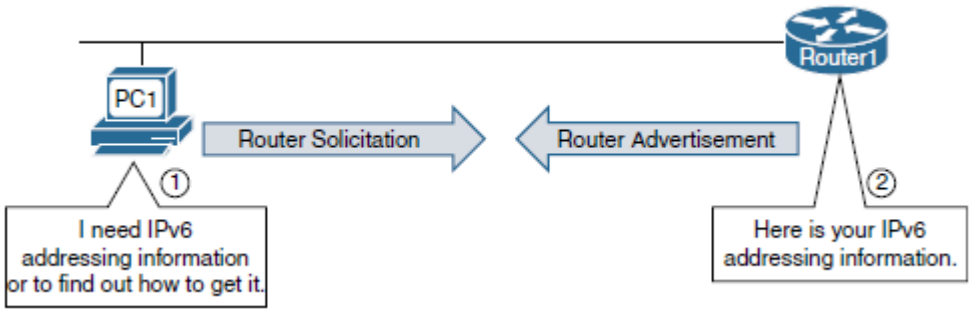
Εικόνα 27. ICMPv6 RA/RS μηνύματα στο IPv6

Το ICMPv6 χρησιμοποιεί τα μηνύματα RA για να υποδείξει στις συσκευές πως θα αποκτήσουν την πληροφορία της IPv6 διευθυνσιοδότησης. Ένας IPv6 δρομολογητής στέλνει περιοδικά ένα RA μήνυμα ή όταν λαμβάνει ένα αίτημα RS από μία συσκευή, όπως φαίνεται αφαιρετικά στην Εικόνα 28. Ένας host στέλνει RS μήνυμα όταν χρειάζεται να ξέρει πως θα αποκτήσει δυναμικά την πληροφορία διευθυνσιοδότησης. Αυτό τυπικά συμβαίνει κατά τη διάρκεια της εκκίνησης και είναι εξορισμού στα περισσότερα λειτουργικά συστήματα.

Εικόνα 28. Τα μηνύματα Router Solicitation και Router Advertisement στο ICMPv6

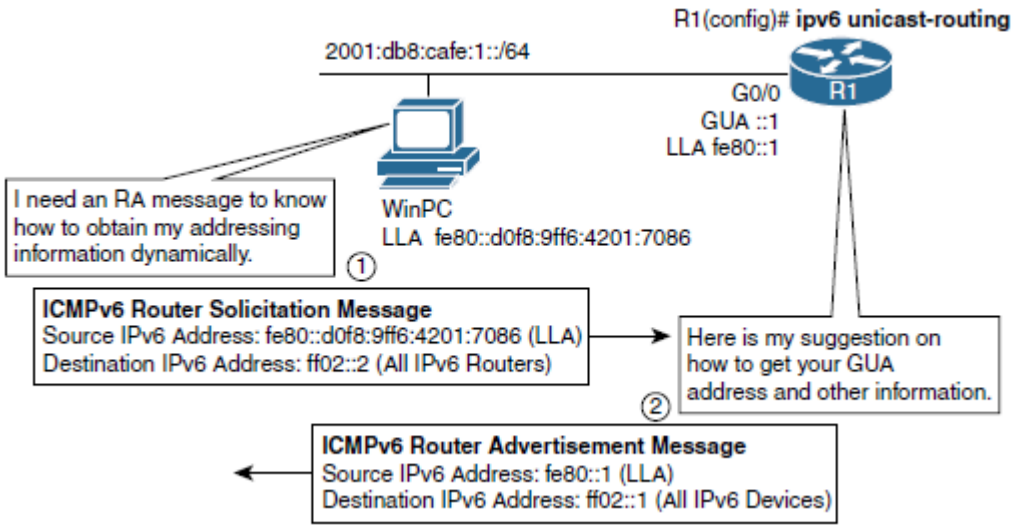
Πηγή: (Graziani, 2017)

Τα μηνύματα RA χρησιμοποιούνται για να υποδείξουν στις συσκευές πως θα αποκτήσουν την πληροφορία της IPv6 διευθυνσιοδότησης. Τα RA αποστέλλονται με τη χρήση της IPv6 διεύθυνσης προορισμού σε όλες τις IPv6 multicast διευθύνσεις των συσκευών (ff02::1), οπότε κάθε IPv6 συσκευή στον σύνδεσμο το παραλαμβάνει. Ουσιαστικά αυτό είναι παρόμοιο με το broadcast. Στην



Εικόνα 29 φαίνεται ένα παράδειγμα αλληλεπίδρασης ενός υπολογιστή (WinPC) που αποστέλλει ένα RA μήνυμα προς έναν δρομολογητή (R1) και ο δρομολογητής απαντά με το σχετικό RS μήνυμα. Το RA μήνυμα περιέχει πληροφορίες διευθυνσιοδότητησης για τις IPv6 συσκευές σχετικές με τα παρακάτω (Graziani, 2017):

- Το πρόθεμα δικτύου και το μήκος προθέματος, μαζί με άλλες πληροφορίες για το υποδίκτυο.
- Τη διεύθυνση του εξορισμού (default) gateway. Είναι μία link-local διεύθυνση της διεπαφής εξόδου του δρομολογητή, η διεύθυνση πηγής του RA μηνύματος.
- Τρία flags που χρησιμοποιούνται για να υποδείξουν σε μια συσκευή πως θα αποκτήσει την πληροφορία της IPv6 διευθυνσιοδότησής της. Αυτά τα flags είναι:
    - Το A flag (Autonomous Address Configuration Flag)
    - Το O flag (Other Configuration Flag) και
    - Το M flag (Managed Address Configuration Flag)
- Προαιρετικές πληροφορίες όπως το domain name και έναν κατάλογο των διευθύνσεων των DNS εξυπηρετητών.



Εικόνα 29. Αλληλεπίδραση μεταξύ Router Solicitation και Router Advertisement μηνυμάτων

Πηγή: (Graziani, 2017)

Στην Εικόνα 29 φαίνεται ένα παράδειγμα αλληλεπίδρασης ενός υπολογιστή (WinPC) που αποστέλλει ένα RA μήνυμα προς έναν δρομολογητή (R1) και ο δρομολογητής απαντά με το σχετικό RS μήνυμα.

Αντίθετα με μία IPv4 συσκευή, μια IPv6 συσκευή μπορεί να ορίσει όλες τις διευθύνσεις της δυναμικά χωρίς να είναι απαραίτητη η ύπαρξη ενός DHCP εξυπηρετητή. Το RA μπορεί να χρησιμοποιήσει μία από τρεις μεθόδους: **1) αυτόματη ρύθμιση των παραμέτρων διεύθυνσης χωρίς καταστάσεις (Stateless Address Autoconfiguration – SLAAC, 2) SLAAC και DHCPv6 εξυπηρετητής χωρίς καταστάσεις (stateless) και 3) DHCPv6 εξυπηρετητής με καταστάσεις (stateful).** Οι μέθοδοι ορίζονται από τις τιμές που παίρνουν τα flags.

Πριν περιγράψουμε τις μεθόδους, θα πρέπει να διευκρινίσουμε τη διαφορά των υπηρεσιών που παρέχει ένας stateless DHCPv6 εξυπηρετητής από αυτές που παρέχει ένας stateful DHCPv6 εξυπηρετητής.

Υπάρχουν δύο μορφές για τις υπηρεσίες DHCPv6:

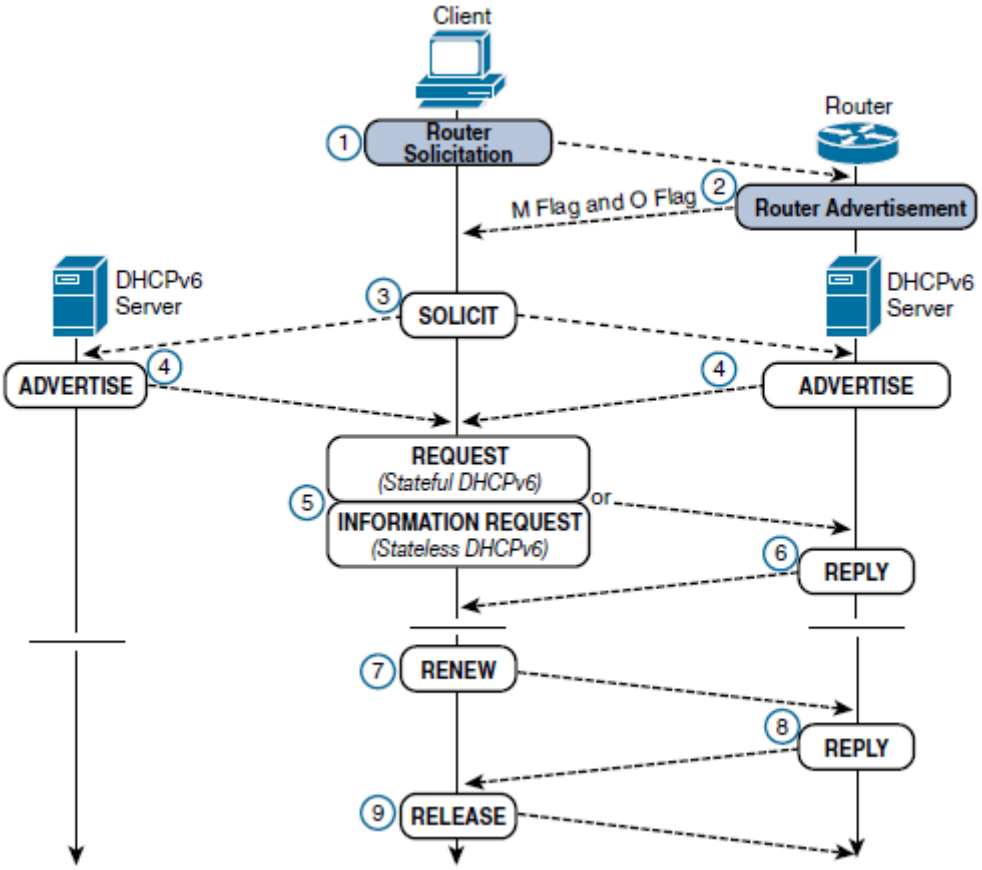
- Οι stateful DHCPv6 υπηρεσίες που περιγράφονται στο RFC 8415 το οποίο κατάργησε το RFC 3315, «*Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*» (Mrugalski *et al.*, 2018)
- Οι stateless DHCPv6 υπηρεσίες που περιγράφονται επίσης στο RFC 8415 το οποίο κατάργησε το αρχικό RFC 3736, *Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6*

Οι stateful DHCPv6 υπηρεσίες παρέχουν την ίδια αυτόματη ρύθμιση παραμέτρων με αυτές του DHCPv4. Οι hosts λαμβάνουν όλες τις πληροφορίες διευθυνσιοδότησης και ρύθμισης παραμέτρων απευθείας από έναν DHCPv6 εξυπηρετητή, εκτός από τη διεύθυνση του default gateway. Οι διαφορές με το stateless DHCPv6 είναι ότι οι hosts λαμβάνουν την πληροφορία διευθυνσιοδότησής τους από μηνύματα Router Advertisement και ανακτούν τις άλλες παραμέτρους ρύθμισης από έναν DHCPv6 server (Graziani, 2017).

Στην Εικόνα 30 φαίνονται τα βήματα της διαδικασίας επικοινωνίας DHCPv6, στην οποία εμπλέκονται ο πελάτης, ο εξυπηρετητής και ο δρομολογητής. Η σημαντική διαφορά ανάμεσα στο

DHCPv6 and DHCPv4 είναι ότι, η απόφαση για τη δυναμική καταχώρηση διευθύνσεων λαμβάνεται από τον δρομολογητή. Ο πελάτης ρυθμίζεται έτσι ώστε να λαμβάνει αυτόματα τις διάφορες πληροφορίες. Χωρίς να μπούμε σε ιδιαίτερες λεπτομέρειες, αναφέρουμε τα κύρια μηνύματα της επικοινωνίας όπως αριθμούνται στην Εικόνα, μεταξύ ενός DHCPv6 client και server (Graziani, 2017):

- **SOLICIT (3):** Οι DHCPv6 πελάτες χρησιμοποιούν SOLICIT μήνυμα για τον εντοπισμό του server.
- **ADVERTISE (4):** Ο server στέλνει ένα ADVERTISE μήνυμα ως απάντηση στο SOLICIT μήνυμα του client SOLICIT για να δηλώσει ότι είναι διαθέσιμος για DHCPv6 υπηρεσία.
- **REQUEST (5):** Ο client στέλνει ένα REQUEST μήνυμα για να ζητήσει τη ρύθμιση παραμέτρων, συμπεριλαμβανομένων των IPv6 διευθύνσεων, από έναν συγκεκριμένο DHCPv6 server.
- **REPLY (6):** Ο server στέλνει ένα REPLY μήνυμα που περιέχει τις εκχωρημένες διευθύνσεις και ρυθμίσεις παραμέτρων ως απάντηση στο REQUEST μήνυμα του client.



Εικόνα 30. Stateless και Statefull DHCPv6 λειτουργίες.

Πηγή: (Graziani, 2017)

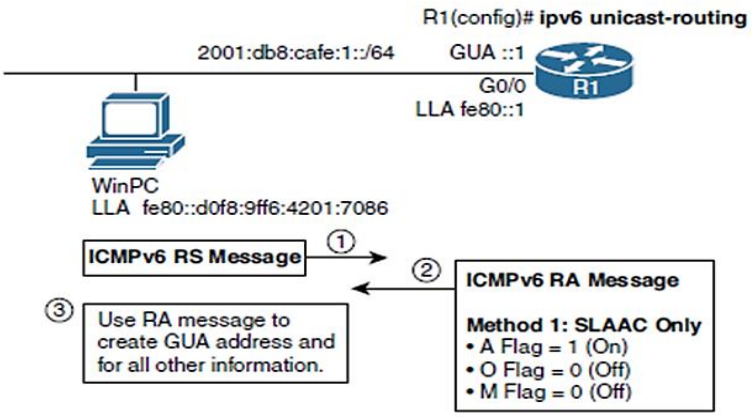
Παρόλες τις ομοιότητες που υπάρχουν, το πρωτόκολλο DHCPv6 έχει επανασχεδιαστεί και είναι ανεξάρτητο DHCPv4. Σε περιπτώσεις ενός dual-stack δικτύου όπου εφαρμόζεται DHCP, απαιτείται ο διαχωρισμός των υπηρεσιών που τρέχουν για κάθε ένα από τα δύο πρωτόκολλα.

Στη συνέχεια περιγράφονται οι τρείς μέθοδοι του RA.

Μέθοδος 1: Αυτόματη ρύθμιση των παραμέτρων διεύθυνσης χωρίς καταστάσεις (Stateless Address Autoconfiguration – SLAAC)

Στη μέθοδο αυτή, που φαίνεται στην Εικόνα 31, η συσκευή χρησιμοποιεί την πληροφορία που υπάρχει στο RA μήνυμα για όλες τις ανάγκες της διευθυνσιοδότησής της, συμπεριλαμβανομένης και της χρήσης του προθέματος μέσα στο RA για να δημιουργήσει μια IPv6 GUA. Η συσκευή θα χρησιμοποιήσει την IPv6 διεύθυνση πηγής του RA ως το δικό της default gateway. Τα τρία RA flags ρυθμίζονται εξορισμού ως εξής κι έτσι η τροποποίησή τους δεν είναι απαραίτητη (Graziani, 2017):

- **A flag = 1:** Χρήση SLAAC για τη δημιουργία της GUA
- **O flag = 0:** Δεν χρειάζεται καμιά άλλη πληροφορία από έναν stateless DHCPv6 server
- **M flag = 0:** Δεν χρειάζεται επικοινωνία με έναν stateful DHCPv6 server



Εικόνα 31. Μέθοδος 1: Μόνο SLAAC

Πηγή: (Graziani, 2017)

Οι συσκευές που έχουν ρυθμιστεί να λαμβάνουν τη διεύθυνση IPv6 δυναμικά:

- Χρησιμοποιούν το πρόθεμα που υπάρχει σε ένα RA μήνυμα για τη δημιουργία μιας GUA.
- Χρησιμοποιούν και άλλη πληροφορία που υπάρχει σε ένα RA message, όπως το μήκος προθέματος και το MTU του συνδέσμου. Επίσης, μπορεί να περιλαμβάνεται πληροφορία για

το domain name και τις διευθύνσεις του DNS server, πληροφορίες οι οποίες δεν περιλαμβάνονται εξορισμού.

- Χρησιμοποιούν την IPv6 διεύθυνση πηγής του πακέτου, μια link-local unicast διεύθυνση, ως διεύθυνση του default gateway.
- Δεν χρειάζονται καμία άλλη πληροφορία από έναν stateless ή stateful DHCPv6 server.

Συνοψίζοντας, θα μπορούσαμε να πούμε ότι ένα RA μήνυμα προς μία συσκευή δίνει την οδηγία: *"Χρησιμοποίησε το SLAAC για να δημιουργήσεις την GUA διεύθυνση, και το RA μήνυμα έχει οτιδήποτε χρειάζεσαι. Δεν χρειάζεται να επικοινωνήσεις με οποιοδήποτε τύπο DHCPv6 server."*

Μέθοδος 2: SLAAC και DHCPv6 εξυπηρετητής χωρίς καταστάσεις

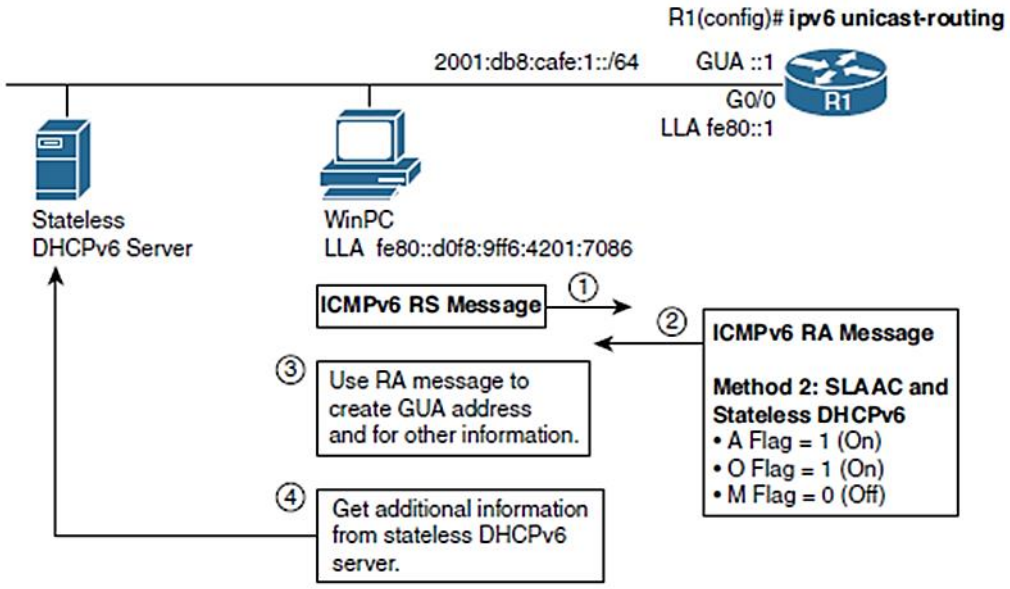
Στη μέθοδο αυτή, που φαίνεται στην Εικόνα 32, όπως και στην πρώτη μέθοδο, η συσκευή χρησιμοποιεί SLAAC για να δημιουργήσει μια GUA και χρησιμοποιεί την IPv6 διεύθυνση πηγής του RA για το default gateway. Όμως, αυτή η μέθοδος υποδεικνύει επιπλέον στη συσκευή ότι χρειάζεται να έλθει σε επικοινωνία με έναν stateless DHCPv6 εξυπηρετητή για πρόσθετη πληροφορία η οποία δεν περιλαμβάνεται στο RA μήνυμα. Αυτή η πληροφορία μπορεί να είναι ένας κατάλογος με DNS εξυπηρετητές. Τονίζεται ότι, ένας stateless DHCPv6 εξυπηρετητής δεν παρέχει ούτε διατηρεί καμία πληροφορία για την global unicast διευθυνσιοδότηση, παραμόνο παρέχει την κοινή πληροφορία του δικτύου για όλες τις συσκευές του δικτύου. Τα τρία RA flags ρυθμίζονται ως εξής (Graziani, 2017):

- **A flag = 1:** Χρήση SLAAC για τη δημιουργία της GUA
- **O flag = 1:** Επικοινωνία με stateless DHCPv6 server για άλλες πληροφορίες διευθυνσιοδότησης
- **M flag = 0:** Δεν χρειάζεται επικοινωνία με έναν stateful DHCPv6 server

Οι συσκευές που έχουν ρυθμιστεί να λαμβάνουν τη διεύθυνση IPv6 δυναμικά με αυτή τη μέθοδο:

- Χρησιμοποιούν το πρόθεμα που υπάρχει σε ένα RA μήνυμα για τη δημιουργία μιας GUA.

- Χρησιμοποιούν και άλλη πληροφορία που υπάρχει σε ένα RA message, όπως το μήκος προθέματος και το MTU του συνδέσμου.
- Χρησιμοποιούν την IPv6 διεύθυνση πηγής του πακέτου, μια link-local unicast διεύθυνση, ως διεύθυνση του default gateway.
- Επικοινωνούν με ένα stateless DHCPv6 server για πρόσθετες πληροφορίες, όπως ένα domain name και διευθύνσεις DNS server. Το RA μήνυμα δεν ορίζει ποια πληροφορία μπορεί να αποκτηθεί από τον stateless DHCPv6 server.



Εικόνα 32. Μέθοδος 2: SLAAC και stateless DHCPv6

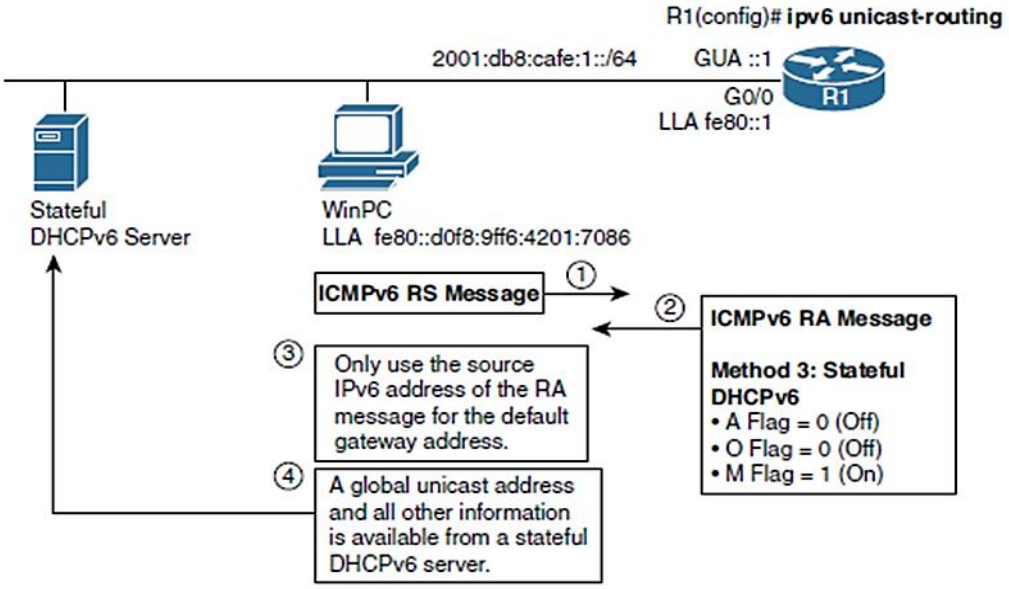
Πηγή: (Graziani, 2017)

Συνοψίζοντας, θα μπορούσαμε να πούμε ότι ένα RA μήνυμα προς μία συσκευή δίνει την οδηγία: *"Χρησιμοποίησε το SLAAC για να δημιουργήσεις την GUA διεύθυνση. Υπάρχουν και άλλες πληροφορίες μέσα στο RA μήνυμα και χρειάζεται να επικοινωνήσεις με έναν stateless DHCPv6 server για άλλες πληροφορίες ρύθμισης παραμέτρων"*

Μέθοδος 3: DHCPv6 εξυπηρετητής με καταστάσεις

Η μέθοδος αυτή, που φαίνεται στην Εικόνα 33, είναι παρόμοια με το DHCP του IPv4. Το RA υποδεικνύει στην συσκευή ότι θα χρησιμοποιήσει έναν DHCPv6 εξυπηρετητή για όλες τις ανάγκες της που αφορούν την IPv6 διευθυνσιοδότησή της, συμπεριλαμβανομένης και της GUA. Όμως, η συσκευή πρέπει να ανακτήσει δυναμικά τη διεύθυνση του default gateway από το RA μήνυμα, όπως στις προηγούμενες δύο μεθόδους. Τα τρία RA flags ρυθμίζονται ως εξής (Graziani, 2017):

- **A flag = 0:** Όχι χρήση SLAAC για τη δημιουργία της GUA
- **O flag = 0:** Δεν χρειάζεται επικοινωνία με έναν stateless DHCPv6 server
- **M flag = 1:** Ανάκτηση της GUA και των υπόλοιπων πληροφοριών από έναν stateful DHCPv6 server.



Εικόνα 33. Μέθοδος 3: Stateful DHCPv6

Πηγή: (Graziani, 2017)

Οι συσκευές που έχουν ρυθμιστεί να λαμβάνουν τη διεύθυνση IPv6 δυναμικά με αυτή τη μέθοδο:

- Χρησιμοποιούν την IPv6 διεύθυνση πηγής του πακέτου, μια link-local unicast διεύθυνση, ως διεύθυνση του default gateway.

- Έρχονται σε επαφή με έναν stateful DHCPv6 server για μια GUA και όλες τις υπόλοιπες πληροφορίες, όπως ένα domain name και DNS server διευθύνσεις.

Συνοψίζοντας, θα μπορούσαμε να πούμε ότι ένα RA μήνυμα προς μία συσκευή δίνει την οδηγία: *"Χρησιμοποίησε το RA μήνυμα για τη διεύθυνση του the default gateway. Μη χρησιμοποιείς SLAAC για τη δημιουργία μιας GUA. Πάρε μια GUA και όλες τις υπόλοιπες πληροφορίες από έναν stateful DHCPv6 server."*

Σύνοψη των Μεθόδων

Στον Πίνακα παρουσιάζονται συγκεντρωτικά οι τρείς μέθοδοι εκχώρησης διευθύνσεων με τις αντίστοιχες τιμές που λαμβάνουν τα flags σε κάθε μέθοδο.

Πίνακας 4. Router Advertisement: Μέθοδοι εκχώρησης και RA Flags

RA Μέθοδοι εκχώρησης διευθύνσεων	A Flag (SLAAC)	O Flag (Stateless DHCPv6)	M Flag (Stateful DHCPv6)
Μέθοδος 1: SLAAC (default)	1 (on)	0 (off)	0 (off)
Μέθοδος 2: SLAAC και stateless DHCPv6	1 (on)	1 (on)	0 (off)
Μέθοδος 3: Stateful DHCPv6	0 (off)	N/A	1 (on)

Οι μέθοδοι 1 και 2 υποδεικνύουν ότι η συσκευή πελάτης χρησιμοποιεί SLAAC για να δημιουργήσει την δική του IPv6 GUA. Ο πελάτης χρησιμοποιεί το πρόθεμα στο RA μήνυμα και δημιουργεί ένα ID διεπαφής μήκους 64 bits, το οποίο μπορεί να δημιουργηθεί με δύο τρόπους (Graziani, 2017):

- Τυχαία 64-bits τιμή: Το λειτουργικό σύστημα μπορεί να δημιουργήσει μια τυχαία 64-bits τιμή για το ID της διεπαφής. (αυτό είναι εξορισμού στο λειτουργικό σύστημα των Windows)

- EUI-64: Δημιουργία 64-bits τιμής με τη χρήση της MAC διεύθυνσης, όπως περιγράψαμε στην παράγραφο 3.3.1.

Σε κάθε περίπτωση, η συσκευή μπορεί να δημιουργήσει την δική της GUA χωρίς τις υπηρεσίας του DHCPv6.

Κεφάλαιο 4 : Cisco Packet Tracer

4.1 Τι είναι το packet Tracer

Το Packet Tracer είναι ένα πρόγραμμα προσομοίωσης δικτύων τα οποία αλληλεπιδρούν μεταξύ τους σε πραγματικό χρόνο. Πριν πραγματοποιηθεί ένα δίκτυο μπορούμε να το δημιουργήσουμε στο γραφικό περιβάλλον το Cisco packet Tracer και να προσθέσουμε τι συσκευές που θέλουμε να δοκιμάσουμε στο δίκτυό μας .Για παράδειγμα μπορεί να έχουμε ένα PC ή laptop τα οποία να εξοπλίζονται με τις κατάλληλες διεπαφές (όπως μπορεί να είναι ασύρματα η ενσύρματα ,η θύρες usb κλτ) και να κάνουμε διαδικτυακές ρυθμίσεις(διεύθυνση IP μάσκες δικτύου DNS server κλπ) .Με τον ίδιο τρόπο ρυθμίζουμε μεταγωγής
(switches) δρομολογητές (routers) εξυπηρετητές (Servers).Το συγκεκριμένο πρόγραμμα μπορεί να τρέξει σε Windows, Linux και Mac ενώ διαθέτει πρόγραμμα και για Android συσκευές όπως και για IOS. (https://www.codebrakes.gr/tutorials/intro_packet_tracer.htm)

4.2 Πώς λειτουργεί το IOS στο packet Tracer

Η δομή και λειτουργία των IOS στο Cisco χωρίζεται σε 3 modes τα οποία είναι τα εξής:

1. User EXEC mode(>)(Λειτουργία χρήστη) : Η σύνδεση σε αυτό το επίπεδο γίνεται αυτόματα έπειτα από την στο σύνδεση Cisco packet Tracer. Οι εντολές που χρησιμοποιούνται σε αυτά τα mode δεν επηρεάζουν τις ρυθμίσεις της συσκευής , απλά αφορά την απλή ενημέρωση για τα υπάρχοντα δεδομένα διαχείρισης την εντολή exit ή logout Μπορούμε να αποχωρήσουμε από το περιβάλλον διότι δεν υπάρχει άλλο ανώτερο mode .Με την εντολή enable μπορούμε να μπούμε στο privilaged mode

Πίνακας 5 Εντελές για τα User EXEC mode

Εντολές user EXEC mode	
Εντολή	**Περιγραφή**
connect	Open a terminal connection
disable	Turn off privileged commands
disconnect	Disconnect an existing network connection
enable	Turn on privileged commands
exit	Exit from the EXEC
logout	Exit from the EXEC
ping	Send echo messages
resume	Resume an active network connection
show	Show running system information
ssh	Open a secure shell client connection
telnet	Open a telnet connection
terminal	Set terminal line parameters
traceroute	Trace route to destination

2. privileged mode(#)(Λειτουργία προνομίων): Είναι το δεύτερο mode του IOS της cisco.Σε αυτό το επίπεδο ο χρήστης μπορεί να εκτελέσει όλες τις εντολές που σχετίζονται Με τη διαχείριση και την διαμόρφωση των δεδομένων του εξοπλισμού.Για να γίνει αναβάθμιση από το Exec mode στο Privilege mode χρησιμοποιείται η εντολή enable ενώ για να γίνει η αντίστροφη διαδικασία χρησιμοποιείται η εντολή disable. Αυτό το επίπεδο διαχωρίζεται με το σύμβολο # (prompt) το οποία εμφανίζεται στο παράθυρο εκτέλεσης των εντολών .Η εκτέλεση των εντολών πραγματοποιείται με την πληκτρολόγηση των κατάλληλων λέξεων και το πλήκτρο enter.
3. Σε αυτό το επίπεδο ο χρήστης μπορεί να εκτελέσει εντολές διαφορετικών δεδομένων σε διαφορετικά επίπεδα.Αυτό έχει σαν αποτέλεσμα την τροποποίηση των ρυθμίσεων. Για να εισέλθουμε στο επόμενο επίπεδο δίνουμε config terminal.

Πίνακας 6 Εντολές για το privelaged EXEC mode

Εντολές privileged EXEC mode	
Εντολή	**Περιγραφή**
auto	Exec level Automation
clear	Reset functions
clock	Manage the system clock
configure terminal	Enter configuration mode
connect	Open a terminal connection
copy	Copy from one file to another
debug	Debugging functions (see also 'undebug')
delete	Delete a file
dir	List files on a filesystem
disable	Turn off privileged commands

disconnect	Disconnect an existing network connection
erase	Erase a filesystem
exit	Exit from the EXEC
logout	Exit from the EXEC
mkdir	Create new directory
more	Display the contents of a file
no	Disable debugging informations
ping	Send echo messages
reload	Halt and perform a cold restart
resume	Resume an active network connection
rmdir	Remove existing directory
send	Send a message to other tty lines
setup	Run the SETUP command facility
show	Show running system information
ssh	Open a secure shell client connection
telnet	Open a telnet connection
traceroute	Trace route to destination
undebug	Disable debugging functions (see also 'debug')
vlan	Configure VLAN parameters
write	Write running configuration to memory, network, or terminal

4. *Configuration Mode* (Λειτουργία διαμόρφωσης)(global and sub configuration).:Είναι το τρίτο mode του IOS της Cisco. Όταν μεταβαίνουμε στο configuration mode η εκτέλεση της εντολής prompt στην οθόνη αλλάζει από # σε (config)#.Εφόσον ο χρήστης βρίσκεται σε "Global Configuration Mode" μπορεί να αποκτήσει πρόσβαση σε πιο ειδικές ομάδες εντολών, όπως αυτές οι οποίες σχετίζονται με τη διαμόρφωση μια συγκεκριμένης διεπαφής ("Interface Configuration Mode"). Για να συμβεί αυτό πρέπει να εκτελεστεί η εντολή

interface < «όνομα» διεπαφής>. Αφού εκτελεστή η εντολή θα αλλάξει το το prompt από (config)# σε (config-if)#.Για παράδειγμα με αυτό το sub mode μπορούμε να ρυθμίσουμε τις διεπαφές ενός router αποδίδοντας IP διεύθυνση. Για να ολοκληρωθούν οι εντολές που αφορούν τη συγκεκριμένη κατάσταση και να επιστρέφουμε στην προηγούμενη κατάσταση ("Global Configuration Mode")Θα πρέπει να πληκτρολογήσουμε exit>enter. Με την ίδια διαδικασία όπως πριν όπως κάναμε την εισαγωγή στο ("Interface Configuration Mode")Μπορούμε να κάνουμε και στα άλλα *Configuration Mode.*

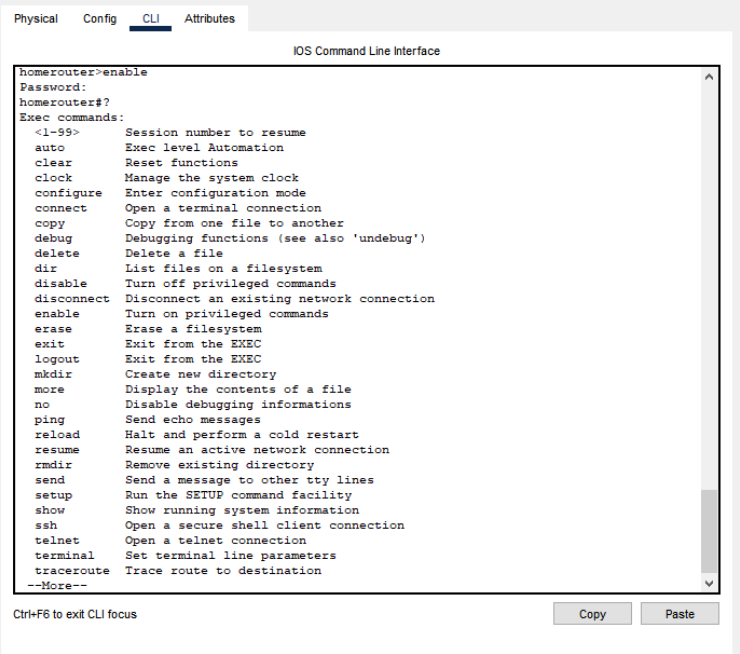
Πίνακας 7 Εντελές για global configure mode

Εντολές global configure mode	
Εντολή	**Περιγραφή**
aaa	Authentication, Authorization and Accounting
access-list	Add an access list entry
banner	Define a login banner
bba-group	Configure BBA Group
boot	Modify system boot parameters
cdp	Global CDP configuration subcommands
class-map	Configure Class Map
clock	Configure time-of-day clock
config-register	Define the configuration register
crypto	Encryption module
default	Set a command to its defaults
do	To run exec commands in config mode
dot11	IEEE 802.11 config commands
end	Exit from configure mode

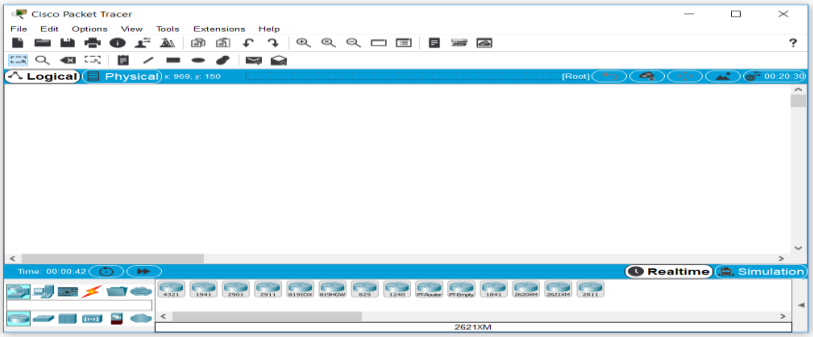
exit	Exit from configure mode
flow	Global Flow configuration subcommands
hostname	Set system's network name
interface	Select an interface to configure
ip	Global IP configuration subcommands
ipv6	Global IPv6 configuration commands
key	Key management
license	Configure license features
line	Configure a terminal line
lldp	Global LLDP configuration subcommands
logging	Modify message logging facilities
login	Enable secure login checking
mac-address-table	Configure the MAC address table
no	Negate a command or set its defaults
ntp	Configure NTP
parser	Configure parser
policy-map	Configure QoS Policy Map
port-channel	EtherChannel configuration
priority-list	Build a priority list
privilege	Command privilege parameters
queue-list	Build a custom queue list
radius-server	Modify Radius query parameters
router	Enable a routing process
secure	Secure image and configuration archival commands
security	Infra Security CLIs
service	Modify use of network based services

snmp-server	Modify SNMP engine parameters
spanning-tree	Spanning Tree Subsystem
tacacs-server	Modify TACACS query parameters
username	Establish User Name Authentication
vpdn	Virtual Private Dialup Network
vpdn-group	VPDN group configuration

Βοήθεια: Για όποια εντολή θέλω να χρησιμοποιήσουν πάνω στο IOS και δεν τη γνωρίζουμε πληκτρολογούμε (?). Παράδειγμα (enable ?)μας βγάζει χρήσιμες πληροφορίες για αυτόν τον όρο.

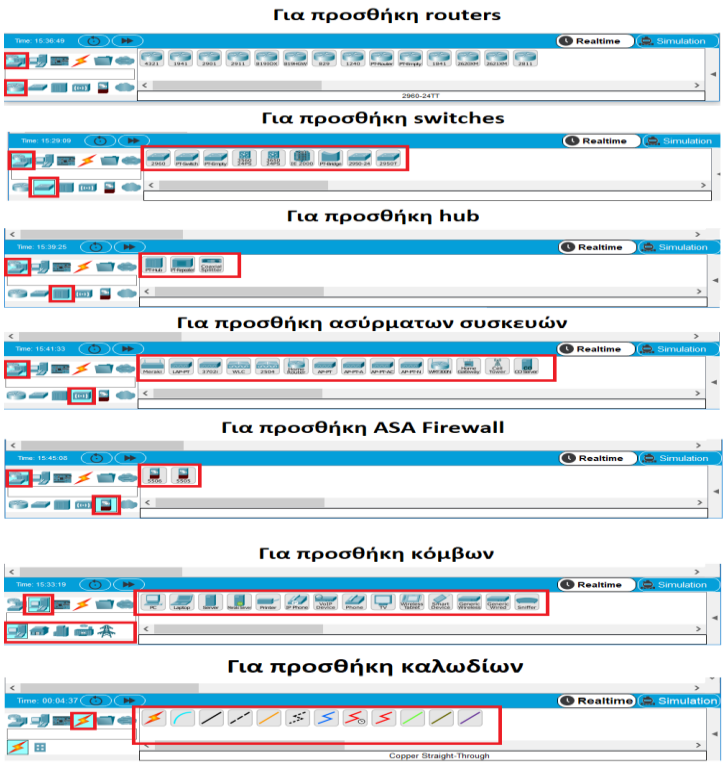


4.3 Υλοποίηση πάνω στο Cisco packet Tracer

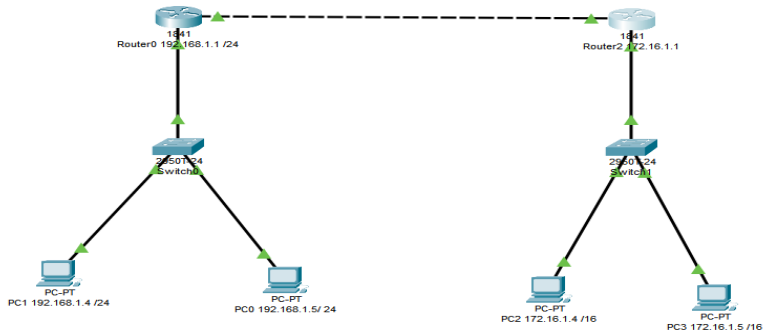


Εικόνα 34 Το γραφικό περιβάλλον του Cisco packet Tracer

Εικόνα 26:Αυτό είναι το γραφικό περιβάλλον μας όταν ανοίγουμε το πρόγραμμα Cisco packet Tracer



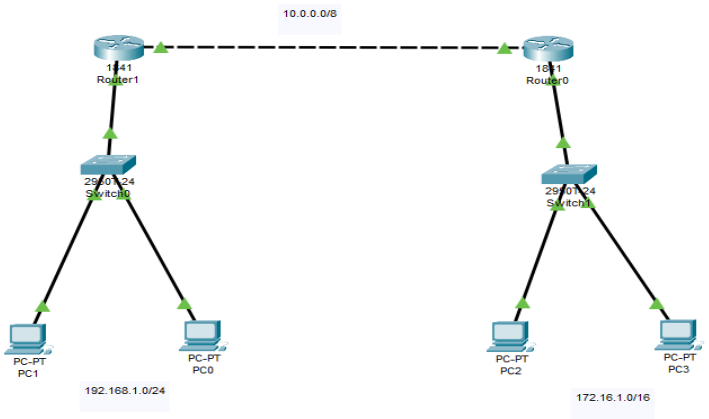
Εικόνα 35 Τι μπορούμε να προσθέσουμε το γραφικό περιβάλλον του προγράμματος



Στο συγκεκριμένο παράδειγμα Θα αναλύσουμε ένα κύκλωμα χρησιμοποιώντας δρομολογητές (routers), μεταγωγής(switches) και υπολογιστές (pc)

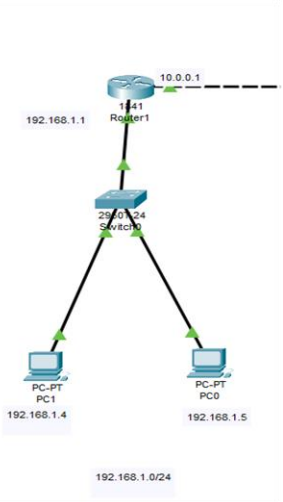
Στο συγκεκριμένο παράδειγμα θα χρησιμοποιήσουμε 2 router με ονομασία (1841) 2 Switch με ονομασία (2950T-24) και 4 PC. Για να συνδέσουμε τα δύο router μεταξύ τους χρησιμοποιήσουμε ένα καλώδιο Cooper Cross over το οποίο συνδέεται την FastEthernet 0/1 και στα δύο router. Τα router με switch θα συνδεθούν από την πλευρά του router στην θύρα FastEthernet 0/0 ενώ από την πλευρά του switch FastEthernet 0/3. Τα Switch με τα Pc μεταξύ τους χρησιμοποιήσουμε ένα καλώδιο Cooper Cross over το οποίο συνδέεται FastEthernet 0/1 και FastEthernet 0/2 του switch με τις FastEthernet του κάθε Pc.

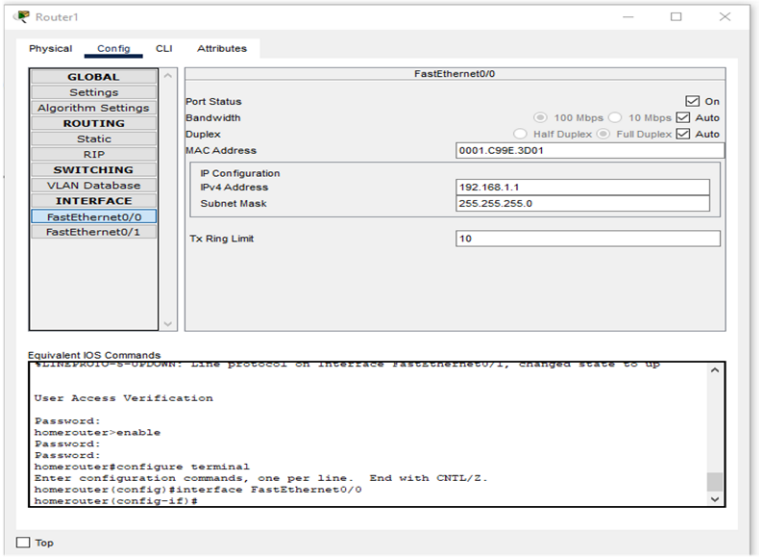
Αφού έχει ολοκληρωθεί η καλωδίωση μας θα πρέπει να φτιάξουμε κάποια interface σε όλες τις συσκευές μας για να μπορούν να επικοινωνούν ακόμη και πιο μακρινοί κόμβοι μεταξύ τους .Στο παράδειγμά μας θα το χωρίσουμε σε τρία μέρη.

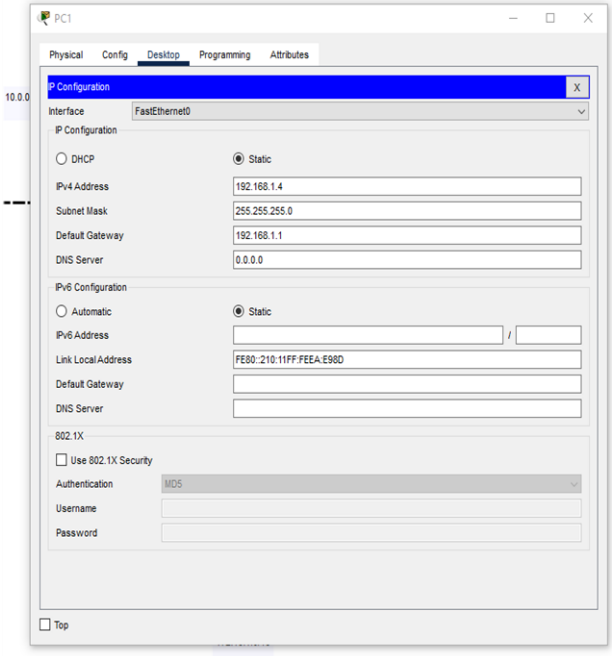


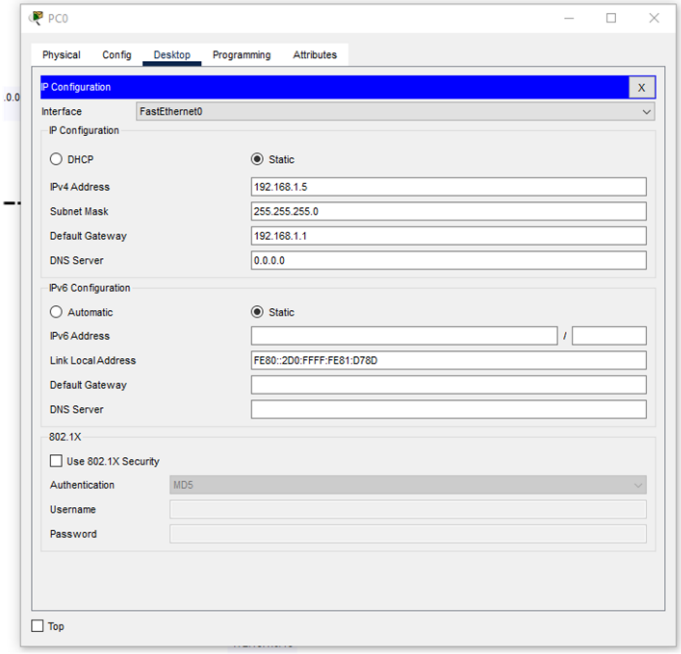
Το δίκτυό μας θα το χωρίσουμε σε 3 υποδίκτυα κλάσης Α , κλάσης Β και κλάσης C. Στα δίκτυα κλάσης Α οι κοινοί οροί είναι 8 Στα κλάσης Β είναι 16 και στα κλάσης C είναι 24.Κλάση Α θα χρησιμοποιήσουμε μεταξύ των router κλάση Β στο δεξί μας υποδίκτυο και κλάση C στο αριστερό μου υποδίκτυο.

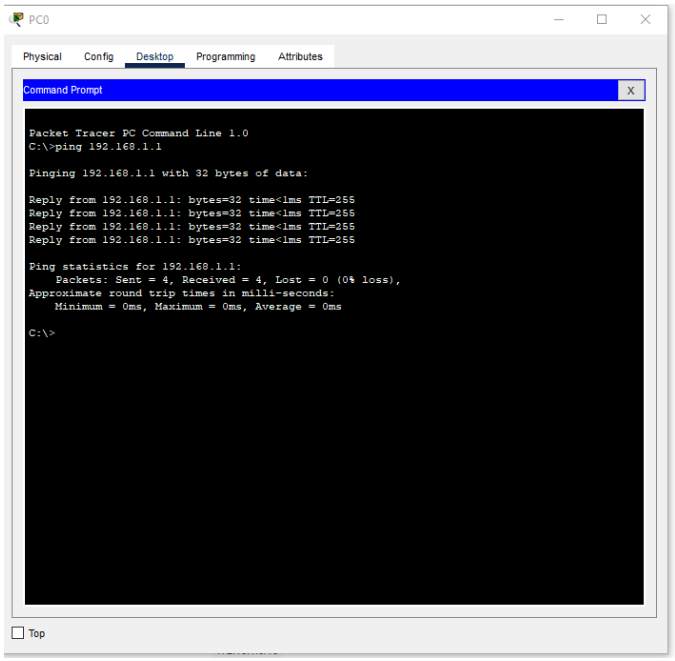
Στο επόμενο βήμα θα πρέπει να προσθέσουμε διευθύνσεις στα 2 router μάς και στα 4 Pc. Στην αρχή Θα προσπαθήσουμε να συνδέσουμε τα 2PC τις παρακάτω φωτογραφίες με το router της. θα πάμε στο PC 0 και έπειτα διπλό κλικ>Desktop> Ip *Configuration.Το ίδιο ακριβώς θα κάνουμε και με το PC 1 και διεύθυνσειεπίσεις που θα βάλουμε καρφωτά θα εμφανίζονται στις παρακάτω φωτογραφία. Γεια να βάλουμε διεύθυνση στο router διιπλό κλικ>Config>interface>FastEtherntet0/0 Όπου κι τοποθετήσουμε την τιμή για να λειτουργήσει το συγκεκριμένο δίκτυο. Στο τέλος κάνω ένα pink μεταξύ του Router για το PC 1 για να δούμε ότι πληροφορίες αποστέλλονται .*


10.0.0.1
1841
Router1
192.168.1.1
2960-24
Switch0
PC-PT
PC1
192.168.1.4
PC-PT
PC0
192.168.1.5
192.168.1.0/24

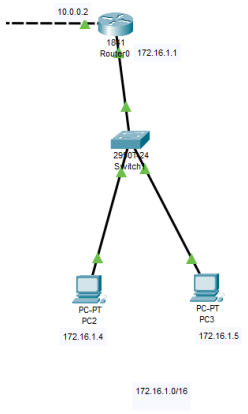

Router1
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
FastEthernet0/0
FastEthernet0/1
FastEthernet0/0
Port Status
On
Bandwidth
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
0001.C99E.3D01
IP Configuration
IPv4 Address
192.168.1.1
Subnet Mask
255.255.255.0
Tx Ring Limit
10
Equivalent IOS Commands
User Access Verification
Password:
homerouter>enable
Password:
Password:
homerouter#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
homerouter(config)#interface FastEthernet0/0
homerouter(config-if)#
Top

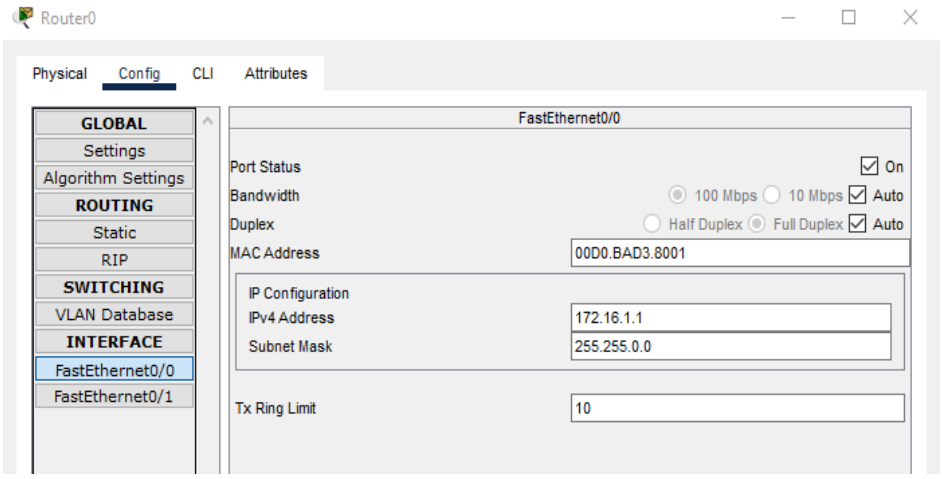

PC1
Physical
Config
Desktop
Programming
Attributes
IP Configuration
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.1.4
Subnet Mask
255.255.255.0
Default Gateway
192.168.1.1
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
Link Local Address
FE80::210:11FF:FEEA:E98D
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top

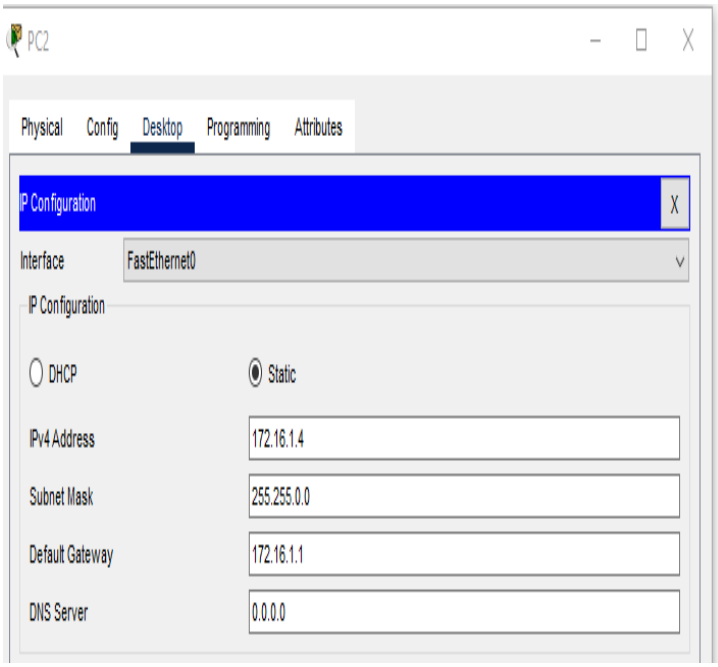

PC0
Physical
Config
Desktop
Programming
Attributes
IP Configuration
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.1.5
Subnet Mask
255.255.255.0
Default Gateway
192.168.1.1
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
Link Local Address
FE80::2D0:FFFF:FE81:D78D
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top

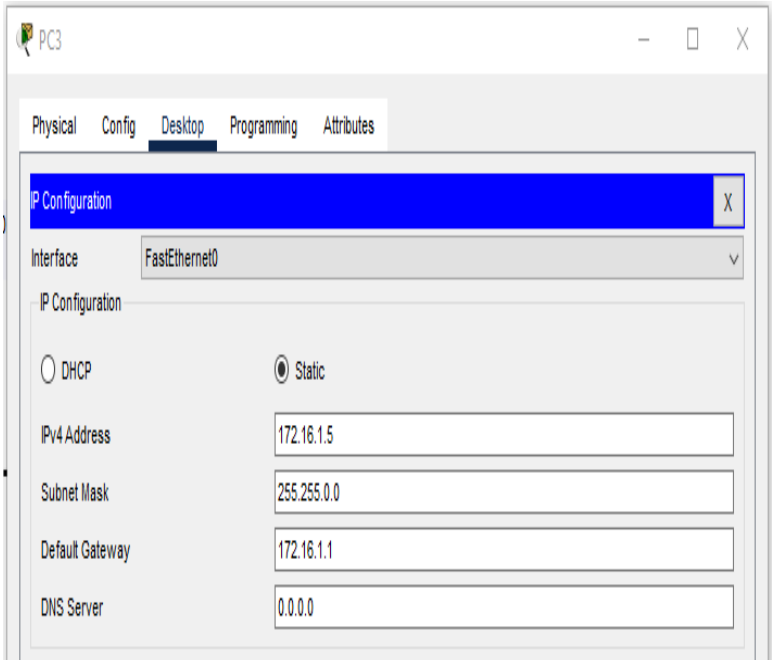


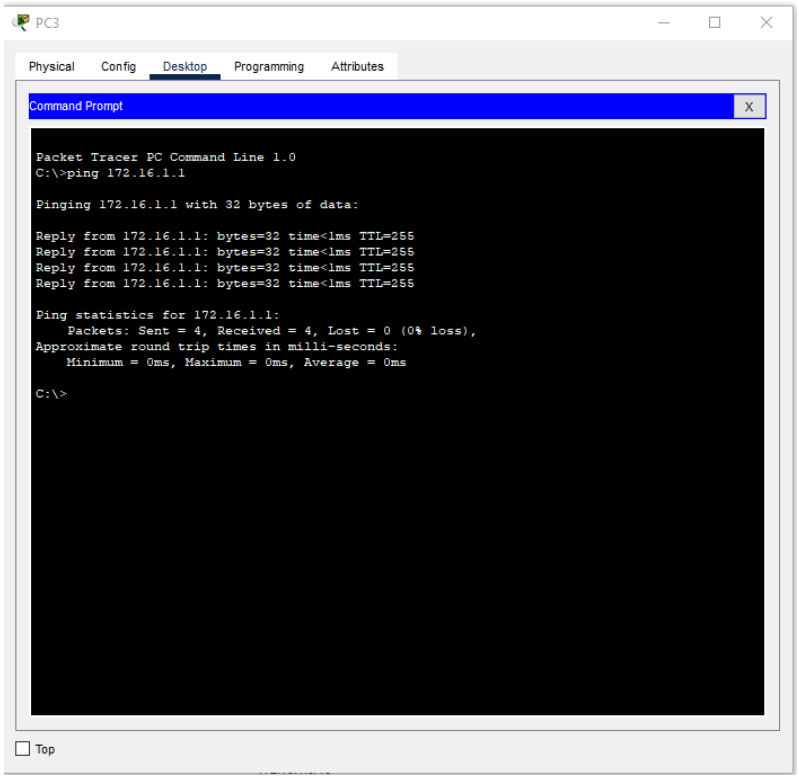
Την ίδια ακριβώς διαδικασία κάνουμε και μεταξύ των PC 2 και PC3 το οποίο έχει σαν αποτέλεσμα την επικοινωνία με το router 0. Παρακάτω εμφανίζονται οι εικόνες του Configuration και ένα ping για το συγκεκριμένο υποδίκτυο μεταξύ του PC3 και του router0


10.0.0.2
1841
Router0
172.16.1.1
2950T-24
Switch1
PC-PT
PC2
172.16.1.4
PC-PT
PC3
172.16.1.5
172.16.1.0/16

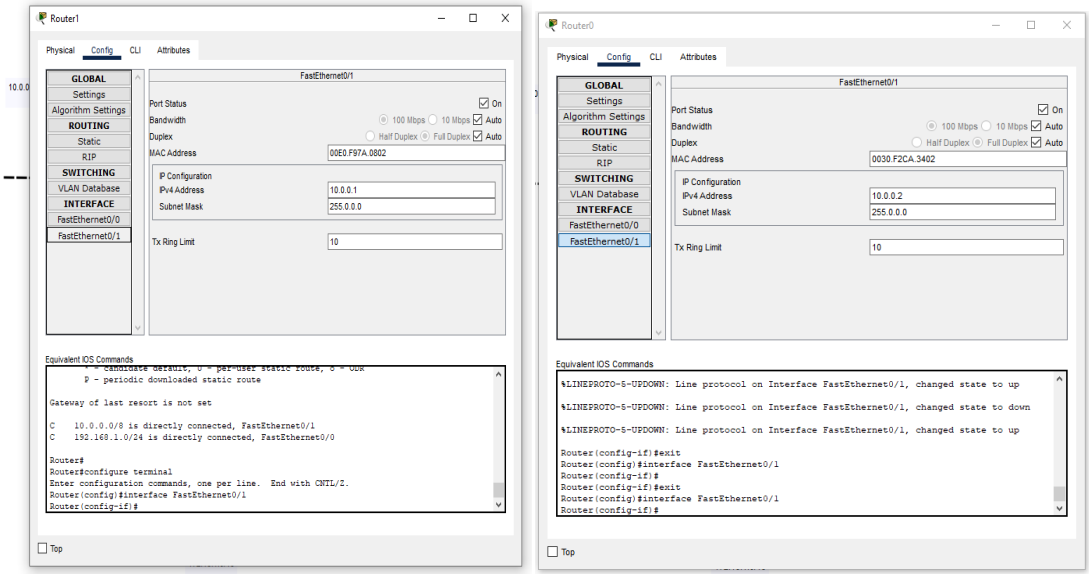

Router0
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
FastEthernet0/0
FastEthernet0/1
FastEthernet0/0
Port Status
On
Bandwidth
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
00D0.BAD3.8001
IP Configuration
IPv4 Address
172.16.1.1
Subnet Mask
255.255.0.0
Tx Ring Limit
10


PC2
Physical
Config
Desktop
Programming
Attributes
IP Configuration
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
172.16.1.4
Subnet Mask
255.255.0.0
Default Gateway
172.16.1.1
DNS Server
0.0.0.0

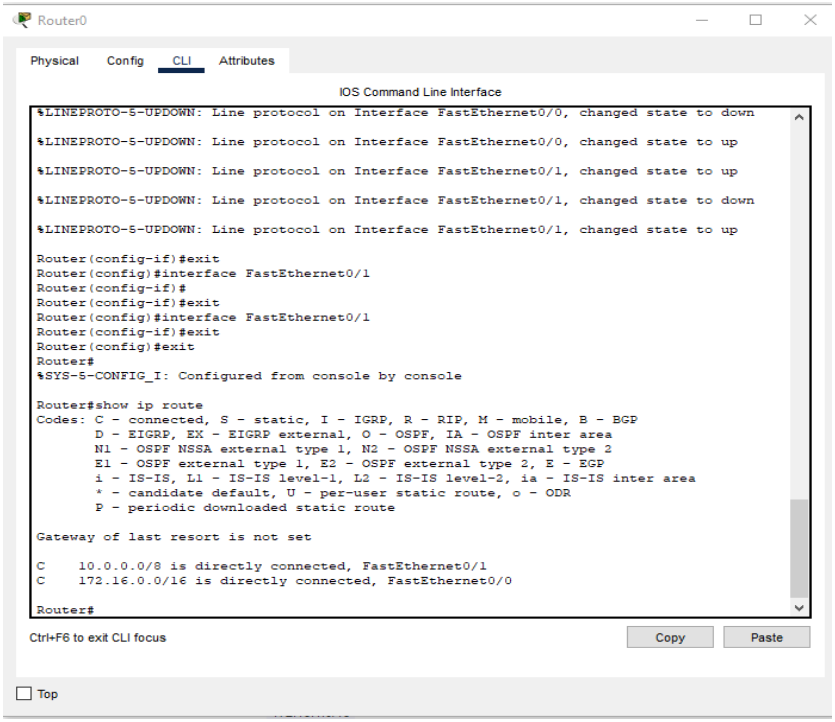

PC3
Physical
Config
Desktop
Programming
Attributes
IP Configuration
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
172.16.1.5
Subnet Mask
255.255.0.0
Default Gateway
172.16.1.1
DNS Server
0.0.0.0



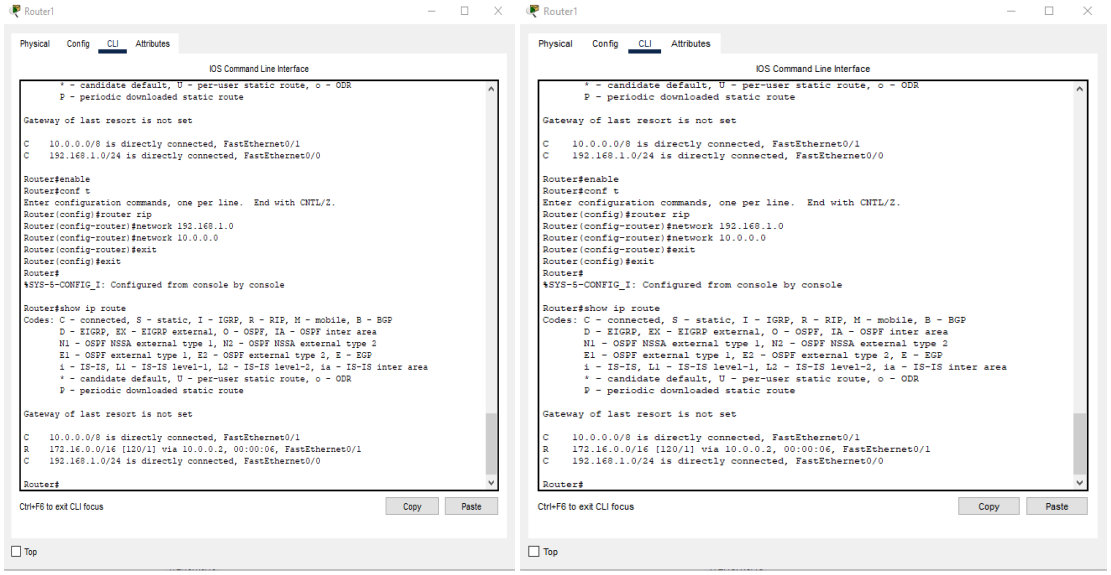
Το επόμενο βήμα Θα κάνω Διευθυνσιοδότηση μεταξύ τα ρούτερ για να μπορούν να επικοινωνούν ακόμη και οι πιο απομακρυσμένη κόμβοι. Η διαδικασία αυτή στην ουσία θα κάνει γνωστό στο άλλο router τα στοιχεία του απέναντι router. Αυτή τη στιγμή παίζεται με τίποτα διευθύνσεις IP του κάθε router ο κάθε router γνωρίζει Το δικό του το δίκτυο υποδίκτυο και μέχρι το απέναντι router 0 και router 1 διευθύνσεις παρουσιάζεται στις παρακάτω εικόνες



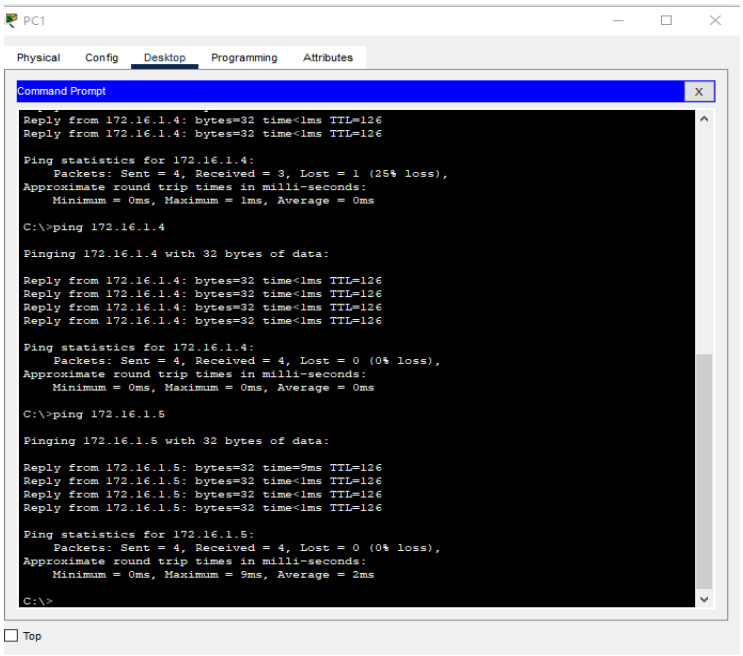
Τώρα πρέπει να πάμε στο CLI του κάθε router να βγούμε από το γραφικό περιβάλλον και να γράψουμε την εντολή show ip route για να δούμε ποια δίκτυα είναι συνδεδεμένα πάνω στο router



Το αποτέλεσμα που βλέπουμε είναι ότι βλέπουμε το μισό δίκτυο οπότε πρέπει να δώσουμε κάποιες εντολές και στα δυο router για να μπορούν να ανταλλάξουν στοιχεία ακόμη και πιο μακρινή κόμβοι του δικτύου .Οι εντολές που θα ακολουθήσουμε είναι πχ διπλό κλικ στο router 0>CLI>Enable>Configure Terminal >Router rip >px: network 192.168.1.0 και network 10.0.0.0 διότι δεν υπάρχει κάποια μάσκα υποδικτύωσης>exit>exit και εμφανίζεται όλο το δίκτυο όπως εμφανίζεται στις παρακάτω εικόνες.



Για να μας εμφανιστούν αυτά τα αποτελέσματα έπειτα από τα δύο exit έχουμε βγει στο router μας και πληκτρολογούμε την εντολή show ip route. Από τις παραπάνω εικόνες φαίνεται ότι τα δυο router αντάλλαξαν δεδομένα οπότε όλοι μπορούν να στείλουν σε όλους. Για να επαληθέψουμε ότι το δίκτυο δουλεύει θα κάνουμε πάμε για παράδειγμα στο PC1 > Desktop > Commant Prompt και θα κάνουμε ping την ip του PC3 και PC2 όπως φαίνεται στην παρακάτω εικόνα



Τα αποτελέσματα δείχνουν ότι η υποδικτύωση έχει ολοκληρωθεί με επιτυχία.

4.4 Στατική και Δυναμική δρομολόγηση και οι διαφορές τους

Η διαφορά μεταξύ στατικής και δυναμικής δρομολόγησης σχετίζεται με τον τρόπο εισόδου των πληροφοριών στο σύστημα. Η δρομολόγηση στη δικτύωση υπολογιστών έχει ως στόχο τα πακέτα να φτάσουν στον σωστό προορισμό τους.

Πιο συγκεκριμένα στην στατική δρομολόγηση, ο διαχειριστής εισάγει μη αυτόματα τις καταχωρήσεις δρομολόγησης στον πίνακα δρομολόγησης για κάθε δρομολογητή και υπολογιστή. Σε κάθε δρομολογητή, υπολογιστή υπάρχει ένας πίνακας ο οποίο εχει πληροφοριες και δείχνει το μοναδικό νούμερο για αυτήν την πόρτα του συστήματος. Για ένα μικρό δίκτυο η χρήση της στατικής δρομολόγηση είναι εφικτή από τη στιγμή που δεν υπάρχουν μετατροπές στο

δίκτυο. Το πλεονέκτημα της είναι ότι χρειάζεται λίγη επεξεργασία . Η μόνη ενέργεια είναι να κάνει αναζήτηση στον πίνακα δρομολόγησης για έναν συγκεκριμένο προορισμό. Αυτό έχει σαν αποτέλεσμα ότι δεν χρειάζεται πολύ εξελιγμένους επεξεργαστές .

Στη δυναμική δρομολόγηση οι καταχωρήσεις δρομολόγησης καταχωρούνται αυτόματα δημιουργώντας αλγόριθμους. Οι αλγόριθμοι δρομολόγησης είναι πολύπλοκη μαθηματικοί αλγόριθμοι όπου οι δρομολογητές διαφημίζουν σχετικά με τους συνδέσμους τους και χρησιμοποιώντας αυτές τις πληροφορίες, υπολογίζονται οι πιο ιδανικές διαδρομές. Αλγόριθμοι κατάστασης σύνδεσης και αλγόριθμοι διανύσματος απόστασης είναι οι πιο διάσημες μεθόδους .Το OSPF (Open Shortest Path First) είναι ένας αλγόριθμος που ακολουθεί έναν αλγόριθμο κατάστασης σύνδεσης και το RIP (Routing Information Protocol) είναι ένας αλγόριθμος που χρησιμοποιεί αλγόριθμο διανύσματος απόστασης. Για μεγάλα δίκτυα που έχουν μεγάλες αλλαγές κατά τη λειτουργία τους είναι ο ιδανικός τρόπος δρομολογησεις . Γενικά στην δυναμική δρομολόγηση οι πίνακες ενημερώνονται περιοδικά . Ακόμα η συμφόρηση και η δρομολόγηση προσαρμόζεται ανάλογα με τις συνθήκες που επικρατούν στο δίκτυο μας.Το μειονέκτημα της είναι ότι θα χρειαστεί σημαντική επεξεργασία. Επομένως, το κόστος ενός τέτοιου υλικού δρομολόγησης θα ήταν δαπανηρό.(https://el.strephonsays.com/static-and-vs-dynamic-routing-13268)

Κεφάλαιο 5: Διαφορές Cisco Packet Tracer στο IPv6

5.1 Η φιλοσοφία του Cisco Packet Tracer στο IPv6

Η διαμόρφωση μιας διεύθυνσης IPv6 είναι εξίσου εύκολη με τη διαμόρφωση μιας διεύθυνσης IPv4 σε μια επαφή Cisco. Υπάρχουν αρκετές εντολές που έχουν μεταφερθεί για να ταιριάζουν στις ανάγκες του IPv6 σε έναν δρομολογητή Cisco, όπως η σύντομη παρουσίαση διασύνδεσης ip για το ipv6 είναι η σύντομη διεπαφή εμφάνισης ipv6.
Για να διαμορφώσετε μια διεύθυνση IPv6 σε μια διεπαφή Cisco, θα χρησιμοποιήσετε την εντολή ipv6 X: X: X: X :: X / <0-128> σε λειτουργία διαμόρφωσης διεπαφής. Οι IPv6 δεν χρησιμοποιεί μάσκα υποδικτύου, αλλά χρησιμοποιεί τη σημείωση bit CIDR. Παραδείγματα Διεύθυνση IPv4 10.55.82.23/24, Διεύθυνση IPv6: 2001: dabd: 32bf :: 1/64. Το τμήμα αναγνωριστικού κεντρικού υπολογιστή μιας διεύθυνσης IPv6 έχει μήκος 64 bit που είναι το μισό της IPV6 διεύθυνσης. Τα υπόλοιπα 64 bits θα συμπληρωθούν από την αυτόματη αυτόματη διαμόρφωση που είναι ένα από τα μεγαλύτερα πλεονεκτήματα του IPv6. Η δυνατότητα ενός κόμβου αυτόματης διαμόρφωσης μιας καθολικής μοναδικής διεύθυνσης IPv6 χωρίς την χρήση του DHCP είναι πολύ χρήσιμο για τις επιχειρήσεις που θέλουν να έχουν το ίδιο αποτέλεσμα.

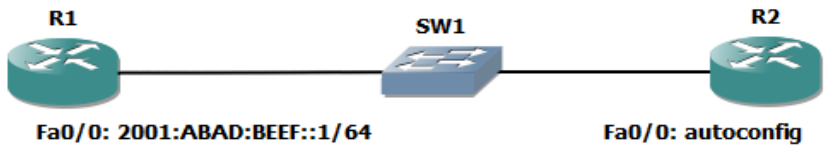
Το IPv6 χρησιμοποιεί έναν μηχανισμό που ονομάζεται Neighbor Discovery Protocol (NDP), ο οποίος παρέχει στο IPv6 τα μοναδικά χαρακτηριστικά plug-and-play. Το NDP εκτελεί διάφορες λειτουργίες που παρατίθενται παρακάτω:
Router Discovery - Η δυνατότητα ενός κόμβου να ανακαλύπτει τοπικούς δρομολογητές σε ένα τμήμα δικτύου χωρίς τη βοήθεια ενός διακομιστή DHCP.

Parameter Discovery - Η ικανότητα ενός κόμβου να ανακαλύπτει παραμέτρους συνδέσμων όπως MTU και όρια hop για τους συνδέσμους του.
Prefix Discovery - Η ικανότητα ενός κόμβου να ανακαλύπτει το πρόθεμα ή τα προθέματα που έχουν εκχωρηθεί σε έναν συγκεκριμένο σύνδεσμο IPv6.
Αυτόματη ρύθμιση παραμέτρων διεύθυνσης - Η δυνατότητα ενός κόμβου να καθορίζει την πλήρη μοναδική διεύθυνση i χωρίς τη βοήθεια διακομιστή DHCP.
Διπλότυπη ανίχνευση διευθύνσεων (DAD) - Η ικανότητα ενός κόμβου να καθορίζει μάλλον ή όχι μια διεύθυνση IPv6 που προσπαθεί να χρησιμοποιήσει υπάρχει ήδη.
Ανάλυση διευθύνσεων - Η δυνατότητα ενός κόμβου να ανακαλύπτει τις διευθύνσεις επιπέδου συνδέσμου άλλων κόμβων σε έναν σύνδεσμο χωρίς τη χρήση του πρωτοκόλλου επίλυσης διευθύνσεων (ARP).
Next-Hop Determination - Η ικανότητα ενός κόμβου να προσδιορίζει το επόμενο link-layer hop σε μια σύνδεση δικτύου. έναν τοπικό κόμβο ή προορισμό δρομολογητή.
Neighbor Unreachability Detection - Η δυνατότητα ενός κόμβου να καθορίζει πότε μια γειτονική συσκευή στη σύνδεση δικτύου δεν είναι πλέον προσβάσιμη.
Ανακατεύθυνση - Η δυνατότητα ενός δρομολογητή να ειδοποιεί έναν κεντρικό υπολογιστή ότι υπάρχει καλύτερη διαδρομή για να φτάσει σε έναν συγκεκριμένο προορισμό.
Τα μηνύματα Network Discovery Protocol θα πρέπει πάντα να προέρχονται από τοπικούς συνδέσμους , για λογούς ασφάλειας. Το Network Discovery Protocol ορίζεται στο RFC2461 το οποίο χρησιμοποιεί το ICMPv6 για την ανταλλαγή μηνυμάτων που απαιτούνται για τις λειτουργίες του. Συγκεκριμένα, ορίζονται πέντε νέα μηνύματα ICMPv6 στο RFc2461 τα οποία γνωρίζετε. Αυτά τα μηνύματα που αναφέρονται παρακάτω είναι υπεύθυνα για τη λειτουργία του NDP.
Router Advertisement (RA) - Ένα RA είναι ένα μήνυμα που προέρχεται από ένα Router, (Cisco ή non-Cisco) για να διαφημίσει την ύπαρξή τους σε έναν σύνδεσμο δικτύου. Αυτές οι RA περιλαμβάνουν επίσης παραμέτρους συνδέσμου και αποστέλλονται αυτόματα περιοδικά και σε απάντηση ενός μηνύματος Router Solicitation (RS).

Router Solicitation (RS) - Αυτά τα μηνύματα προέρχονται από κόμβους κεντρικού υπολογιστή για να ζητήσουν από οποιονδήποτε δρομολογητή στον σύνδεσμο να ανταποκριθεί με RA.
Neighbor Solicitation (NS) - Αυτά τα μηνύματα αποστέλλονται από έναν κόμβο που ζητά τη διεύθυνση επιπέδου συνδέσμου ενός άλλου κόμβου και χρησιμοποιούνται επίσης από τους μηχανισμούς ανίχνευσης διπλότυπων διευθύνσεων και ανίχνευσης γειτονικών.
Neighbor Advertisement (NA) - Αυτά τα μηνύματα αποστέλλονται ως απάντηση σε ένα μήνυμα NS. Εάν ένας κόμβος αλλάξει τη διεύθυνση του επιπέδου συνδέσμου, τότε ένα NA μπορεί να χρησιμοποιηθεί για την αποστολή μιας ανεπιθύμητης διαφήμισης για να διαφημίσει τη νέα του διεύθυνση.
Ανακατεύθυνση - Αυτά τα μηνύματα χρησιμοποιούνται με τον ίδιο τρόπο όπως το IPv4 ICMP ανακατευθύνσεις, ωστόσο έχουν μεταφερθεί από το ICMP στο IPv4 σε εγγενή λειτουργία NDP που χρησιμοποιεί το ICMPv6 για να λειτουργήσει.

5.2 Θεωρητικό παράδειγμα για IPV6

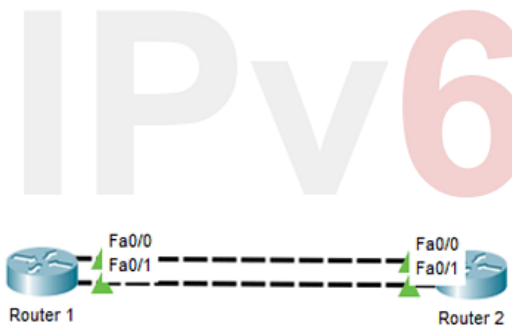
Σε αυτό το παράδειγμα θα δείξουμε την επικοινωνία ενός router με ενδιάμεσα ένα switch.



Για να διαμορφώσουμε έναν δρομολογητή Cisco πρέπει πρώτα να ενεργοποιήσετε τη δρομολόγηση unvast IPv6 σε αυτόν τον δρομολογητή εκτελώντας την εντολή ipv6 unicast-routing.Στην συνέχεια θα πρέπει να διαμορφώσουμε το πρόθεμα χρησιμοποιώντας την εντολή ipv6 nd x: x: x: x :: / x σε

λειτουργία διαμόρφωσης διεπαφής. Μόλις διαμορφωθεί το πρόθεμα, ο δρομολογητής θα διαφημίσει το πρόθεμα διεπαφής που καθορίζεται περιοδικά στο Network Discovery Protocol (NDP) Router Advertisements (RA) και μετά τη λήψη ενός Router Solicitation (RS).

5.3 Εντολές Υλοποίηση IPv6 Πάνω στο Cisco Packet Tracer.



1 βήμα→Enable IPv6 Globally(Ενεργοποιήστε το IPv6 παγκοσμίως)

Router 1# **configure terminal**

Router 1(config)# **ipv6 unicast-routing**

Router 2# **configure terminal**

Router 2(config)# **ipv6 unicast-routing**

Με την εντολή ipv6 unicast-routing το IPv6 ενεργοποιείται παγκοσμίως στον δρομολογητή

2 βήμα -> Enable IPv6 on Interface(Ενεργοποίηση IPv6 στη διεπαφή)

Router 1 (config)# **interface FastEthernet0/0**

Router 1 (config-if)# **ipv6 enable**

Router 1 (config-if)# **no shutdown**

Router 1 (config)# **interface FastEthernet0/1**

Router 1 (config-if)# **ipv6 enable**

Router 1 (config-if)# **no shutdown**

Router 2 (config)# **interface FastEthernet0/0**

Router 2 (config-if)# **ipv6 enable**

Router 2 (config-if)# **no shutdown**

Router 2 (config)# **interface FastEthernet0/1**

Router 2 (config-if)# **ipv6 enable**

Router 2 (config-if)# **no shutdown**

Αφού ενεργοποιήσουμε το IPv6 παγκοσμίως, θα πρέπει να ενεργοποιήσουμε το IPv6 στις διεπαφές. Έτσι χρησιμοποιήσουμε την εντολή "ipv6 enable"

3 βήμα-> Configure EUI-64 Format Global Unicast Address(Ρύθμιση παραμέτρων EUI-64 Format Global Unicast Address)

Router 1 (config)# **interface FastEthernet0/0**

Router 1(config-if)# **ipv6 address 2001:AAAA:BBBB:CCCC::/64 eui-64**

Router 1(config-if)# **end**

Let's check the IPv6 address that is created with EUI-64 format with "**show ipv6 interface brief**" command.

Router 1# **sho ipv6 interface brief**

FastEthernet0/0 [up/up]

FE80::2E0:B0FF:FE0E:7701

2001:AAAA:BBBB:CCCC:2E0:B0FF:FE0E:7701

FastEthernet0/1 [up/up]

FE80::2E0:B0FF:FE0E:7702

Vlan1 [administratively down/down]

Unassigned

Για να διαμορφώσετε μια διεπαφή με μορφή EUI-64, καταρχάς θα πάμε κάτω από τη διεπαφή και μετά θα χρησιμοποιήσουμε την εντολή "ip address ipv6-address / prefix-length eui-64". Εδώ, η διεύθυνση IPv6 και το μήκος προθέματος είναι το 2001: AAAA: BBBB: CCCC :: / 64. Η πραγματική EUI-64 Global Unicast Διεύθυνση θα δημιουργηθεί με αυτήν τη διεύθυνση και διεύθυνση MAC μετά τη διαμόρφωση IPv6.

4 βήμα-> Configure Manual Link Local Address(Διαμόρφωση μη αυτόματης σύνδεσης ιδιωτικής διεύθυνσης)

Router 2 (config)# **interface FastEthernet0/0**

Router 2 (config-if)# **ipv6 address 2001:AAAA:BBBB:CCCC:1234:1234:1234:1234/64**

Router 2(config-if)# **end**

Router 2# **show ipv6 interface brief**

FastEthernet0/0 [up/up]

FE80::206:2AFF:FE15:BD01

2001:AAAA:BBBB:CCCC:1234:1234:1234:1234

FastEthernet0/1 [administratively up/up]

FE80::206:2AFF:FE15:BD02

Vlan1 [administratively down/down]

Unassigned

Εάν δεν χρησιμοποιούμε διεύθυνση μορφής EUI-64, πρέπει να γράψουμε ολόκληρη τη διεύθυνση IPv6 στη γραμμή διαμόρφωσης

5 βήμα->IPv6 Ping (Επικοινωνία IPv6)

Router 1# **ping ipv6 2001:AAAA:BBBB:CCCC:1234:1234:1234:1234**

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 2001:AAAA:BBBB:CCCC:1234:1234:1234:1234, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

Router 1# **show ipv6 interface FastEthernet0/0**

2001:AAAA:BBBB:CCCC:2E0:B0FF:FE0E:7701, subnet is **2001:AAAA:BBBB:CCCC::/64 [EUI]**

Router 2# **show ipv6 interface FastEthernet0/0**

2001:AAAA:BBBB:CCCC:1234:1234:1234:1234, subnet is **2001:AAAA:BBBB:CCCC::/64**

6 βήμα->Manual Link Local Address Configuration(Μη αυτόματη διαμόρφωση ιδιωτικής διεύθυνσης)

Router 1 (config)# **interface FastEthernet0/1**

Router 1 (config-if)# **ipv6 address FE80::AAAA:BBBB:CCCC:DDDD link-local**

Router 1 (config-if)# **end**

Router 1# **show ipv6 interface brief**

FastEthernet0/0 [up/up]

FE80::2E0:B0FF:FE0E:7701

2001:AAAA:BBBB:CCCC:2E0:B0FF:FE0E:7701

FastEthernet0/1 [administratively down/down]

FE80::AAAA:BBBB:CCCC:DDDD

Vlan1 [administratively down/down]

unassigned

Με την εντολή **show ipv6 interface brief ελέγχουμε** τη μη αυτόματη ρύθμιση παραμέτρων ipv6.

7 βήμα->Auto IPv6 Address Configuration(Αυτόματη διαμόρφωση διεύθυνσης IPv6)

Router 2 (config)# **interface FastEthernet0/1**

Router 2 (config-if)# **ipv6 address autoconfig**

Router 2 (config-if)# **end**

Router 2# **show ipv6 interface brief**

FastEthernet0/0 [up/up]

FE80::206:2AFF:FE15:BD01

2001:AAAA:BBBB:CCCC:1234:1234:1234:1234

FastEthernet0/1 [up/down]

FE80::206:2AFF:FE15:BD02

Vlan1 [administratively down/down]

unassigned

Αν κάνουμε ping από το Router 2 στο Router 1 βαζουμε

Router 2# **ping ipv6 FE80::AAAA:BBBB:CCCC:DDDD**

Output Interface: **FastEthernet0/1**

ype escape sequence to abort.

Sending 5, 100-byte ICMP Echos to FE80::AAAA:BBBB:CCCC:DDDD, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

Οι διευθύνσεις IPv6 μπορούν να ρυθμιστούν αυτόματα. Αυτό είναι ένα από τα πιο σημαντικά χαρακτηριστικά που συνοδεύει το IPv6. Για την αυτόματη διαμόρφωση IPv6, θα χρησιμοποιήσουμε την εντολή "ipv6 autoconfig".

8 βήμα->Enable DHCPv6 Client(Ενεργοποίηση πελάτη DHCPv6)

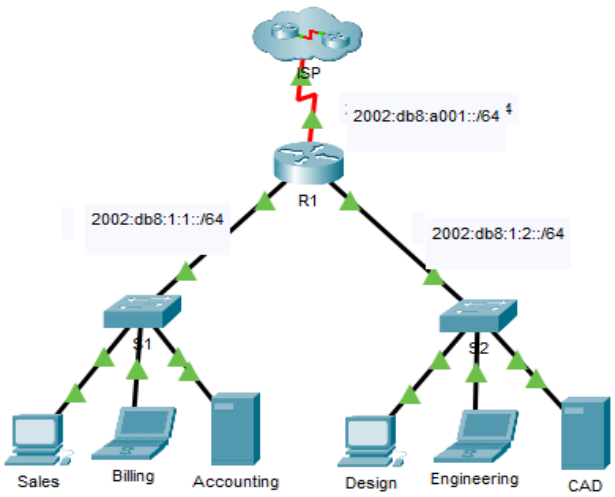
Router 1 (config)# **interface FastEthernet0/1**

Router 1 (config-if)# **ipv6 address dhcp**

Router 1 (config)# **end**

Για να ενεργοποιήσουμε τη λειτουργία DHCPv6 χρησιμοποιούμε την **εντολή "ipv6 address dhcp"** κάτω από αυτήν τη διεπαφή

5.4 Άσκηση με ISP πάνω στο Cisco Packet Tracer

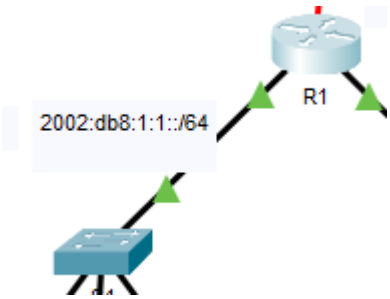


Device	Interface	IPv6 Address/Prefix	Default Gateway
R1	G0/0	2002:DB8:1:1::1/64	N/A
	G0/1	2002:DB8:1:2::1/64	N/A
	S0/0/0	2002:DB8:1:A001::2/64	N/A
	Link-local	FE80::1	N/A
Sales	NIC	2002:DB8:1:1::2/64	FE80::1
Billing	NIC	2002:DB8:1:1::3/64	FE80::1
Accounting	NIC	2002:DB8:1:1::4/64	FE80::1
Design	NIC	2002:DB8:1:2::2/64	FE80::1
Engineering	NIC	2002:DB8:1:2::3/64	FE80::1
CAD	NIC	2002:DB8:1:2::4/64	FE80::1

Μέρος 1: Διαμόρφωση διεύθυνσης IPv6 στο δρομολογητή

Βήμα 1 :

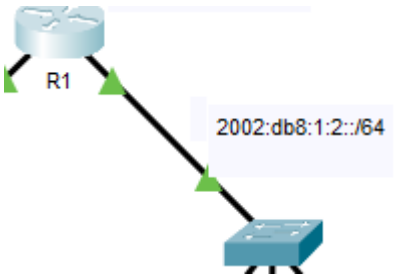
Κάνουμε κλικ στο R1 δρομολογητή>Cli>enable(Έτσι μπαίνουμε στο Exec mode)>config term>ipv6 unicast-routing>int g0/0(η πόρτα που ενωνεται με το switch 1)>ipv6 address 2002:db8:1:1::1/64>ipv6 address fe80::1 link-local>no shutdown



Αυτές τις κινήσεις της κάναμε για να επικοινωνήσει το router με αυτή την πλευρά του δικτύου μας .

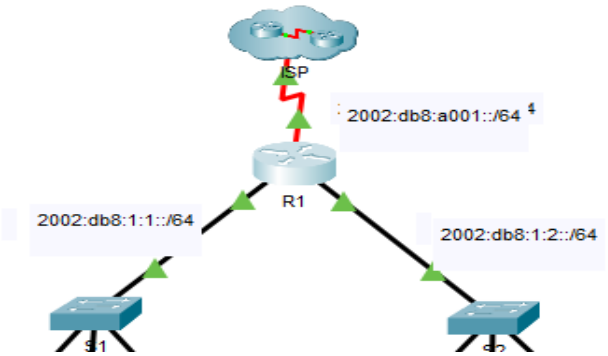
Βήμα 2 :

int g0/1(η πόρτα που ενωνεται με το switch 2)>ipv6 address 2002:db8:1:2::1/64>ipv6 address fe80::1 link-local>no shutdown



Βήμα 3 :

int s0/0/0>ipv6 address 2002:db8:1:a001::2/64>ipv6 address fe80::1 link-local>no shutdown



Εισαγάγουμε τις απαραίτητες εντολές για μετάβαση σε λειτουργία διαμόρφωσης διεπαφής για το Serial 0/ 0/0.

Βήμα 4:

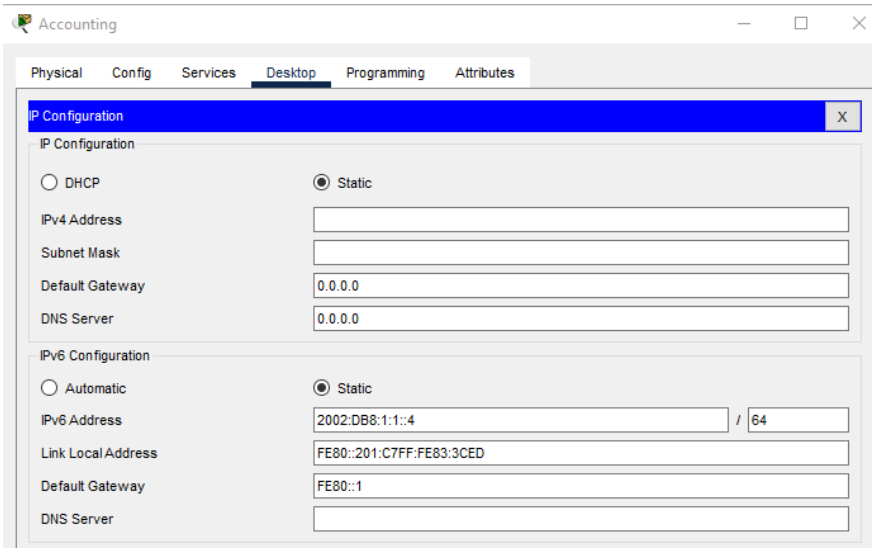
Exit>exit>show ip interface brief

Αποτέλεσμα : igabitEthernet0/0 [up/up]
FE80::1
2002:DB8:1:1::1
GigabitEthernet0/1 [up/up]
FE80::1
2002:DB8:1:2::1
GigabitEthernet0/2 [administratively down/down]
unassigned
Serial0/0/0 [up/up]
FE80::1
2002:DB8:1:A001::2
Serial0/0/1 [administratively down/down]
unassigned
Vlan1 [administratively down/down]

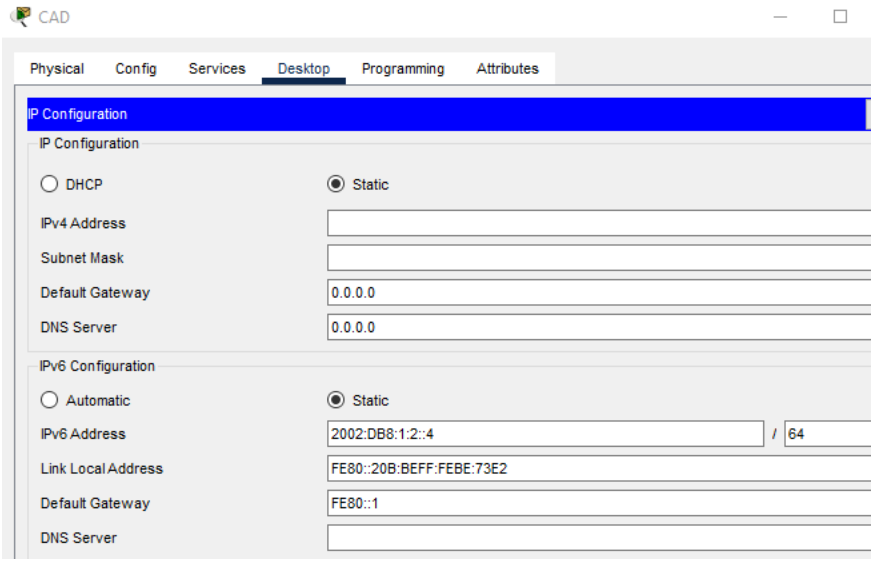
Unassigned

Μέρος Β: Διαμόρφωση διευθύνσεων IPv6 στους διακομιστές

Κάνουμε κλικ στο Accounting> Desktop tab > IP Configuration και προσθέτουμε τις τιμές IPv6 Adress: 2002:DB8:1:1::4/64 και Default Getaway: FE80::1 συμφώνα με τον πινάκα.

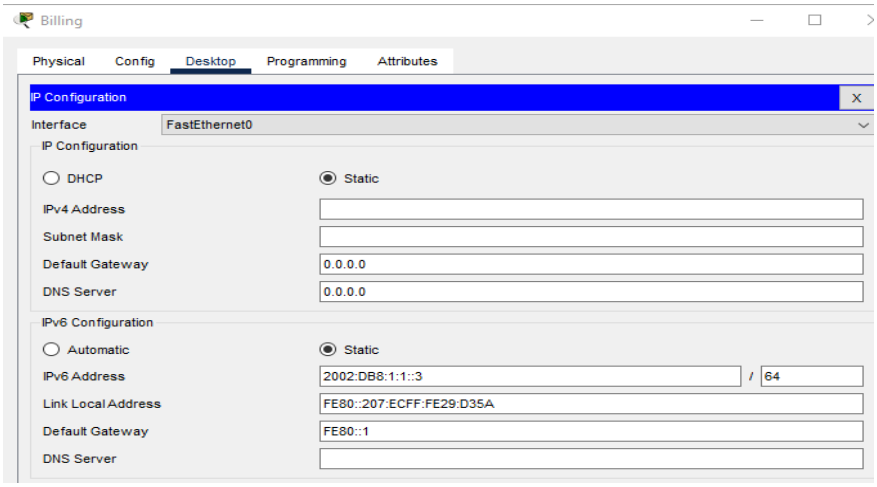


Την ιδία διαδικασία κάνουμε και στο GAD και προσθέτουμε τις τιμές IPv6 Adress: 2002:DB8:1:2::4/64 και Default Getaway: FE80::1 συμφώνα με τον πινάκα.

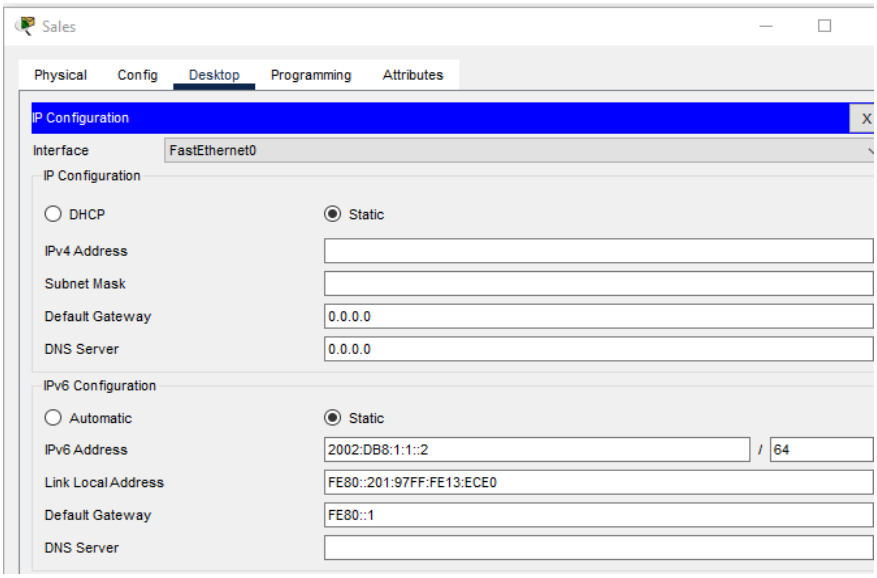


Μέρος 3: Ρύθμιση παραμέτρων IPv6 που απευθύνεται στους πελάτες.

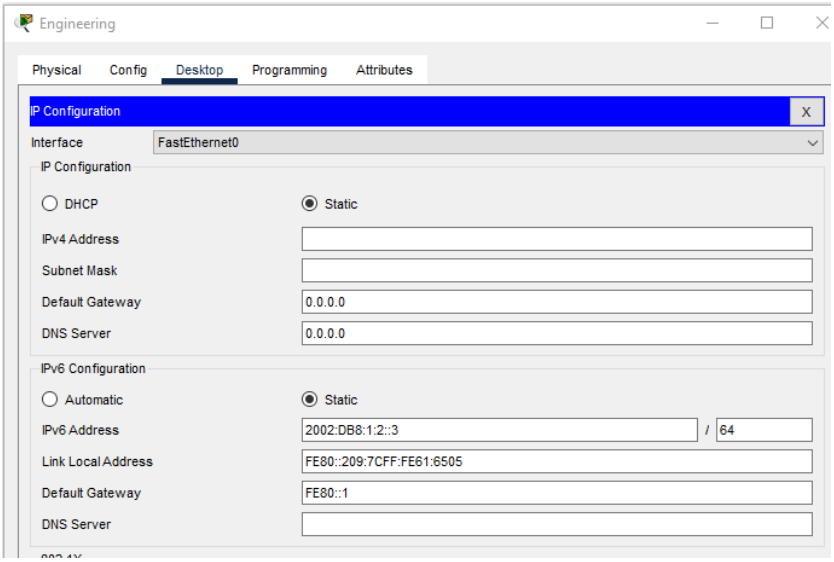
Πάμε στο biling και προσθέτουμε τις τιμές IPv6 Adress: 2002:DB8:1:1::3/64 και Default Getaway: FE80::1 συμφώνα με τον πινάκα.



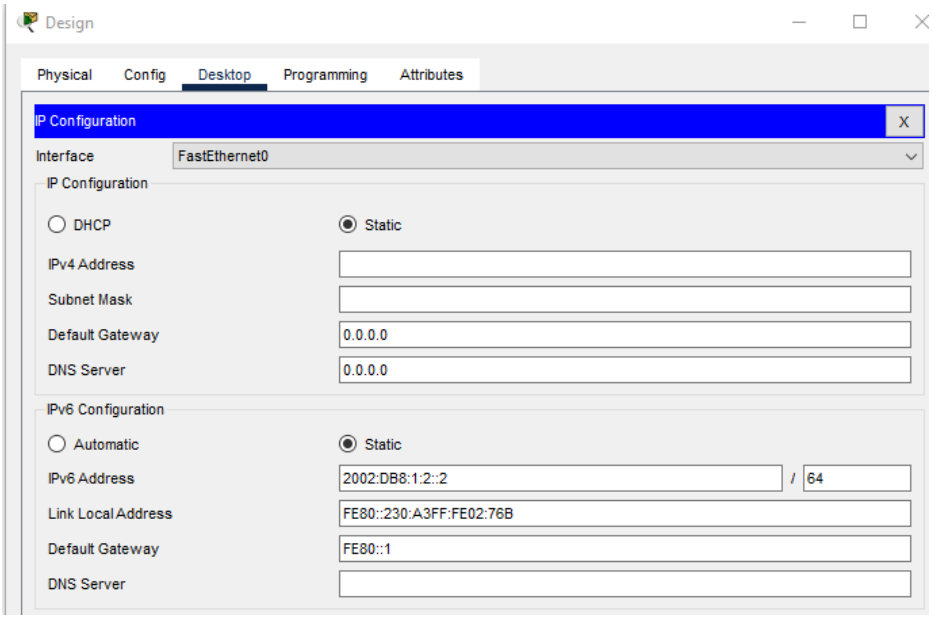
Στο sales και προσθέτουμε τις τιμές IPv6 Adress: 2002:DB8:1:1::2/64 και Default Getaway: FE80::1 συμφώνα με τον πινάκα.



Στο Engineering προσθέτουμε τις τιμές IPv6 Adress : 2002:DB8:1:2::3/64 και Default Getaway: FE80::1 συμφώνα με τον πινάκα.



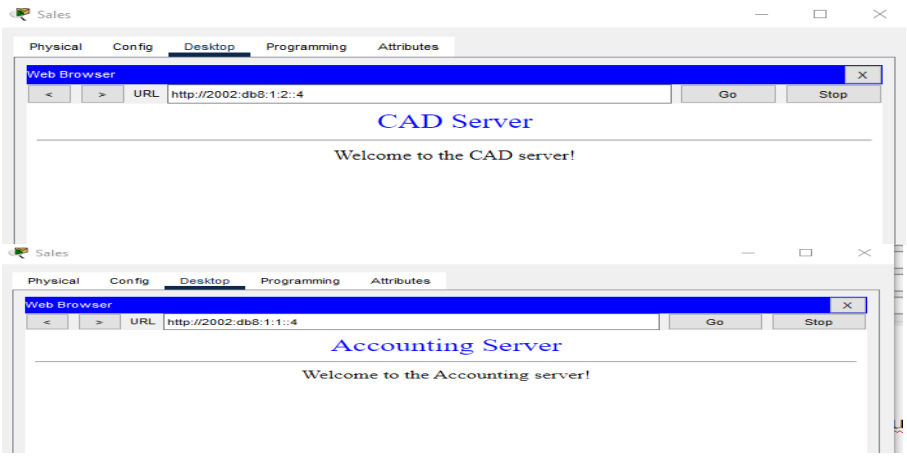
Στο Desing και προσθέτουμε τις τιμές IPv6 Adress: 2002:DB8:1:2::2/64 και Default Getaway: FE80::1συμφωνα με τον πινάκα.



Μέρος 4: Δοκιμή και επαλήθευση συνδεσιμότητας δικτύου

Βήμα 1:Ανοιγουμε μια σελίδα από ένα Pc

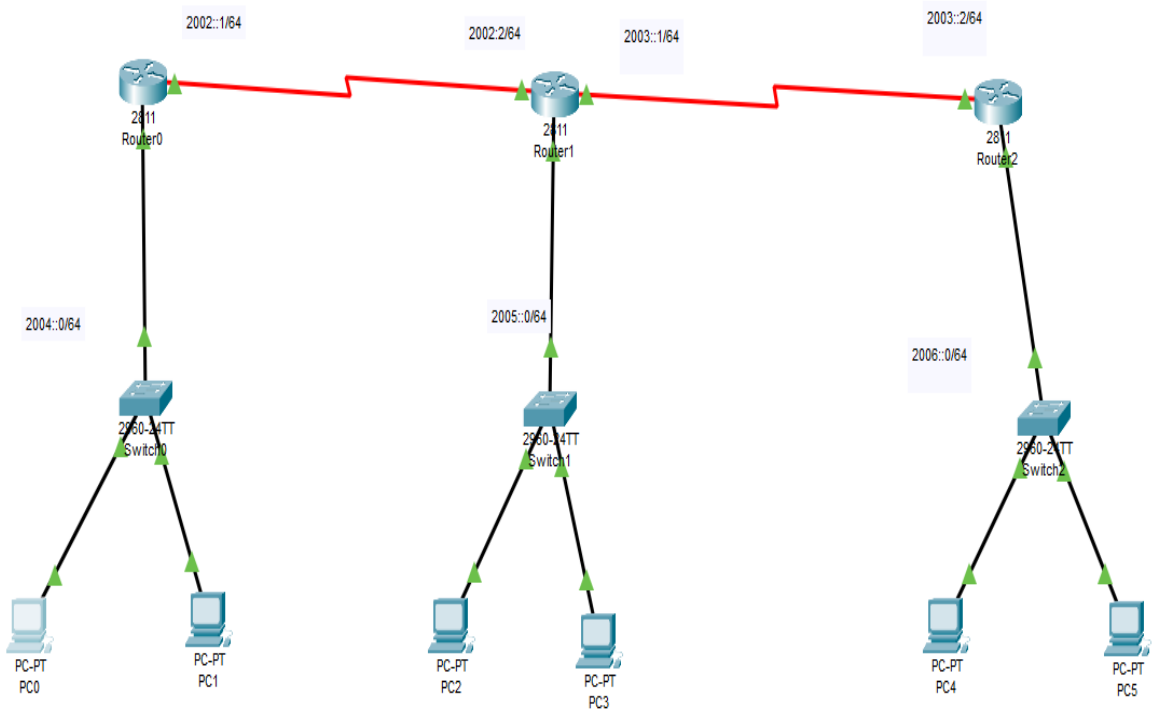
Θα πάμε στο seles desing στα δυο Pc και θα τα συνδέσουμε με τους διακομηστες.Στο seles διπλό κλικ>Desktop>wed server και θα γράψουμε 2002:db8:1:1::4 και θα πατήσουμε go για να μπούμε στο server του Acounting.Για να συνδεθούμε στους sever του GAD γραφούμε την διεύθυνση 2002:db8:1:2::4.Το ίδιο κάνουμε και στο desing με τις ίδιες διευθύνσεις



Βήμα 2:Κανουμε ping στο ISP

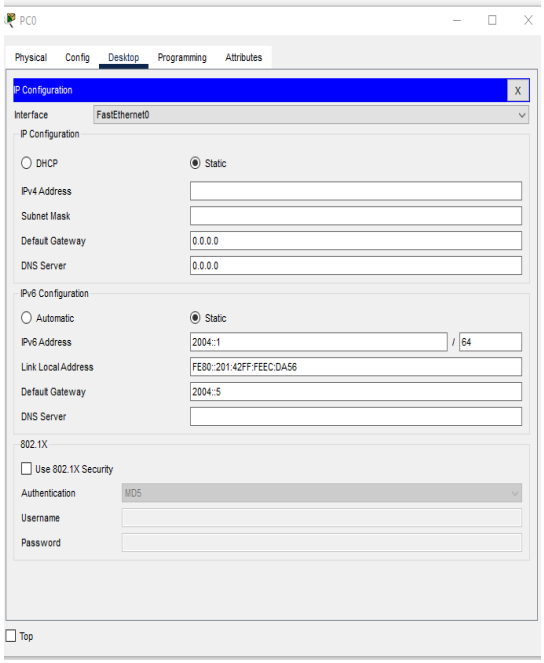
Πάμε στο sales και στο design και γραφούμε ping 2002:1:a001:1 και επικοινωνεί με το ICP

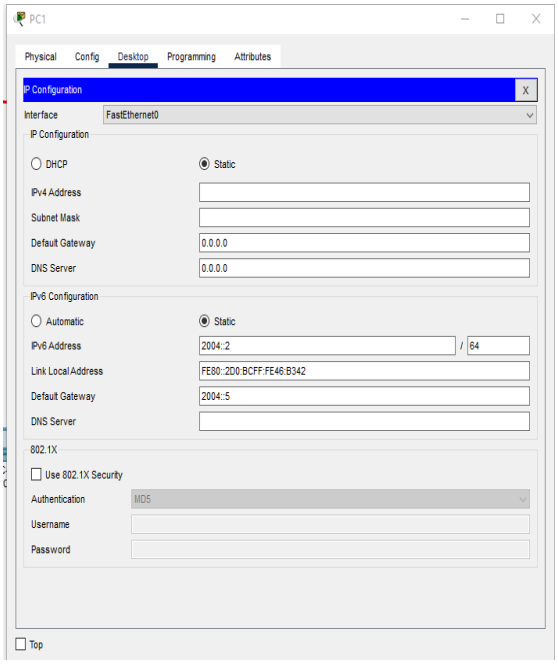
5.5 Άσκηση με επικοινωνία router πάνω στο Cisco Packet Tracer

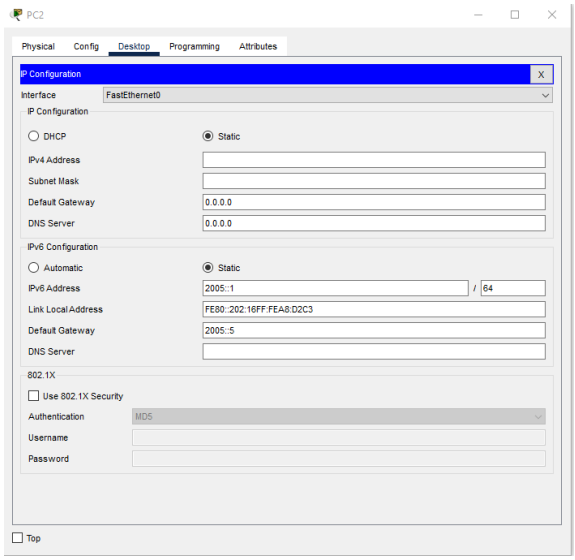


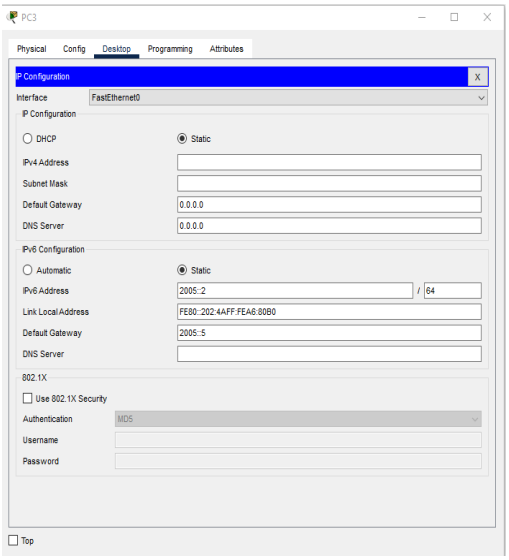
Device	Interface	IPv6 Address/Prefix	Default Gateway
Router 0	S0/1/0	2002::1/64	N/A
	Link-local	2004::5/64	N/A
Router 1	S0/1/0	2002::2/64	N/A
	S0/1/1	2003::1/64	N/A
	Link-local	2005::5/64	N/A
Router 2	0/1/0	2003::5/64	N/A
	Link-local	2006::5/64	N/A
Pc0	NIC	2004::1/64	2004::5
Pc1	NIC	2004::2/64	2004::5
Pc2	NIC	2005::1/64	2005::5
Pc3	NIC	2005::2/64	2005::5
Pc4	NIC	2006::2/64	2006:5
Pc5	NIC	2006::2/64	2006::5

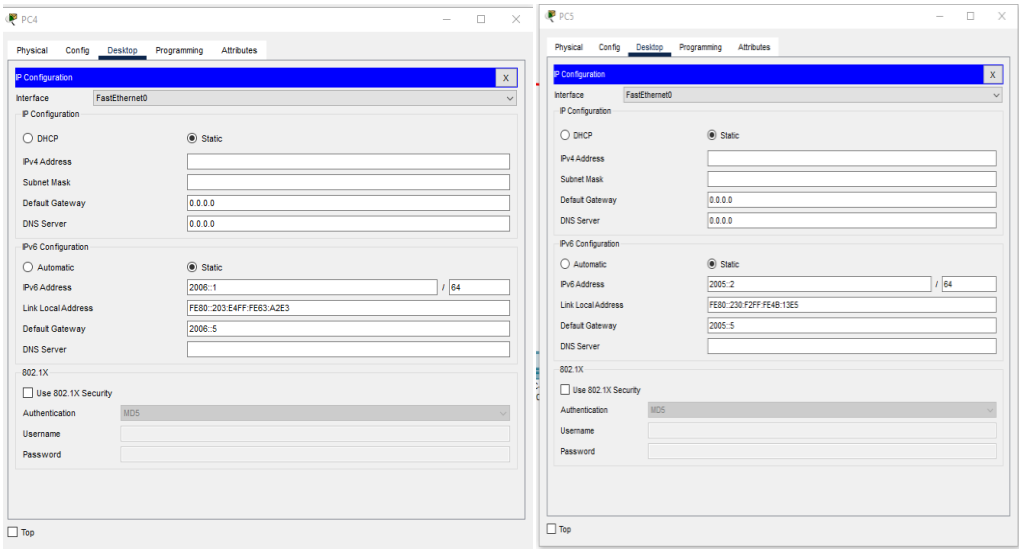
Βήμα 1:Διευθυνσεις στα Pc μας όπως στις παρακατω εικόνες.







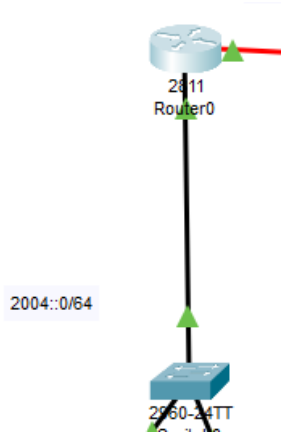




Βήμα 2:

Αφού έχουν άριστοι οι διευθύνσεις των pc θα πρέπει να ορίσουμε παραμέτρους στα router μας.Κάνουμε κλικ στο Pc0>cli>enable> config term>inter ser 0/1/0>ipv6 enable>ipv6 address 2002::2/64>clock rate 64000>no shutdown

Inter fa 0/0>ipv6 address 2004::5/64>ipv6 enable>no shut>end



Show ipv6 int br

Αποτέλεσμα :

FastEthernet0/0 [up/up]

FE80::20C:85FF:FE79:2D01

2004::5

FastEthernet0/1 [administratively down/down]

unassigned

Serial0/1/0 [up/up]

FE80::20C:85FF:FE79:2D01

2002::1

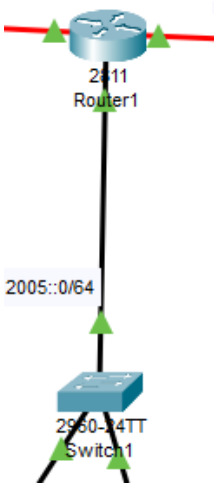
Serial0/1/1 [administratively down/down]

unassigned

Vlan1 [administratively down/down]

Unassigned

Στην συνεχεία κάνουμε κλικ στο router1>Cli>enable> config term>inter fa 0/0>ipv6 enable>ipv6 address 2005::5/64> no shut



Inter ser 0/1/0 >ipv6 enable>ipv6 address 2002::2/64>no shut>do ping 2002::2/64

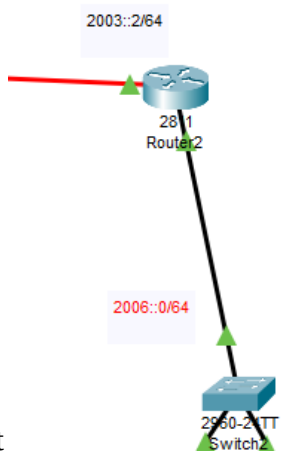

```
Router(config)#do ping 2002::1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2002::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/13/23 ms

Router(config)#
```

Inter ser 0/1/1>ipv6 enable>ipv6 add 2003::1/64>no shut>do wr

Στην συνεχεια κάνουμε κλικ στο router2>Cli>conf t>inter fa 0/0>ipv6 enable>ipv6 address

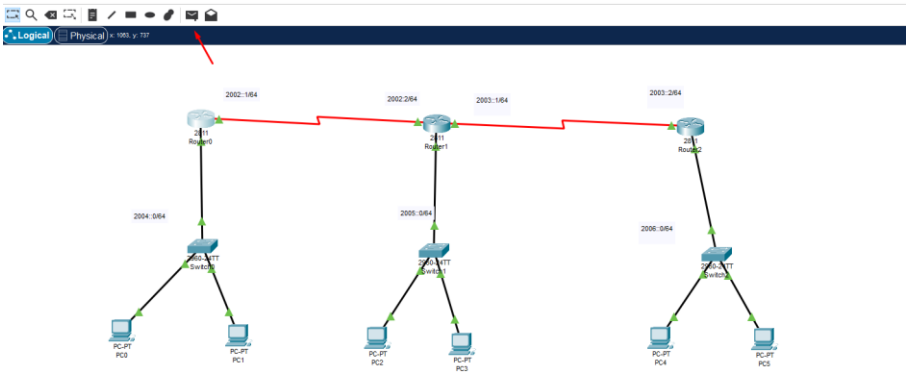


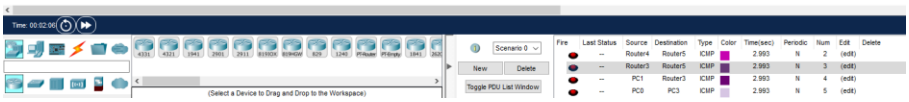
2006::5/64> no shut

Inter ser 0/1/0>Ipv6 enable>Ipv6 address 2003::2/64>no shut>do wr

Μέρος 3:Ping

Το επόμενο βήμα είναι να προσπαθήσουμε να κάνουμε μερικά Ping μεταξύ των router και τον συσκευων.Θα το κάνουμε με έναν πιο γρήγορο τρόπο στο πρόγραμμα μας.Θα κάνουμε κλικ στις κουμπάκι Add simle Pdu και θα μας εμφανιστούν τα ping στον κάτω μέρος της οθόνης όπως στην φωτογραφία παρακατω


Logical
Physical
2002::1/64
2002:2/64
2003::1/64
2003::2/64
2004::0/64
2005::0/64
2006::0/64
PC-PT PC0
PC-PT PC1
PC-PT PC2
PC-PT PC3
PC-PT PC4
PC-PT PC5


(Select a Device to Drag and Drop to the Workspace)
New
Delete
Toggle PDU List Window

Amante, S. *et al.* (2011) 'IPv6 Flow Label Specification'. RFC Editor (Request for Comments). doi: 10.17487/RFC6437.

Amante, S. and Carpenter, B. E. (2011) 'Using the IPv6 Flow Label for Equal Cost Multipath Routing and Link Aggregation in Tunnels'. RFC Editor (Request for Comments). doi: 10.17487/RFC6438.

Atkinson, R. and Kent, S. (1998) 'Security Architecture for the Internet Protocol'. RFC Editor (Request for Comments). doi: 10.17487/RFC2401.

Baker, F. *et al.* (1998) 'Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers'. RFC Editor (Request for Comments). doi: 10.17487/RFC2474.

Borman, D. A., Deering, D. S. E. and Hinden, B. (1999) 'IPv6 Jumbograms'. RFC Editor (Request for Comments). doi: 10.17487/RFC2675.

Carpenter, B. E., Jiang, S. and Tarreau, W. (2014) 'Using the IPv6 Flow Label for Load Balancing in Server Farms'. RFC Editor (Request for Comments). doi: 10.17487/RFC7098.

Cerf, V. and Kahn, R. (1974) 'A Protocol for Packet Network Intercommunication', *IEEE Transactions on Communications*, 22(5), pp. 637–648. doi: 10.1109/TCOM.1974.1092259.

Chown, T., Loughney, J. A. and Winters, T. (2019) 'IPv6 Node Requirements'. RFC Editor (Request for Comments). doi: 10.17487/RFC8504.

Cisco (2020) *Cisco Annual Internet Report (2018–2023) White Paper*. Available at: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html (Accessed: 12 February 2021).

Cisco (no date) *IP Mobility*. Available at: https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Data_Center/DCI/5-0/LISPmobility/DCI_LISP_Host_Mobility/LISPmobile_1.pdf (Accessed: 15 February 2021).

Deering, D. S. E. and Hinden, B. (2006) 'IP Version 6 Addressing Architecture'. RFC Editor (Request for Comments). doi: 10.17487/RFC4291.

Deering, S. and Hinden, R. (1998) 'RFC2460: Internet Protocol, Version 6 (IPv6) Specification'. USA: RFC Editor.

Doraswamy, N., Glenn, K. R. and Thayer, R. L. (1998) 'IP Security Document Roadmap'. RFC Editor (Request for Comments). doi: 10.17487/RFC2411.

Egevang, K. B. and Francis, P. (1994) 'The IP Network Address Translator (NAT)'. RFC Editor (Request for Comments). doi: 10.17487/RFC1631.

Egevang, K. B. and Srisuresh, P. (2001) 'Traditional IP Network Address Translator (Traditional NAT)'. RFC Editor (Request for Comments). doi: 10.17487/RFC3022.

Fuller, V. *et al.* (1993) 'Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy'. RFC Editor (Request for Comments). doi: 10.17487/RFC1519.

Fuller, V. and Li, T. (2006) 'Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan'. RFC Editor (Request for Comments). doi: 10.17487/RFC4632.

Graziani, R. (2017) *IPv6 Fundamentals: A Straightforward Approach to Understanding IPv6, Second Edition*. Cisco Systems, Inc.

Gupta, M. and Conta, A. (2006) 'Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification'. RFC Editor (Request for Comments). doi: 10.17487/RFC4443.

Haberman, B. and Hinden, B. (2005) 'Unique Local IPv6 Unicast Addresses'. RFC Editor (Request for Comments). doi: 10.17487/RFC4193.

Hassan, R. and Jabbar, R. (2017) ‘End-to-end (e2e) Quality of Service (QoS) for IPv6 video streaming’, *International Conference on Advanced Communication Technology, ICACT*, pp. 1–4. doi: 10.23919/ICACT.2017.7890045.

Holder, D. (2019) *Common misconceptions about IPv6 security*. Available at: https://blog.apnic.net/2019/03/18/common-misconceptions-about-ipv6-security/ (Accessed: 18 February 2021).

Holdrege, M. and Srisuresh, P. (1999) ‘IP Network Address Translator (NAT) Terminology and Considerations’. RFC Editor (Request for Comments). doi: 10.17487/RFC2663.

Internet Assigned Numbers Authority (2019) *Internet Protocol Version 6 Address Space*. Available at: https://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xhtml (Accessed: 20 March 2021).

Internet Engineering Task Force (2021). Available at: https://www.ietf.org/ (Accessed: 12 February 2021).

‘Internet Standard Subnetting Procedure’ (1985). RFC Editor (Request for Comments). doi: 10.17487/RFC0950.

Kawamura, S. and Kawashima, M. (2010) ‘A Recommendation for IPv6 Address Text Representation’. RFC Editor (Request for Comments). doi: 10.17487/RFC5952.

Kurose, J. F. *et al.* (2017) *Computer Networking A Top-Down Approach Seventh Edition*. Pearson Education, Inc.

Miniwatts Marketing Group (2021) *INTERNET USAGE STATISTICS The Internet Big Picture*. Available at: https://www.internetworldstats.com/stats.htm (Accessed: 12 February 2021).

Mobility support (2021). Available at: https://www.sciencedirect.com/topics/computer-science/mobility-support (Accessed: 15 February 2021).

Moskowitz, R. *et al.* (1996) ‘Address Allocation for Private Internets’. RFC Editor (Request for

Comments). doi: 10.17487/RFC1918.

Mrugalski, T. *et al.* (2018) ‘Dynamic Host Configuration Protocol for IPv6 (DHCPv6)’. RFC Editor (Request for Comments). doi: 10.17487/RFC8415.

Parra, O. J. S., Rios, A. P. and Lopez Rubio, G. (2011) ‘Quality of Service over IPV6 and IPV4’, in *2011 7th International Conference on Wireless Communications, Networking and Mobile Computing*, pp. 1–4. doi: 10.1109/wicom.2011.6040165.

Perkins, C. E. (2002) ‘IP Mobility Support for IPv4’. RFC Editor (Request for Comments). doi: 10.17487/RFC3344.

Perkins, C. E., Arkko, J. and Johnson, D. B. (2004) ‘Mobility Support in IPv6’. RFC Editor (Request for Comments). doi: 10.17487/RFC3775.

Postel, J. (ed.) (1981) ‘RFC 791 Internet Protocol - DARPA Inernet Programm, Protocol Specification’. Available at: http://tools.ietf.org/html/rfc791.

Reynolds, J. K. and Postel, D. J. (1994) ‘Assigned Numbers’. RFC Editor (Request for Comments). doi: 10.17487/RFC1700.

Simpson, W. A. *et al.* (2007) ‘Neighbor Discovery for IP version 6 (IPv6)’. RFC Editor (Request for Comments). doi: 10.17487/RFC4861.

Wikipedia the free encyclopedia (2021a) *Classless Inter-Domain Routing*. Available at: https://en.wikipedia.org/wiki/Classless_Inter-Domain_Routing (Accessed: 15 February 2021).

Wikipedia the free encyclopedia (2021b) *Internet Protocol Options*. Available at: https://en.wikipedia.org/wiki/Internet_Protocol_Options (Accessed: 1 March 2021).

Wikipedia the free encyclopedia (2021c) *IPv4*. Available at: https://en.wikipedia.org/wiki/IPv4 (Accessed: 12 February 2021).

Wikipedia the free encyclopedia (2021d) *IPv4 address exhaustion*. Available at: https://en.wikipedia.org/wiki/IPv4_address_exhaustion (Accessed: 12 February 2021).

Wikipedia the free encyclopedia (2021e) *IPv6*. Available at: https://en.wikipedia.org/wiki/IPv6 (Accessed: 12 February 2021).

Wikipedia the free encyclopedia (2021f) *Network address translation*. Available at: https://en.wikipedia.org/wiki/Network_address_translation (Accessed: 15 February 2021).

https://www.codebrakes.gr/tutorials/intro_packet_tracer.htm (Accessed:7 May 2021)

https://el.strephonsays.com/static-and-vs-dynamic-routing-13268 ((Accessed: 12 May 2021)

https://ipcisco.com/lesson/ipv6-configuration-on-cisco-packet-tracer/?fbclid=IwAR3NC8CvXbJQR1zg6nnaM3umCRLEAf2X68Vnfj8et-MFYAmyUBgjGyJ115k#Enable_IPv6_Globally ((Accessed: 18 jun 2021)