Εργαστηριακή Άσκηση 9
Το πρωτόκολλο IPv6

Εισαγωγή

Το βασικό πρωτόκολλο στρώματος δικτύου στο Διαδίκτυο (Internet) είναι το Internet Protocol (IP). Η έκδοση 4 του πρωτόκολλου IP που χρησιμοποιείται ευρέως σήμερα (IPv4) έχει ορισμένες ελλείψεις οι οποίες σε κάποιες περιπτώσεις δυσκολεύουν ή και αποτρέπουν την ανάπτυξη του διαδικτύου. Η έκδοση 6 (IPv6) αποτελεί τη νέα έκδοση του πρωτοκόλλου, η οποία έχει ως στόχο να επιτρέψει την απρόσκοπτη επικοινωνία και να αποτελέσει το περιβάλλον ανάπτυξης των νέων δικτυακών εφαρμογών.

Η ιστορία ανάπτυξης του IPv6 ξεκίνησε όταν, κατά την δεκαετία του 90, έγινε εμφανές ότι ο αριθμός των ελεύθερων διευθύνσεων του IPv4 μειωνόταν με γοργούς ρυθμούς. Σύμφωνα με τις τότε προβλέψεις, οι IP διευθύνσεις αναμενόταν να εξαντληθούν γύρω στο 2005. Για την αντιμετώπιση του προβλήματος ως προσωρινό μέτρο υιοθετήθηκε η μετάφραση διευθύνσεων δικτύου NAT (Network Address Translation) και ως μακροπρόθεσμη λύση η ανάπτυξη ενός νέου πρωτοκόλλου που θα επέτρεπε την εισαγωγή νέων χαρακτηριστικών και βελτιώσεων στο IP. Το πρώτο πρότυπο RFC (Request For Comments) για το IPv6, το RFC 1883, εκδόθηκε το 1995. Εντούτοις, η αναμενόμενη εξάντληση των διευθύνσεων IPv4 καθυστέρησε μέχρι το 2012 εξ αιτίας της ευρείας αποδοχής της NAT σε συνδυασμό με τη χρήση μη δρομολογήσιμων στο δημόσιο διαδίκτυο διευθύνσεων, ήτοι των 10.0.0.0/8, 172.16.0.0/12 ή 192.168.0.0/16, στο εσωτερικό των ιδιωτικών δικτύων.

Η IANA (Internet Assigned Numbers Authority) είναι ο αρμόδιος οργανισμός που διαχειρίζεται ομάδες διευθύνσεων σε παγκόσμια επίπεδο. Ανά γεωγραφική περιοχή οι διευθύνσεις διαχειρίζονται από πέντε περιοχικούς ληξίαρχους RIR (Regional Internet Registry). Οι RIR χωρίζουν τις διευθύνσεις που διαχειρίζονται σε μικρότερες ομάδες και τις εκχωρούν σε παρόχους ή άλλους οργανισμούς ή τοπικούς ληξίαρχους. Με την εισαγωγή του CIDR, η IANA τυπικά εκχωρεί χώρους διευθύνσεων με πρόθεμα /8. Η IANA εξάντλησε τις διευθύνσεις που διαθέτει σε RIR την 31/1/2011. Εκ των περιοχικών ληξίαρχων (AfriNIC για την Αφρική, APNIC για την Ασία και τον Ειρηνικό, ARIN για τη Β. Αμερική, LACNIC για τη Ν. Αμερική και RIPE NCC για την Ευρώπη), το APNIC άρχισε να εκχωρεί διευθύνσεις από το τελευταίο /8 την 15/4/2011 και το RIPE NCC άρχισε να εκχωρεί διευθύνσεις από το τελευταίο /8 την 14/9/2012, Για τους υπόλοιπους RIR αυτό θα συμβεί σε λίγα χρόνια και θα περάσει ακόμη αρκετός καιρός μέχρι να εκχωρηθεί και η τελευταία διεύθυνση σε χρήστη. Εν τω μεταξύ, οι ενδιαφερόμενοι φορείς πρέπει πλέον να αρχίσουν την εγκατάσταση IPv6 προκειμένου να εξασφαλίσουν τη συνέχιση και επέκταση της λειτουργίας τους.

Παρότι το IPv6 σχεδιάσθηκε για να αντικαταστήσει το IPv4, η πλειονότητα της διαδικτυακής κίνησης ακόμη είναι IPv4. Υπολογίζεται ότι στο τέλος του 2012 μόνο το 1% της κίνησης ήταν IPv6.

Πακέτο IPv6

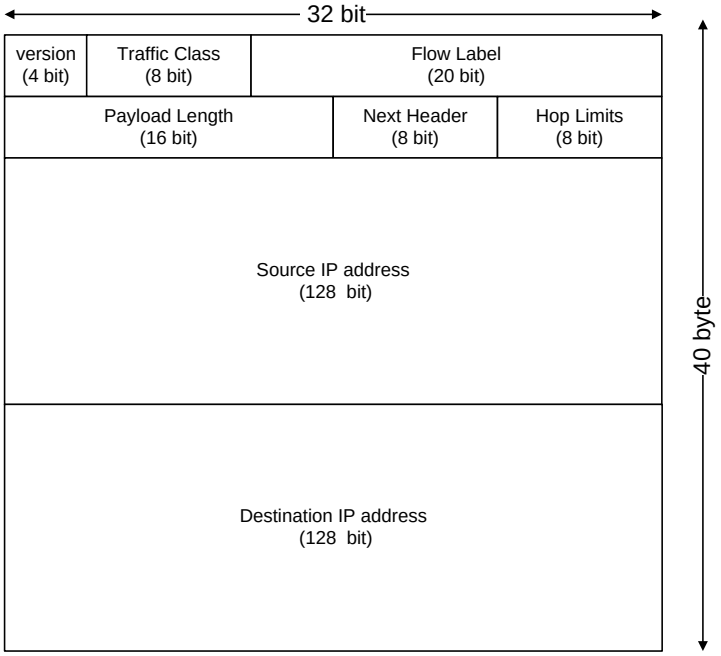
Το RFC2460 περιέχει την τρέχουσα προδιαγραφή του πρωτόκολλου IPv6.Σε συντομία, τα πακέτα IPv6 έχουν εκτεταμένες διευθύνσεις 128 bit, τετραπλάσιου μήκους σε σχέση με το IPv4, με δομή που επιτρέπει απλούς τρόπους απόδοσής των σε host (auto-configuration) και διευκολύνει την πολλαπλή διανομή. Εισάγεται ένας νέος τύπος διευθύνσεων "anycast" για αποστολή σε έναν (οποιονδήποτε) από μια ομάδα κόμβων, ενώ δεν υποστηρίζεται η εκπομπή (broadcast). Η επικεφαλίδα των πακέτων IPv6 έχει απλούστερη δομή έτσι ώστε να μειωθεί το υπολογιστικό κόστος επεξεργασίας της πλειονότητάς τους.

Οι προαιρετικές επιλογές κωδικοποιούνται πιο αποδοτικά σε αλληλουχία επικεφαλίδων επέκτασης και η προσθήκη νέας λειτουργικότητας, όπως υποστήριξη κινητικότητας, είναι πιο εύκολη. Προβλέπεται μια ελάχιστη MTU των 1280 byte για τα πακέτα IPv6, τα οποία σε τοπικά δίκτυα (LAN) μεταφέρονται ως πλαίσια Ethernet τύπου 86DD. Το μέγιστο μέγεθός τους είναι 64 KB, αλλά με τη βοήθεια των επικεφαλίδων επέκτασης Jumbogram επιτρέπονται πακέτα μήκους μέχρι 2^{32}-1 byte.

Επικεφαλίδα πακέτου IPv6

Η επικεφαλίδα του πακέτου IPv6 ορίζεται στο RFC 2460. Η σχεδίαση της επικεφαλίδας στοχεύει στην απλότητα και στο μικρό μέγεθος, ώστε να ελαχιστοποιηθεί η απαιτούμενη υπολογιστική ισχύς κατά την επεξεργασία των πεδίων της και κατά συνέπεια να είναι εφικτή η επεξεργασία σε μεγάλες ταχύτητες. Αντίθετα με το IPv4, το οποίο χρησιμοποιεί επικεφαλίδα μεταβλητού μήκους, στο IPv6 η βασική επικεφαλίδα είναι μικρού και σταθερού μεγέθους και περιέχει μόνο βασικές πληροφορίες όπως διευθύνσεις και μέγεθος πακέτου. Οι υπόλοιπες πληροφορίες έχουν μετακινηθεί σε αυτό που ονομάζεται επικεφαλίδες επέκτασης οι οποίες προστίθενται σύμφωνα με τις ανάγκες των εφαρμογών ή βάση άλλων απαιτήσεων. Για παράδειγμα, ένας κινούμενος κόμβος μπορεί να προσθέτει πληροφορίες δρομολόγησης με την μορφή επιπλέον επικεφαλίδων στα εξερχόμενα πακέτα του και να επηρεάζει με τον τρόπο αυτό το μονοπάτι από το οποίο θα δρομολογούνται τα πακέτα του.

Η μορφή της βασικής επικεφαλίδας φαίνεται στο επόμενο σχήμα. Τα πεδία της επικεφαλίδας είναι:



Επικεφαλίδα πακέτου IPv6

Version

Ενδεικτικό της έκδοσης του πρωτοκόλλου, αντίστοιχη με το Version του IPv4. Περιέχει την τιμή 6 για να προσδιορίσει το IPv6.

Traffic Class

Προορίζεται για την ένδειξη της ποιότητας υπηρεσίας (Quality of Service - QoS). Μπορεί να διαφοροποιήσει μεταξύ διαφορετικών κλάσεων κίνησης (σε συνδυασμό με πληροφορίες από άλλα

πεδία της επικεφαλίδας π.χ. διεύθυνση αφετηρίας /προορισμού). Έχει χρήση ανάλογη με το πεδίο DiffServ του πακέτου IPv4.

Flow Label

Ταυτοποιεί μια ομάδα πακέτων τα οποία ανήκουν στην ίδια ροή (flow). Δεν υπάρχει παρόμοιο πεδίο στα πακέτα IPv4. Αρχικά δημιουργήθηκε ώστε υπηρεσίες πραγματικού χρόνου να απολαμβάνουν ξεχωριστή εξυπηρέτηση (π.χ. τα πακέτα τους να ακολουθούν την ίδια διαδρομή στο δίκτυο). Το πεδίο αυτό χαρακτηρίζεται πλέον πειραματικό.

Payload Length

Το μέγεθος του πακέτου πλην της βασικής επικεφαλίδας σε byte συμπεριλαμβανομένων των πρόσθετων επικεφαλίδων (extension headers), με άνω όριο την τιμή των 64 KB. Αντίστοιχο του TotalLengh στα πακέτα IPv4.

Next Header

Καθορίζει τον τύπο της επόμενης επικεφαλίδας. Συνήθως υποδεικνύει το πρωτόκολλο ανωτέρου στρώματος π.χ. TCP, UDP, ICMP που ακολουθεί. Χρησιμοποιούνται οι ίδιες τιμές με αυτές του πεδίου Protocol στα πακέτα IPv4. Όταν ακολουθεί επικεφαλίδα επέκτασης προσδιορίζει το είδος της.

Hop Limit

Αντικαθιστά το πεδίο TTL των πακέτων IPv4. Ο κόμβος αποστολής ορίζει τη μέγιστη τιμή. Κάθε κόμβος που προωθεί ένα πακέτο μειώνει αυτή την τιμή κατά 1. Όταν φτάσει την τιμή 0, το πακέτο απορρίπτεται και αποστέλλεται ένα μήνυμα τύπου ICMP στον αποστολέα. Με αυτό τον τρόπο αποφεύγεται αέναη κίνηση λόγω βρόχων στο δίκτυο.

Source Address

Η διεύθυνση πηγής μήκους 128 bit. Λεπτομέρειες για την δομή της σε επόμενη παράγραφο.

Destination Address

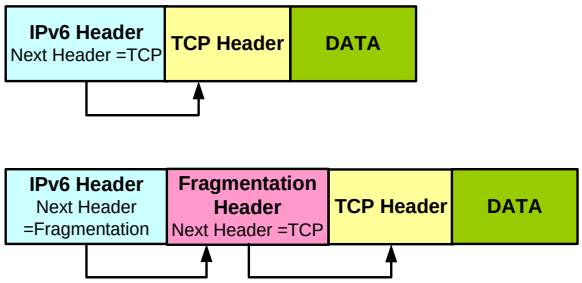
Η διεύθυνση του παραλήπτη.

Συγκρίνοντας με το IPv4 βλέπουμε ότι παρόλο που το μήκος της διεύθυνσης τετραπλασιάστηκε το συνολικό μήκος της βασικής επικεφαλίδας είναι το διπλάσιο. Αυτό έγινε επειδή στην βασική επικεφαλίδα συμπεριλήφθηκαν ορισμένες μόνο πληροφορίες που περιλάμβανε η επικεφαλίδα IPv4. Οι υπόλοιπες μετακινήθηκαν σε νέες, άλλου τύπου επικεφαλίδες επέκτασης. Για παράδειγμα, έχουν απαλειφτεί τα πεδία που σχετίζονται με τον θρυμματισμό. Εάν απαιτείται θρυμματισμός, αυτός γίνεται από τον αποστολέα, ενώ οι δρομολογητές IPv6 δεν θρυμματίζουν πακέτα. Επίσης δεν υπάρχει άθροισμα ελέγχου CRC (Cyclic Redundancy Check) για δύο λόγους: (α) η εγκυρότητα των πεδίων ελέγχεται ούτως ή άλλως σε χαμηλότερο επίπεδο και (β) ο υπολογισμός του είναι η κύρια πηγή καθυστέρησης κατά την επεξεργασία του πακέτου.

Αλληλουχία Επικεφαλίδων

Σε αντίθεση με το IPv4 όπου ορίζονται προαιρετικές επιλογές (options) στο τέλος της επικεφαλίδας του πακέτου, οι σχεδιαστές του IPv6 επέλεξαν μια διαφορετική προσέγγιση. Στο IPv6 επιτρέπεται η αλληλουχία (concatenation) επικεφαλίδων. Τα πρόσθετα πεδία περιλαμβάνονται σε ξεχωριστές

επικεφαλίδες που ακολουθεί η μία την άλλη. Για παράδειγμα, εάν ένα πακέτο έχει θρυμματισθεί στην πηγή λόγω μεγέθους, θα προστεθεί η επικεφαλίδα θρυμματισμού όπως φαίνεται στο ακόλουθο σχήμα. Το πλήθος των πρόσθετων επικεφαλίδων είναι μεταβλητό.



Παράδειγμα ακολουθίας επικεφαλίδων

Στον επόμενο πίνακα αναφέρονται οι τιμές του πεδίου Next Header που χρησιμοποιούνται για να δηλώσουν επικεφαλίδα επέκτασης. Οι τιμές για πρωτόκολλα είναι αυτές που χρησιμοποιούνται από το IPv4.

Πεδίο (δεκαδική τιμή)	Επικεφαλίδα επέκτασης	Χρήση
0	Hop by Hop	Επιλογές που πρέπει να εξετασθούν από όλους τους κόμβους της διαδρομής
43	Routing	Μέθοδοι για τον ορισμό της διαδρομής με Mobile IPv6
44	Fragment	Τιμές παραμέτρων θρυμματισμού
50	Encapsulating Security Payload	Κρυπτογραφημένα δεδομένα για ασφαλή επικοινωνία
51	Authentication Header	Πληροφορία για την πιστοποίηση αυθεντικότητας του πακέτου
59	No next header	Το πακέτο IPv6 τελειώνει με αυτή την επικεφαλίδα
60	Destination Option	Επιλογές που πρέπει να εξετασθούν μόνο από τον προορισμό
62	Mobility	Παράμετροι για το Mobile IPv6

Αυτός ο μηχανισμός της αλληλουχίας επικεφαλίδων ενέχει κάποια πολυπλοκότητα η οποία έγκειται στο ότι απαιτείται συνολική ανάγνωση όλων των επικεφαλίδων για να καταστεί εφικτή η προώθηση του πακέτου. Ευτυχώς υπάρχουν κανόνες οι οποίοι κάνουν την επεξεργασία πιο εύκολη. Οι επικεφαλίδες που είναι απαραίτητες για την προώθηση-δρομολόγηση τοποθετούνται στην αρχή, ενώ πληροφορίες που έχουν νόημα μόνο για τον τελικό παραλήπτη τοποθετούνται τελευταίες. Με αυτό τον τρόπο οι ενδιάμεσοι κόμβοι χρειάζεται απλά να επεξεργάζονται επικεφαλίδες μέχρι κάποιο σταθερό μήκος και να αφήνουν τις άλλες επικεφαλίδες ανεπεξέργαστες. Στη συνέχεια θα αναφερθούμε στις πιο σημαντικές επικεφαλίδες.

Επικεφαλίδα δρομολόγησης

Η επικεφαλίδα δρομολόγησης επηρεάζει τη διαδρομή που ακολουθεί ένα πακέτο. Η επικεφαλίδα επιτρέπει τον ορισμό ενδιάμεσων σημείων («Σταθμών Ελέγχου») μέσω των οποίων υποχρεούται να περάσει το πακέτο. Έχουν οριστεί δύο τύποι επικεφαλίδων δρομολόγησης (που ταυτοποιούνται από πεδίο εντός της επικεφαλίδας). Ο τύπος 0 χρησιμοποιείται προκειμένου να οριστεί μια αυθαίρετη

διαδρομή από διευθύνσεις IPv6 τις οποίες πρέπει να διασχίσει το πακέτο. Ο τύπος 2 χρησιμοποιείται για υποστήριξη κινητικότητας. Ο ορισμός είναι επεκτάσιμος και μπορεί να προστεθούν περισσότεροι τύποι επικεφαλίδων αργότερα εάν χρειαστεί. Η γενική μορφή της επικεφαλίδας δρομολόγησης αποτελείται από δύο μέρη: την ακολουθία των ενδιάμεσων διευθύνσεων και τον μετρητή (με όνομα Segments Left) ο οποίος δείχνει πόσοι ενδιάμεσοι σταθμοί απομένουν.

Ο κόμβος που επιθυμεί να χρησιμοποιήσει το παραπάνω χαρακτηριστικό προσθέτει την επικεφαλίδα δρομολόγησης και τοποθετεί τη διεύθυνση του πρώτου «σταθμού ελέγχου» στο πεδίο της διεύθυνσης προορισμού στη βασική επικεφαλίδα. Προσθέτει επίσης την ακολουθία από τους ενδιάμεσους σταθμούς στην επικεφαλίδα δρομολόγησης. Ο τελικός προορισμός του πακέτου φαίνεται από τον τελευταίο σταθμό στην ακολουθία που περιγράφεται στην επικεφαλίδα δρομολόγησης. Το πεδίο Segments Left δείχνει πόσοι ενδιάμεσοι σταθμοί πρέπει να περάσουν για τη τελική παράδοση του πακέτου. Στην συνέχεια το πακέτο ακολουθεί την τυπική διαδικασία δρομολόγησης. Με την παραλαβή του πακέτου από το σταθμό που περιγράφεται στο πεδίο Destination Address (που είναι ο πρώτος ενδιάμεσος σταθμός), ο δρομολογητής εντοπίζει την επικεφαλίδα δρομολόγησης και αντιλαμβάνεται ότι αποτελεί ενδιάμεσο σταθμό. Ανταλλάσσει τη διεύθυνση προορισμού με το N-ιοστό (μετρώντας από το τέλος) κομμάτι των διευθύνσεων στην ακολουθία των σταθμών ελέγχου όπου N είναι η τρέχουσα τιμή του πεδίου Segments Left. Στην συνέχεια μειώνει κατά ένα την τιμή του πεδίου Segments Left και το πακέτο στέλνεται στο νέο του προορισμό που είναι ο επόμενος σταθμός ελέγχου. Αυτή η διαδικασία εκτελείται σε κάθε σταθμό ελέγχου. Όταν η τιμή γίνει μηδέν ο δρομολογητής γνωρίζει ότι αυτός είναι ο τελικός προορισμός.

Ο τύπος 2 της επικεφαλίδας δρομολόγησης είναι μια απλούστευση της γενικής μορφής που περιγράφτηκε παραπάνω. Περιέχει μόνο ένα ενδιάμεσο σταθμό ελέγχου. Η ιδέα είναι η ακόλουθη: Ένας κινητός σταθμός IPv6, ο οποίος έχει μια σταθερή διεύθυνση (Home address), επισκέπτεται ένα νέο υποδίκτυο από το οποίο αποκτά μια νέα διεύθυνση (care of address). Ο στόχος είναι τα πακέτα που προορίζονται για τον κινητό κόμβο να προωθηθούν στη διεύθυνση care of address χωρίς να ενημερωθούν τα υψηλότερα στρώματα. Έτσι όταν αποστέλλεται ένα πακέτο στον κινητό κόμβο, η διεύθυνση προορισμού είναι η care of address αλλά προστίθεται και μια επικεφαλίδα δρομολόγησης (τύπου 2) η οποία περιέχει τη διεύθυνση Home Address. Όταν το πακέτο παραδίδεται οι διευθύνσεις (care of address και Home address) ανταλλάσσονται και τα παραπάνω στρώματα λογισμικού νομίζουν ότι απευθύνονται στη διεύθυνση Home Address.

Θρυμματισμός (Fragmentation)

Κάθε τεχνολογία επιπέδου 2 έχει εγγενείς περιορισμούς στο μέγεθος του πλαισίου που μπορεί να προωθήσει. Το μέγιστο μέγεθος πλαισίου που μπορεί να περάσει ονομάζεται MTU (Maximum Transmission Unit). Εάν το πακέτο IPv6 είναι μεγαλύτερο, τα δεδομένα πρέπει να θρυμματισθούν σε μικρότερα κομμάτια, τα οποία θα αποστέλλονται αυτόνομα. Ο παραλήπτης θα ανακατασκευάσει το αρχικό πακέτο από τα θραύσματα. Αυτή η διαδικασία ονομάζεται θρυμματισμός (fragmentation). Κάθε θρυμματισμένο πακέτο περιέχει ένα τμήμα των αρχικών δεδομένων και μια επικεφαλίδα που δείχνει ότι αποτελεί τμήμα ενός μεγαλύτερου πακέτου. Η επικεφαλίδα θρυμματισμού περιέχει τα αντίστοιχα πεδία της επικεφαλίδας IPv4, δηλαδή, ταυτοποίηση (identification), η οποία είναι μοναδική για το αρχικό υπερμέγεθες πακέτο, απόσταση (offset), που είναι η θέση στο αρχικό υπερμέγεθες πακέτο των δεδομένων που μεταφέρονται από το παρόν πακέτο και σήμανση (More Fragments) που δείχνει ότι ακολουθούν και άλλα κομμάτια

Ο παραλήπτης μαζεύει τα κομμάτια και χρησιμοποιεί την τιμή Ταυτοποίησης για να ομαδοποιήσει τα πακέτα της ίδιας ομάδας. Όταν έχουν ληφθεί όλα τα κομμάτια του αρχικού πακέτου, το οποίο σηματοδοτείται από την παραλαβή πακέτου χωρίς την ένδειξη More Fragments, τα θραύσματα τοποθετούνται στη σωστή σειρά με βάση την τιμή που έχει το πεδίο offset της επικεφαλίδας.

Στο IPv6 οι δρομολογητές δεν θρυμματίζουν πακέτα. Μόνο ο αρχικός αποστολέας επιτρέπεται να κάνει θρυμματισμό. Οι host πρέπει να μάθουν την ελάχιστη MTU της διαδρομής (Path MTU Discovery) και να κάνουν τα πακέτα τους αρκετά μικρά ώστε να φτάνουν στον προορισμό χωρίς θρυμματισμό. Για να μειωθεί η ανάγκη θρυμματισμού, το IPv6 ορίζει ως ελάχιστη MTU στους συνδέσμους που υποστηρίζουν IPv6 τα 1280 byte (με συνιστώμενη τιμή τα 1500 byte). Εάν κάποιος ενδιάμεσος κόμβος δεν μπορεί να προωθήσει το πακέτο εξαιτίας μικρής τιμής της MTU απορρίπτει το πακέτο και στέλνει μήνυμα ICMP στον αποστολέα που περιγράφει το μέγεθος που προκάλεσε το πρόβλημα.

Επιλογές (Options)

Οι επικεφαλίδες μπορεί να περιέχουν επιλογές που προσφέρουν επιπλέον πληροφορίες για την επεξεργασία του πακέτου. Υπάρχουν δύο επικεφαλίδες για επιλογές: επιλογές που επεξεργάζονται από κάθε κόμβο (Hop-By-Hop options) και επιλογές που σχετίζονται με τον τελικό κόμβο προορισμού (destination options). Οι επιλογές Hop-By-Hop, όταν υπάρχουν, μπαίνουν στην αρχή της αλληλουχίας επικεφαλίδων επειδή είναι σημαντικές για κάθε ενδιάμεσο κόμβο. Η θέση των επιλογών Destination Options δεν είναι συγκεκριμένη. Οι σημαντικότερες επιλογές είναι:

Router alert

Τα μηνύματα που έχουν ορίσει την τιμή router alert μπορούν να ενεργοποιήσουν το ενδιαφέρον όλων των δρομολογητών π.χ. για τη δέσμευση πόρων κατά μήκος της διαδρομής.

Jumbo payload

Επιτρέπει την μεταφορά πακέτων που είναι μεγαλύτερα από το μέγιστο των 64 KB. Η εν λόγω επιλογή ζητά την ειδική χρήση πακέτου για jumbograms με μέγιστο μέγεθος τα 4 GB.

Home Address

Για υποστήριξη κινητικότητας. Περιέχει την (σταθερή) διεύθυνση (home address) του κινητού κόμβου.

Αριθμοδότηση IPv6

Η ραγδαία μείωση των διαθέσιμων IPv4 διευθύνσεων ήταν ο λόγος για την κινητοποίηση γύρω από το IPv6. Ο σχεδιαστικός στόχος ήταν να μην χρειαστεί ποτέ να αντιμετωπιστεί το ίδιο πρόβλημα. Το διαθέσιμο μήκος των διευθύνσεων έχει αυξηθεί σημαντικά για να ικανοποιήσει οποιαδήποτε μελλοντική ανάγκη. Μια διεύθυνση IPv6 έχει μήκος 128 bit (16 byte), το οποίο είναι τέσσερις φορές περισσότερο από αυτό του IPv4. Επειδή κάθε bit που προστίθεται στο πεδίο της επικεφαλίδας διπλασιάζει το διαθέσιμο εύρος είναι αντιληπτό ότι το διαθέσιμο πλήθος των διευθύνσεων είναι ασύγκριτα μεγαλύτερο από το πλήθος των IPv4 διευθύνσεων. Περιλαμβάνει γύρω στις $3{,}4\times10^{38}$ διαφορετικές διευθύνσεις. Ο αριθμός αυτός είναι τεράστιος και επαρκεί για το απώτερο μέλλον, ακόμα και εάν όλα τα κινητά τηλέφωνα και όλες οι φορητές συσκευές απαιτούσαν πρόσβαση στο Internet. Ενδεικτικά, υπάρχουν περίπου $6{,}5\times10^{23}$ διευθύνσεις για κάθε τετραγωνικό μέτρο της επιφάνειας της Γης.

Οι βασικοί κανόνες της αριθμοδότησης του IPv6 τέθηκαν στο RFC 3513. Μερικά συνοδευτικά RFC ορίζουν περιπτώσεις και χρήσεις ειδικού τύπου διευθύνσεων. Δεδομένου του μεγάλου μήκος των διευθύνσεων, η αναπαράστασή τους γίνεται με χρήση δεκαεξαδικών συμβόλων, τα οποία ομαδοποιούνται σε 8 ομάδες των 4 συμβόλων. Για να βελτιωθεί η αναγνωσιμότητα, οι ομάδες χωρίζονται με ":" και επιτρέπονται συντομεύσεις, όπως η παράλειψη των αρχικών μηδενικών: “0000”→“0”, “0db8”→“db8”. Επίσης, το “:0000:…:0000” γράφεται σαν “::” Συνεπώς οι ακόλουθες αναπαριστούν όλες την ίδια διεύθυνση IPv6:

2001:0db8:0000:0000:0000:0000:1428:57ab

2001:db8:0:0:0:0:1428:57ab

2001:db8:0:0::1428:57ab

2001:db8::1428:57ab

Κατά την αναγραφή μιας διεύθυνσης IPv6 μπορούμε να υποδείξουμε το πρόθεμα δικτύου (routing prefix) χρησιμοποιώντας τον συμβολισμό CIDR. Για παράδειγμα, μια διεπαφή με διεύθυνση 2001:db8:a::123 που συνδέεται στο υποδίκτυο 2001:db8:a::/64 γράφεται ως 2001:db8:a::123/64.

Τα υποδίκτυα IPv6 χρησιμοποιούν μια ομάδα συνεχόμενων διευθύνσεων που είναι δύναμη του 2. Η διεύθυνση ενός δικτύου γράφεται με τον συμβολισμό CIDR, ως η πρώτη διαθέσιμη διεύθυνση του δικτύου, που τελειώνει με συνεχόμενα μηδενικά, ακολουθούμενη από το σύμβολο "/" και ένα ακέραιο αριθμό που δείχνει το μήκος του προθέματος. Για παράδειγμα, το δίκτυο 2001:db8:1234::/48 ξεκινά από τη διεύθυνση 2001:db8:1234:0000:0000:0000:0000:0000 και τελειώνει με τη διεύθυνση 2001:db8:1234:ffff:ffff:ffff:ffff:ffff.

Το IPv6, RFC 4291, υποστηρίζει τρεις τύπους διευθύνσεων:

Διευθύνσεις Unicast (μοναδιαίες) που προσδιορίζουν μοναδικά μια διεπαφή ενός host στο δίκτυο ώστε τα πακέτα να μπορούν να δρομολογηθούν προς αυτή.

Διευθύνσεις Anycast (επιλεκτικές) που προσδιορίζουν μια ομάδα διεπαφών συνήθως σε διαφορετικούς host. Ένα πακέτο που αποστέλλεται σε μια τέτοια διεύθυνση παραδίδεται σε μία μόνο διεπαφή, δρομολογούμενο συνήθως στην πλησιέστερη της ομάδας.

Διευθύνσεις Multicast (ομάδας) που προσδιορίζουν διεπαφές διαφορετικών host. Οι host αποκτούν μια τέτοια διεύθυνση λόγω συμμετοχής σε κάποια ομάδα. Ένα πακέτο που αποστέλλεται σε μια τέτοια διεύθυνση παραδίδεται σε όλες τις διεπαφές που έχουν εγγραφεί στην εν λόγω ομάδα.

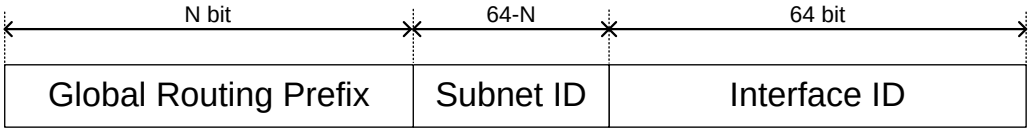
Συγκεκριμένα, στην αριθμοδότητηση IPv6 η διεύθυνση ::/128 θεωρείται ως μη ορισμένη (Unspecified) και έχει νόημα μόνο σε πακέτα που δημιουργούνται προτού ο host αποκτήσει μια διεύθυνση (π.χ. μέσω DHCP). Η διεύθυνση ::1/128 είναι για το βρόχο επιστροφής (loopback). Οι διευθύνσεις FF00::/8 είναι για ομάδες (multicast). Οι διευθύνσεις FE80::/8 είναι τοπικές στη ζεύξη (Link-local). Οι διευθύνσεις FEC0::/10 είναι τοπικές στο site[1] (site-local). Όλες οι υπόλοιπες είναι παγκόσμια μοναδικές (global unicast). Δεν υπάρχουν διευθύνσεις εκπομπής (Broadcast). Η εκπομπή προς όλες τις διεπαφές μπορεί να γίνει με ειδικού τύπου διευθύνσεις multicast.

Όλες οι διευθύνσεις IPv6 έχουν μια καθορισμένη εμβέλεια εφαρμογής (scope). Μερικές από τις διευθύνσεις έχουν αυστηρά τοπικό χαρακτήρα. Η διεύθυνση ::1/128 είναι ο βρόχος επιστροφής (loopback) και πακέτα που στέλνονται εκεί επιστρέφουν στην ίδια διεπαφή (αντίστοιχη με την 127.0.0.1/8 στο IPv4). Διευθύνσεις FE80::/10 (link-local) είναι τοπικές στη ζεύξη με την έννοια ότι ισχύουν μόνο στην τοπική ζεύξη και δεν δρομολογούνται εκτός αυτής. Εξ αυτών, μόνο το FE80::/64 έχει εκχωρηθεί, αντίστοιχο του 169.254.0.0/16 για το IPv4. Οι διευθύνσεις με το πρόθεμα FC00::/7 είναι μοναδικές τοπικές (unique local) διευθύνσεις και προορίζονται για δρομολόγηση στο εσωτερικό ιδιωτικών δικτύων, ανάλογες των 10.0.0.0/8, 172.16.0.0/12 και 192.168.0.0/16 στο IPv4.

[1] Οι διευθύνσεις site-local έχουν καταργηθεί λόγω της δυσκολίας του ορισμού τι είναι site και έχουν αντικατασταθεί από τις unique local.

Διευθύνσεις τύπου Unicast

Ο σημαντικότερος τύπος διεύθυνσης είναι οι παγκόσμια μοναδικές (global unicast) και ορίζονται στο RFC 3587. Η δομή των διευθύνσεων ακολουθεί μια ιεραρχία δύο επιπέδων με ένα πρόθεμα δικτύου μήκους 64 bit που χρησιμοποιείται για δρομολόγηση και μια ταυτότητα 64 bit που προσδιορίζει τη διεπαφή. Το πρόθεμα δικτύου αποτελείται από δύο μέρη: το πρόθεμα δρομολόγησης συνήθως μήκους μεγαλύτερου των 48 bit που ταυτοποιεί μοναδικά το δίκτυο και τον αριθμό του υποδικτύου, τα υπολειπόμενα bit, που προσδιορίζουν μοναδικά το τελικό δίκτυο (δίκτυο πελάτη) που και αυτό μπορεί να χωρισθεί σε υποδίκτυα όπως γίνεται στο CIDR.



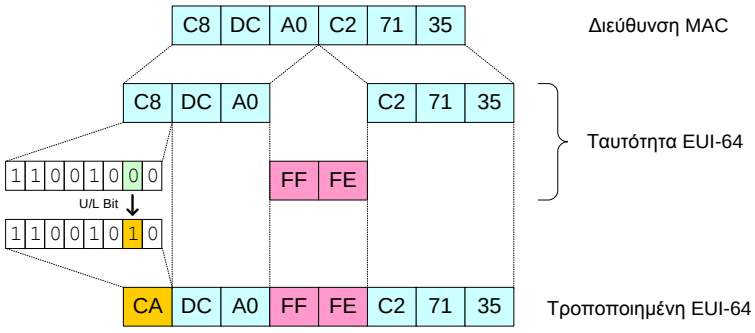
Δομή μιας παγκόσμιας διεύθυνσης τύπου Unicast

Η ταυτότητα διεπαφής μπορεί να παράγεται από τη διεύθυνση MAC της διεπαφής ακολουθώντας τη μορφή του τροποποιημένου EUI-64 ή να δίδεται από τον εξυπηρετητή DHCPv6 είτε να παράγεται με τυχαίο τρόπο ή να τίθεται χειροκίνητα.

Τροποποιημένο EUI-64

Η χρήση 64 bit για τον καθορισμό της φυσικής διεύθυνσης μιας διεπαφής φαίνεται εξαιρετικά σπάταλη, αφού θα μπορούσε να περιορίζεται στα παγκοσμίως μοναδικά 48 bit της διεύθυνσης MAC. Εξάλλου είναι πολύ δύσκολο να φανταστούμε υποδίκτυα τα οποία να χρειάζονται παραπάνω από 16 bit για την αριθμοδότηση όλων των κόμβων. Από την άλλη πλευρά, η διεύθυνση μήκους 64 bit απλοποιεί σημαντικά τις λειτουργίες του μηχανισμού αυτορρύθμισης. Η σύσταση RFC 4291 καθορίζει μια τροποποιημένη έκδοση των ταυτοτήτων EUI-64 ως μέρος της διεύθυνσης IPv6. Η ταυτότητα EUI-64 πρακτικά είναι μια διεύθυνση IEEE MAC μήκους 64 bit, ανάλογη προς τις συνήθεις διευθύνσεις MAC που είναι τύπου EUI-48. Στην τροποποιημένη EUI-64, το 7^{ο} bit της ταυτότητας αντιστρέφεται και έτσι η τιμή 0 σημαίνει τοπική διεύθυνση (έχει νόημα μόνο εντός της τοπικής διαχειριστικής επικράτειας) και η τιμή 1 σημαίνει παγκόσμια μοναδική (globally unique).

Στην περίπτωση διεπαφών Ethernet με διευθύνσεις MAC των 48 bit, η αντίστοιχη ταυτότητα EUI-64 προκύπτει παρεμβάλλοντας το FF:FE στο μέσο της. Έτσι για παράδειγμα η διεύθυνση MAC C8:DC:A0:C2:71:35 μετατρέπεται σε interface ID CADC:A0FF:FEC2:7135 όπως φαίνεται στο σχήμα.



Μετατροπή της διεύθυνσης MAC σε τροποποιημένη EUI-64

Απαιτούμενες διευθύνσεις

Στον κόσμο του IPv4 κάθε δικτυακή διεπαφή έχει μια μόνο διεύθυνση. Εάν χρειάζεται να αποκτήσει η διεπαφή και άλλες διευθύνσεις αυτό γίνεται συνήθως με τρόπους και μεθόδους που εξαρτώνται εν πολλοίς από τα λειτουργικά συστήματα και δεν υπακούουν σε πρότυπα. Στο περιβάλλον IPv6, η κατάσταση είναι διαφορετική: η χρήση πολλαπλών διευθύνσεων επιβάλλεται

για λόγους λειτουργικότητας. Οι απαιτούμενες διευθύνσεις για κάθε τερματικό σταθμό (που δεν προωθεί πακέτα σε άλλο σταθμό) είναι:

- η διεύθυνση loopback ::1
- μία διεύθυνση link-local για κάθε διεπαφή
- unicast και multicast διευθύνσεις για κάθε διεπαφή κατόπιν ανάθεσης
- η multicast διεύθυνση all-nodes ff01::1 (στη τοπική διεπαφή) και ff02::1 (στη τοπική ζεύξη)
- η ομαδική διεύθυνση Solicited Node, η οποία χρησιμοποιείται όταν δεν είναι γνωστή εκ των προτέρων η διεύθυνση αποστολής στη φάση της αναζήτησης γείτονα (Neighbor Discovery). Ένας host απαιτείται να συμμετέχει στην ομάδα Solicited-Node για κάθε unicast ή anycast διεύθυνση που του έχει αποδοθεί και προκύπτει από τα τελευταία 24 bit της διεύθυνσης unicast ή anycast προσθέτοντας σε αυτά το πρόθεμα ff02:0:0:0:0:1:ff00:0/104. Π.χ., η fc00::1/64 θα γίνει ff02::1:ff00:1 και η fe80::2aa:ff:fe28:9c5a θα γίνει ff02::1:ff28:9c5a.

Για παράδειγμα ένας host που έχει μία κάρτα δικτύου Ethernet με διεύθυνση MAC 02:2a:0f:32:5e:d1, συμμετέχει στα υποδίκτυα 2001:a:b:c::/64 και 2001:a:b:1::/64 και είναι μέλος της ομάδας ff15::1:2:3 πρέπει να λαμβάνει δεδομένα στις ακόλουθες διευθύνσεις:

- ::1 (loopback)
- fe80::2a:fff:fe32:5ed1 (link-local)
- ff01::1 (όλοι οι κόμβοι στη διεπαφή)
- ff02::1 (όλοι οι κόμβοι στη ζεύξη)
- ff02::1:ff32:5ed1 (solicited node multicast)
- 2001:a:b:c:2a:fff:fe32:5ed1 (unicast κατόπιν ανάθεσης)
- 2001:a:b:1:2a:fff:fe32:5ed1 (επιπλέον unicast κατόπιν ανάθεσης)
- ff15::1:2:3 (multicast κατόπιν ανάθεσης)

Ένας δρομολογητής χρειάζεται ακόμη περισσότερες διευθύνσεις. Πρέπει να υποστηρίζει όλες τις προηγούμενες ανά διεπαφή καθώς και τις ακόλουθες:

- την anycast διεύθυνση subnet-router που προσδιορίζει όλους τους δρομολογητές σε κάθε υποδίκτυο όπου είναι ρυθμισμένος να δρα ως δρομολογητής και είναι απλά το πρόθεμα δικτύου της τοπικής ζεύξης ακολουθούμενο από μηδενικά
- όλες τις anycast διευθύνσεις κατόπιν ανάθεσης
- τη multicast διεύθυνση all-routers ff01::2 (στη τοπική διεπαφή), ff02::2 (στη τοπική ζεύξη) και ff05::2 (στο τοπικό site)

Εάν ο δρομολογητής διασυνδέει τα παραπάνω υποδίκτυα θα έχει επιπλέον τις διευθύνσεις:

- 2001:a:b:c:: (δρομολογητής υποδικτύου για το πρώτο υποδίκτυο)
- 2001:a:b:1:: (δρομολογητής υποδικτύου για το δεύτερο υποδίκτυο)
- ff01::2 (όλοι οι δρομολογητές σε αυτή τη διεπαφή)
- ff02::2 (όλοι οι δρομολογητές σε αυτή τη ζεύξη)
- ff05::2 (όλοι οι δρομολογητές σε αυτό το site)

Ας υποθέσουμε ότι ο παραπάνω δρομολογητής ενεργεί και ως home agent στα παραπάνω δύο υποδίκτυα και κατά συνέπεια πρέπει να ακούει στην anycast διεύθυνση all-homeagents. Σε αυτή την περίπτωση πρέπει επιπλέον να αποδοθούν και οι διευθύνσεις:

- 2001:a:b:c::fdff:ffff:ffff:fffe (home agents στο πρώτο υποδίκτυο)
- 2001:a:b:1::fdff:ffff:ffff:fffe (home agents στο δεύτερο υποδίκτυο)

Επιλογή διευθύνσεων

Η επιλογή μίας εκ των διαθέσιμων διευθύνσεων (είτε πρόκειται για διεύθυνση πηγής είτε προορισμού) έναντι των υπολοίπων επηρεάζει την συμπεριφορά και ως εκ τούτου ο τρόπος επιλογής της είναι σημαντικός. Η σύσταση RFC 3484 ορίζει τους κανόνες. Για διευθύνσεις πηγής ορίζονται κανόνες ταξινόμησης ώστε να προκύψει η "καλύτερη" διεύθυνση πηγής για μια δεδομένη διεύθυνση προορισμού. Οι κανόνες εφαρμόζονται μόνο στις διευθύνσεις IPv6, όχι στις IPv4. Ο αλγόριθμος ταξινόμησης σχηματίζει ένα σύνολο υποψηφίων CandidateSource(D) για τον προορισμό D και επιλέγεται η πρώτη διεύθυνση.

Ο αλγόριθμος επιλογής διεύθυνσης προορισμού ξεκινά με μια λίστα διευθύνσεων, που τυπικά λαμβάνεται από το DNS, και διατάσει τις διευθύνσεις σε μια νέα λίστα. Εδώ ο αλγόριθμος διατάσει τόσο διευθύνεις IPv6 όσο και IPv4. Η ταξινόμηση στη νέα λίστα γίνεται συγκρίνοντας τις διευθύνσεις σε ζεύγη ανά σειρά εμφάνισης στην αρχική λίστα σύμφωνα με συγκεκριμένους κανόνες δοθείσης της διεύθυνσης πηγής.

Δείκτης ζώνης

Επειδή όλες οι τοπικής εμβέλειας (link-local) διευθύνσεις έχουν όλες το ίδιο πρόθεμα δικτύου, η διαδικασία δρομολόγησης δεν μπορεί επιλέξει την απερχόμενη διεπαφή όταν ο προορισμός είναι τέτοια διεύθυνση. Για το λόγο αυτό χρειάζεται επιπλέον πληροφορία δρομολόγησης. Στην αναγραφή των διευθύνσεων χρησιμοποιείται μια ειδική ταυτότητα που αποκαλείται δείκτης ζώνης (zone index). Ο δείκτης ζώνης αντιστοιχεί στις διεπαφές του κόμβου και επισυνάπτεται στο τέλος της διεύθυνσης μετά το σύμβολο “%”. Η σύνταξη του δείκτη εξαρτάται από το λειτουργικό σύστημα. Στα Windows χρησιμοποιούνται αριθμοί, π.χ. fe80::3%12. Σε συστήματα τύπου Unix (BSD, Linux, Mac OS X) χρησιμοποιείται το όνομα της διεπαφής, π.χ. fe80::3%eth0.

Διευθύνσεις στην πράξη

Συνοψίζοντας, ο χώρος των διευθύνσεων IPv6 έχει χωριστεί σε ορισμένες περιοχές όπως απεικονίζει ο πίνακας

::0/128	Ακαθόριστη διεύθυνση
::1/128	Διεύθυνση Loopback
ff00::/8	Διευθύνσεις Multicast
fe80::/10	Διευθύνσεις Link-local
fec0::/10	Καταργηθείσες (πρώην site-local διευθύνσεις)
fc00::/7	Μοναδικές τοπικές Unique local
άλλες	παγκόσμια μοναδικές διευθύνσεις unicast

Από τις παγκόσμια μοναδικές χρησιμοποιείται μόνο ένα μικρό μέρος όπως στον επόμενο πίνακα

2001::/16	Κανονικές διευθύνσεις IPv6
2002::/16	Διευθύνσεις 6to4
2003::/18	Κανονικές διευθύνσεις IPv6
2400::/12	Διευθύνσεις που έχουν εκχωρηθεί στον APNIC
2600::/12	Διευθύνσεις που έχουν εκχωρηθεί στον ARIN
2800::/12	Διευθύνσεις που έχουν εκχωρηθεί στον ARIN
2A00::/12	Διευθύνσεις που έχουν εκχωρηθεί στο RIPE
2C00::/12	Διευθύνσεις που έχουν εκχωρηθεί στον AfriNIC

Ανακάλυψη γείτονα (Neighbor Discovery)

Υπάρχουν μερικές υπηρεσίες που είναι απαραίτητες για την λειτουργία του πρωτοκόλλου IPv6. Με άλλα λόγια χωρίς αυτές δεν θα ήταν δυνατό να υπάρχει λειτουργία με την έννοια της συνδεσιμότητας στο IPv6. Πρώτα θα περιγράψουμε τη λειτουργία του Neighbor Discovery και στην συνέχεια τη λειτουργία του DNS στο IPv6.

Η ανακάλυψη γείτονα είναι το πρωτόκολλο που επιτρέπει σε διαφορετικούς κόμβους στο ίδιο καλώδιο (υποδίκτυο) να συνδεθούν και να διαφημίσουν την ύπαρξη τους στους γείτονες. Αυτή η λειτουργικότητα είναι βασική και πρέπει να υλοποιείται από όλους τους κόμβους. Η διαδικασία ανεύρεσης γείτονα αντικαθιστά τα πρωτόκολλα αναζήτησης δρομολογητή, ARP και ICMPv4 redirect του IPv4. Οι λειτουργίες ορίζονται στις ακόλουθες συστάσεις:

- RFC 4861, Neighbor Discovery for IP Version 6 (IPv6)
- RFC 4862, IPv6 Stateless Address Autoconfiguration
- RFC 4443, Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification

Ο συνδυασμός αυτών των λειτουργιών επιτρέπει την αυτόματη ανίχνευση των άλλων κόμβων και των δρομολογητών σε ένα τοπικό δίκτυο. Από τα μηνύματα που ανταλλάσσονται επιτρέπεται στους τερματικούς κόμβους να κατασκευάσουν την τερματική τους διεύθυνση και να αποκτήσουν πληροφορίες για τη λειτουργία τους. Η αναζήτηση γείτονα υλοποιεί την ανίχνευση ταυτόσημων διευθύνσεων ώστε ένας σταθμός να μην χρησιμοποιεί μια διεύθυνση η οποία είναι ήδη σε χρήση και να επιτρέπει την ανίχνευση απροσπέλαστων σταθμών. Η λειτουργία της ανακάλυψης γείτονα χρησιμοποιεί τα μηνύματα πρωτοκόλλου Internet Control Message έκδοση 6 (ICMPv6):

- router solicitation (RS)
- router advertisement (RA)
- neighbor solicitation (NS)
- neighbor advertisement (NA)
- redirect

Ανακάλυψη δρομολογητή (Router Discovery)

Η ανακάλυψη του πλησιέστερου δρομολογητή (Router Discovery) γίνεται με τη λήψη μηνυμάτων RA (router advertisement) από τον δρομολογητή που βρίσκεται εντός του ίδιου υποδικτύου. Αυτά είτε αποστέλλονται περιοδικά από τον δρομολογητή με διεύθυνση προορισμού την ομαδική διεύθυνση all-nodes είτε σε απάντηση σε μήνυμα RS (router solicitation) από ένα σταθμό IPv6. Τα μηνύματα RA μπορεί να περιέχουν ένα σύνολο από προθέματα (prefixes). Αυτά τα προθέματα χρησιμοποιούνται για τη λειτουργία stateless address autoconfiguration των σταθμών και για την διατήρηση μιας λίστας προθεμάτων για τη ζεύξη (on-link prefixes) καθώς επίσης και για την ανακάλυψη ταυτόσημων διευθύνσεων. Για τους δρομολογητές, η λίστα προθεμάτων χρησιμοποιείται για την προώθηση πακέτων. Εάν η διεύθυνση προορισμού ενός πακέτου βρίσκεται εντός των προθεμάτων της ζεύξης ο δρομολογητής το στέλνει στην εν λόγω ζεύξη, διαφορετικά το στέλνει σε κάποιο γειτονικό δρομολογητή.

Συνοπτικά, τα IPv6 μηνύματα RA περιέχουν την ακόλουθη πληροφορία:

- ένα ή περισσότερα προθέματα IPv6 τα οποία μπορούν να χρησιμοποιηθούν από τους τοπικούς κόμβους για την ρύθμιση των διευθύνσεων τους,
- το μήκος προθέματος (prefix length) και την έγκυρη διάρκεια χρήσης (valid lifetime) για κάθε πρόθεμα
- ένα σύνολο από σημάνσεις (flags) που εξειδικεύουν τον τύπο και τον τρόπο της αυτόματης ρύθμισης διεύθυνσεων (stateless ή stateful) που υποστηρίζεται

- τον προκαθορισμένο δρομολογητή (Default router)
- επιπλέον πληροφορίες για τους τερματικούς σταθμούς όπως hop limit και MTU

Αυτόματη ρύθμιση διευθύνσεων (Automatic Address Configuration)

Ένας σταθμός μπορεί να ρυθμίσει αυτόματα (χωρίς παρέμβαση του διαχειριστή του σταθμού) τη διεύθυνση που χρησιμοποιεί για επικοινωνία στο δίκτυο. Ο σταθμός μπορεί να χρησιμοποιεί ταυτόχρονα και τους δύο διαθέσιμους μηχανισμούς ρύθμισης διευθύνσεων stateless και stateful. Η συγκεκριμένη μέθοδος μπορεί να ρυθμιστεί με χρήση flags στα μηνύματα RA. Φυσικά είναι δυνατό ο σταθμός να ρυθμιστεί και χειροκίνητα.

Stateless Address Autoconfiguration (SLAAC)

Υπάρχου δύο τρόποι για την αυτόματη ρύθμιση διευθύνσεων με τον μηχανισμό αυτό:

- Αυτόματη ρύθμιση με ανακάλυψη προθέματος
- Χρήση Stateless DHCPv6

Η αυτόματη ρύθμιση με χρήση του προθέματος καθορίζεται στη σύσταση RFC 4862. Εάν υπάρχει η σήμανση ‘autonomous’ στην περιοχή Prefix Information Option στο μήνυμα RA, ο σταθμός μπορεί να ρυθμίσει την παγκόσμια διεύθυνση IPv6 επιθέτοντας την ταυτότητα διεπαφής 64 bit στο πρόθεμα που περιέχεται στο μήνυμα RA. Υπάρχουν διάφοροι τρόποι με τους οποίος ο σταθμός μπορεί να δημιουργήσει την ταυτότητα διεπαφής (π.χ. από τη διεύθυνση MAC, με τυχαίο τρόπο ή κρυπτογραφικά). Η χρήση Stateless DHCPv6 δεν αναφέρεται ως επιλογή στα RA, εν τούτοις πρόσφατες ανακοινώσεις σε ομάδες εργασίας IPv6 προτείνουν την χρήση stateless DHCPv6 μέσω της σήμανσης ‘O’ στα μηνύματα prefix announcements.

Stateful Address Configuration

Η χρήση stateful DHCPv6 δεν είναι πολύ διαφορετική από την stateless DHCPv6. Παρότι η αποθήκευση κατάστασης στην μνήμη του εξυπηρετητή DHCPv6 μπορεί να επιφέρει καθυστερήσεις, η χρήση του προτιμάται από τους διαχειριστές επειδή προσφέρει επιπλέον έλεγχο και τεκμηρίωση των υπό χρήση διευθύνσεων.

Duplicate Address Detection - DAD

Από την στιγμή που ένας τερματικός σταθμός έχει ρυθμίσει τη διεύθυνσή του πρέπει να προχωρήσει στην διαδικασία DAD για να αποτρέψει τη χρήση ταυτόσημων διευθύνσεων στο τοπικό υποδίκτυο. Αυτό θα γίνει ανεξάρτητα από τον τρόπο σχηματισμού της διεύθυνσης stateless, stateful ή χειροκίνητου. Ο σταθμός δεν επιτρέπεται να χρησιμοποιήσει μια διεύθυνση εάν δεν ολοκληρωθεί η διαδικασία DAD επιτυχώς. Μέχρι να ολοκληρωθεί επιτυχώς η διαδικασία DAD, η διεύθυνση φαίνεται να βρίσκεται σε δοκιμαστική (tentative) κατάσταση που σημαίνει ότι μπορεί να χρησιμοποιηθεί μόνο για λειτουργίες ανίχνευσης γείτονα. Για να επιτευχθεί ο σκοπός, ο τερματικός σταθμός στέλνει ένα μήνυμα NS (neighbor solicitation) με στην δικιά του διεύθυνση στο πεδίο target address και διεύθυνση προορισμού την ομαδική διεύθυνση solicited node που προκύπτει από την target address). Η διεύθυνση αποστολέα είναι η ακαθόριστη διεύθυνση (::). Εάν υπάρχει και άλλος κόμβος που χρησιμοποιεί την ίδια διεύθυνση δύο ενδεχόμενα μπορεί να συμβούν:

1. Ο σταθμός που θα λάβει το μήνυμα NS του αιτούντος σταθμού να απαντήσει με μήνυμα NA (neighbor advertisement) που θα αποσταλεί στην ομαδική διεύθυνση all-nodes εκθέτοντας με αυτό τον τρόπο την ταυτόσημη διεύθυνση στον αιτούντα.
2. Ο σταθμός να πάρει ένα μήνυμα NS με τη δικιά του διεύθυνση στο πεδίο target address από ένα άλλο κόμβο ο οποίος προσπαθεί να ολοκληρώσει την διαδικασία DAD.

Η διαδικασία DAD παρέχει μια έμμεση αλλά όχι οριστική ένδειξη για το εάν υπάρχει άλλος κόμβος που χρησιμοποιεί τη διεύθυνση. Ένας κόμβος που πραγματοποιεί DAD μπορεί να θεωρήσει τη

δοκιμαστική διεύθυνσή του μοναδική εάν δεν ληφθούν ενδείξεις ταυτόσημης διεύθυνσης μετά από έλευση χρόνου ίσου με RETRANS_TIMER msec αφότου έστειλε αριθμό DUP_ADDR_DETECT_TRANSMITS πακέτων NS. Οι τυπικές τιμές των παραπάνω μεταβλητών είναι 1.000 και 1, αντίστοιχα. Κατά συνέπεια σε τυπικές συνθήκες χρειάζεται περίπου 1 sec συν την επιπλέον καθυστέρηση για την μετάδοση πακέτων και τους υπολογισμούς.

Επιπλέον, ένας σταθμός πρέπει να καθυστερήσει την αποστολή NS για ένα τυχαίο χρονικό διάστημα μεταξύ 0 και MAX_RTR_SOLICITATION_DELAY sec εάν τα πακέτα αυτά πρόκειται να είναι τα πρώτα που θα σταλούν μετά την αρχικοποίηση μιας δικτυακής διεπαφής. Η τιμή αυτής της παραμέτρου ορίζεται να είναι 1 sec. Ως εκ τούτου ένας σταθμός που δεν έχει στείλει προηγουμένως πακέτα RS θα καθυστερήσει κατά μέσο όρο επιπλέον 0,5 sec (1 sec στην χειρότερη περίπτωση).

Ένας κόμβος που επιθυμεί την επιτάχυνση της διαδικασίας αυτόματης ρύθμισης διευθύνσεων μπορεί να εκτελέσει παράλληλα τις διαδικασίες DAD και ανεύρεσης δρομολογητή. Αυτό είναι εφικτό επειδή ο σταθμός με την γνώση της link local διεύθυνσης μπορεί να προχωρήσει στην διαδικασία DAD χωρίς να περιμένει τον επιπλέον χρόνο της ανακοίνωσης του δρομολογητή υποδικτύου. Εάν ο δρομολογητής κατευθύνει τον σταθμό να ορίσει τη διεύθυνσή του χρησιμοποιώντας την μέθοδο της αυτόματης απονομής δεν απαιτείται να πραγματοποιηθεί η διαδικασία DAD με την προκύπτουσα παγκόσμια διεύθυνση unicast εάν έχει επιβεβαιωθεί η μοναδικότητα της διεύθυνσης link-local. Έτσι ο σταθμός μπορεί να μειώσει τον χρόνο αφού δεν χρειάζεται να περιμένει για την απάντηση στο αίτημα τύπου RS.

Ανίχνευση Έλλειψης Επικοινωνίας (Neighbor Unreachability Detection)

Όταν ένας σταθμός θέλει να στείλει ένα πακέτο ελέγχει τον πίνακα Neighbor Cache για να καθορίσει τη φυσική διεύθυνση του κόμβου στον οποίο θα αποσταλεί. Στον πίνακα Neighbor Cache δίπλα από κάθε εγγραφή υπάρχει και η κατάσταση λειτουργίας. Μια εγγραφή με το χαρακτηριστικό REACHABLE σημαίνει ότι ο σταθμός είναι προσβάσιμος. Στο IPv6 ένας σταθμός θεωρεί ένα γείτονα προσβάσιμο εάν του έχει αποστείλει πακέτα και έχει λάβει θετική επιβεβαίωση λήψης. Αυτό επιτυγχάνεται με δύο τρόπους: με τη λήψη πακέτων τύπου NA από τους γείτονες σε ερώτηση τύπου NS ή από ενδείξεις πρωτοκόλλων ανωτέρων στρωμάτων.

Μηχανισμοί Μετάβασης

Κατά την δεκαετία του ’90 είχε εδραιωθεί η ιδέα ότι η μετάβαση στο IPv6 θα ήταν πολύ γρήγορη και θα λειτουργούσε ως χιονοστιβάδα στην τεχνολογία του διαδικτύου. Για αυτό δημιουργήθηκαν πολλές ομάδες εργασίας οι οποίες θα μελετούσαν το σύνθετο πρόβλημα της μετάβασης στη νέα τεχνολογία του διαδικτύου. Η δυναμική της μετάβασης των δικτύων (δρομολογητών) και των τερματικών συστημάτων (hosts) στο νέο πρωτόκολλο ήταν εντελώς διαφορετική. Για τους τερματικούς σταθμούς εμφανίστηκαν σχετικά γρήγορα επικαιροποιήσεις του λειτουργικού τους συστήματος που υλοποιούσε διπλές στοίβες (Dual Stack). Στον μηχανισμό διπλών στοιβών, ο εξοπλισμός υλοποιεί παράλληλα τα δύο πρωτόκολλα IPv4 και IPv6 και επιτρέπει την συνύπαρξη συσκευών IPv4 και IPv6 στο ίδιο δίκτυο. Όμως η επικαιροποίηση των δικτύου άργησε με αποτέλεσμα να εμφανιστούν αρκετές λύσεις ενθυλάκωσης για τη διάβαση μέσω νησίδων IPv4 δικτύων, όπως (6bone, 6to4, 6rd, teredo, …).

Μηχανισμός Ενθυλάκωσης Teredo

Μεταξύ των μηχανισμών μετάβασης, ο teredo είναι μια ενδιαφέρουσα λύση, ικανή να διασχίζει τις νησίδες NAT που συναντιούνται στα οικιακά περιβάλλοντα. Εδώ ο τερματικός σταθμός ενθυλακώνει τα πακέτα IPv6 σε πακέτα IPv4 ως μηνύματα πρωτοκόλλου UDP. Η επιλογή του UDP έγινε για να μην παρουσιάζονται προβλήματα με τους μηχανισμούς NAT. Ο μηχανισμός teredo υποστηρίζεται εγγενώς σε σύγχρονα λειτουργικά συστήματα ως εικονική διεπαφή (pseudo

interface) μέσω της οποίας διέρχονται ενθυλακωμένα πακέτα IPv6. Χρησιμοποιεί διευθύνσεις από το πρόθεμα 2001:0:/32 που σχηματίζονται ως εξής:

Bit 0 έως 31 το Teredo prefix (2001:0::/32)

Bit 32 έως 63 η κύρια διεύθυνση του εξυπηρετητή Teredo

Bit 64 έως 79 διάφορες σημάνσεις (flags)

Bit 80 έως 95 η θύρα UDP που το NAT δίνει στον πελάτη με όλα τα bit αντεστραμμένα

Bit 96 έως 127 η δημόσια διεύθυνση IPv4 του NAT με όλα τα bit αντεστραμμένα

Για παράδειγμα η IPv6 διεύθυνση 2001:0000:4136:e378:8000:63bf:3fff:fdd2 αναφέρεται σε πελάτη Teredo:

- που χρησιμοποιεί Teredo server με διεύθυνση 65.54.227.120 (4136e378 σε δεκαεξαδικό),
- μέσω NAT στην UDP θύρα 40000 (40000_{10} = $9c40_h$ = NOT($63bf_h$))
- και δημόσια διεύθυνση IPv4 μετά το NAT 192.0.2.45 ($192.0.2.45_{10}$ = $c000022d_h$ = NOT($3ffffdd2_h$)

Οδηγίες εγκατάστασης δυναμικών πρωτοκόλλων για το IPv6

Στις ασκήσεις που ακολουθούν θα χρησιμοποιήσετε τις εκδόσεις των δυναμικών πρωτοκόλλων RIP και OSPF που υποστηρίζουν το IPv6, δηλαδή τις RIPng και OSPFv3, αντίστοιχα.

Εάν χρησιμοποιήσετε τον εικονικό δρομολογητή BSDRP, θα βρείτε τα RIPng και OSPFv3 εγκατεστημένα. Όμως για να τα ενεργοποιήσετε πρέπει να προσθέσετε στα quagga_deamons του αρχείου /etc/rc.conf τα ripngd, ospf6d, bgpd και να επανεκκινήσετε την υπηρεσία με "service quagga restart".

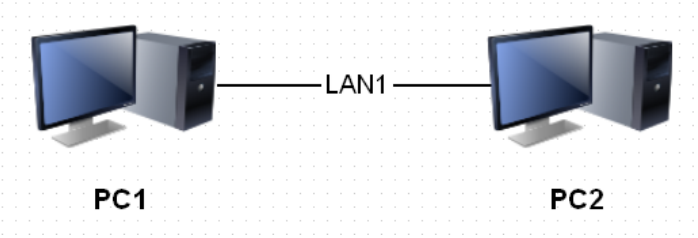
Αν έχετε εγκαταστήσει το Quagga μόνοι σας στο FreeBSD με βάση τις οδηγίες της προηγούμενης εργαστηριακής άσκησης, θα χρειαστεί να ξεκινήσετε τη διεργασία ripngd και ospf6d ως εξής:

1. Κλείστε την υπηρεσία quagga με "service quagga stop".
2. "touch /usr/local/etc/quagga/ripngd.conf" ώστε να δημιουργήσετε άδειο αρχείο παραμετροποίησης RIPng για το quagga.
3. "touch /usr/local/etc/quagga/ospf6d.conf" ώστε να δημιουργήσετε άδειο αρχείο παραμετροποίησης OSPFv3 για το quagga.
4. "touch /usr/local/etc/quagga/bgpd.conf" ώστε να δημιουργήσετε άδειο αρχείο παραμετροποίησης BGP για το quagga.
5. "chown quagga:quagga /usr/local/etc/quagga/*" για να ρυθμίσετε σωστά τον ιδιοκτήτη των αρχείων.
6. Ξεκινήστε την υπηρεσία quagga ξανά με "service quagga start".

Επειδή τα δυναμικά πρωτόκολλα υλοποιούνται σε ξεχωριστές διεργασίες στο quagga, ο πιο απλός τρόπος για να τα παραμετροποιήσετε είναι με το ενιαίο περιβάλλον που παρέχει το vtysh. Διαφορετικά, μπορείτε να συνδεθείτε με telnet (στη θύρα 2603/tcp για το RIPng, θύρα 2606/tcp για το OSPFv3 και θύρα 2605/tcp για το BGP), αφού πρώτα ορίσετε συνθηματικό στο αρχείο παραμετροποίησης του κάθε πρωτοκόλλου (ripngd.conf για το RIPng, ospf6d.conf για το OSPFv3 και bgpd.conf για το BGP).

Άσκηση 1: Εισαγωγή στο IPv6

Κατασκευάστε στο VirtualBox την παρακάτω τοπολογία. Το IPv6 είναι απενεργοποιημένο στο FreeBSD και θα πρέπει να το ενεργοποιήσετε. Για τη διεπαφή em0, η εντολή είναι "ifconfig em0 inet6 –ifdisabled accept_rtadv"και αν θέλετε η ρύθμιση να παραμείνει και μετά από reboot θα πρέπει να προσθέσετε στο αρχείο /etc/rc.conf τη γραμμή ifconfig_em0_ipv6=" inet6 accept_rtadv" και να επανεκκινήσετε το εικονικό μηχάνημα.



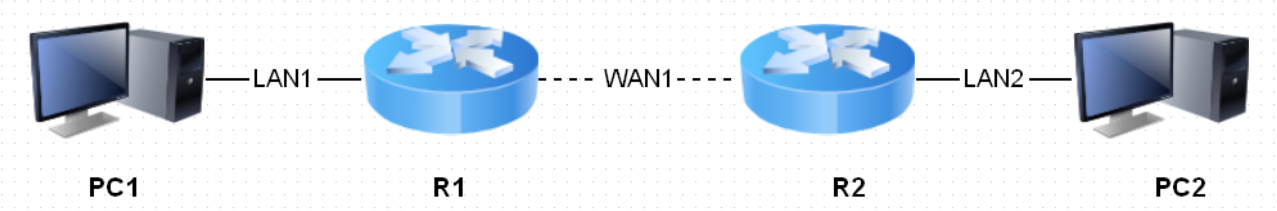
Απαντήστε τις παρακάτω ερωτήσεις καταγράφοντας παράλληλα, όπου απαιτείται, την ακριβή σύνταξη των εντολών που χρησιμοποιήσατε. *Προσοχή, στο IPv6 οι αντίστοιχες εντολές για ping και traceroute είναι οι ping6 και traceroute6.*

1.1 Ποιες διευθύνσεις IPv6 έχουν αποδοθεί στις διεπαφές του PC1;
1.2 Ποιες διευθύνσεις IPv6 έχουν αποδοθεί στις διεπαφές του PC2;
1.3 Τι είδους είναι αυτές οι διευθύνσεις IPv6;
1.4 Σε κάποιο από τα δυο PC εμφανίστε τον πίνακα δρομολόγησης για το IPv6. Πόσες εγγραφές υπάρχουν;
1.5 Στον πίνακα δρομολόγησης η στήλη Netif υποδεικνύει τη διεπαφή εξόδου των πακέτων για τον δεδομένο προορισμό. Πόσες από τις προηγούμενες εγγραφές αφορούν τη διεπαφή em0;
1.6 Από το PC1 κάντε ping στην link-local διεύθυνση του PC2. *[Υποδ. Θα πρέπει να προσδιορίσετε τον δείκτη ζώνης της **απερχόμενης** διεπαφής στο **PC1**.]*
1.7 Ορίστε στη διεπαφή του PC1 στο LAN1 τη στατική διεύθυνση fc80:1::2/64.
1.8 Ορίστε στη διεπαφή του PC2 στο LAN1 τη στατική διεύθυνση fc80:1::3/64.
1.9 Πόσες διευθύνσεις υπάρχουν στις διεπαφές em0 των PC;
1.10 Εμφανίστε ξανά τον πίνακα δρομολόγησης για το IPv6. Πόσες εγγραφές αφορούν τη διεπαφή em0 τώρα;
1.11 Τι πρέπει να προσθέσετε και σε ποια αρχεία για να μπορείτε να χρησιμοποιείτε τα ονόματα των μηχανημάτων αντί των IP διευθύνσεών τους στις διάφορες δικτυακές εντολές;
1.12 Μετά την αλλαγή αυτή μπορείτε να κάνετε ping από το PC1 στο PC2 χρησιμοποιώντας το όνομά του;
1.13 Στο PC1 εμφανίστε τον πίνακα ARP. Πόσες εγγραφές βλέπετε;
1.14 Εμφανίστε τη βοήθεια της εντολής NDP.
1.15 Ποια είναι η σύνταξη της παραπάνω εντολής για να εμφανίσετε τον πίνακα NDP του PC1;
1.16 Πόσες εγγραφές βλέπετε;
1.17 Τι διάρκεια ζωής βλέπετε να έχουν οι εγγραφές;
1.18 Στο PC1 ξεκινήστε μια καταγραφή πακέτων σε χωριστό παράθυρο.
1.19 Καθαρίστε τον πίνακα NDP.
1.20 Εκτελέστε την εντολή "ping6 –c 1 PC2". Τι είδους πακέτα IP βλέπετε;

1.21 Μηνύματα ποιου πρωτοκόλλου μεταφέρουν τα πακέτα IPv6 της καταγραφής και ποια είναι η τιμή του πεδίου Next header της επικεφαλίδας που το προσδιορίζει;
1.22 Σχεδιάστε ένα διάγραμμα που να δείχνει τη σειρά αποστολής και τον τύπο των μηνυμάτων που καταγράψατε προηγουμένως.

Άσκηση 2: SLAAC και Στατική δρομολόγηση IPv6

Κατασκευάστε στο VirtualBox την παρακάτω τοπολογία. Κρατήστε τα PC από την προηγούμενη άσκηση.



Απαντήστε τις παρακάτω ερωτήσεις καταγράφοντας παράλληλα, όπου απαιτείται, την ακριβή σύνταξη των εντολών που χρησιμοποιήσατε.

2.1 Διαγράψτε τη διεύθυνση fc80:1::3/64 στο PC2 και ορίστε στατική διεύθυνση fc80:2::2/64.
2.2 Ορίστε στο quagga του R1 τη διεύθυνση fc80:1::1/64 για το LAN1.
2.3 Ορίστε στο quagga του R1 τη διεύθυνση fc80:3::1/126 για το WAN1.
2.4 Ορίστε στο quagga του R2 τη διεύθυνση fc80:2::1/64 για το LAN2.
2.5 Ορίστε στο quagga του R2 τη διεύθυνση fc80:3::2/126 για το WAN1.
2.6 Ορίστε τη σωστή προεπιλεγμένη πύλη στο PC1 με την εντολή "route add -inet6".
2.7 Ορίστε τη σωστή προεπιλεγμένη πύλη στο PC2.
2.8 Ενεργοποιήστε στους R1 και R2 την προώθηση πακέτων IPv6.
2.9 Ενεργοποιήστε μια καταγραφή πακέτων στο PC1.
2.10 Από το PC1 μπορείτε να κάνετε ping στο PC2; Αιτιολογήστε.
2.11 Τι είδους μηνύματα παράγονται και ποια είναι η IPv6 διεύθυνση προορισμού τους;
2.12 Στο quagga του R1 προσθέστε την κατάλληλη στατική εγγραφή για το LAN2.
2.13 Από το PC1 μπορείτε να κάνετε ping στο PC2; Αιτιολογήστε.
2.14 Στο quagga του R2 προσθέστε την κατάλληλη στατική εγγραφή για το LAN1.
2.15 Μπορείτε τώρα να κάνετε ping από το PC1 στο PC2;
2.16 Στο quagga του R1 η λειτουργία router advertisement είναι ρητά απενεργοποιημένη για όλες τις διεπαφές όπως μπορείτε να δείτε με “show running-config”. Ενεργοποιήστε την.
2.17 Στο quagga του R1 για τη διεπαφή στο LAN1 ορίστε neighbor discovery prefix το fc80:1::/64 μέσω της εντολής "ipv6 nd prefix".
2.18 Στο quagga του R2 ενεργοποιήστε το router advertisement για όλες τις διεπαφές.
2.19 Στο quagga του R2 για τη διεπαφή στο LAN2 ορίστε neighbor discovery prefix το fc80:2::/64.
2.20 Ξεκινήστε μια καταγραφή πακέτων στον R1 στη διεπαφή στο LAN1.
2.21 Επανεκκινήστε την υπηρεσία δικτύου (netif) στο PC1.

2.22 Ποια μηνύματα ανταλλάσσονται κατά τη διαδικασία αυτόματης διευθυνσιοδότησης (SLAAC) του PC1;
2.23 Ποια διεύθυνση έχει λάβει το PC1 αυτόματα μέσω του SLAAC;
2.24 Από το PC2 μπορείτε να κάνετε ping στο PC1 χρησιμοποιώντας τη διεύθυνση που αποδόθηκε αυτόματα;
2.25 Πόσες εγγραφές έχουν προστεθεί στον πίνακα δρομολόγησης του PC1;

Άσκηση 3: Δυναμική δρομολόγηση IPv6

Θα χρησιμοποιήσετε την τοπολογία της προηγούμενης άσκησης.

Απαντήστε τις παρακάτω ερωτήσεις καταγράφοντας παράλληλα, όπου απαιτείται, την ακριβή σύνταξη των εντολών που χρησιμοποιήσατε.

3.1 Διαγράψτε τις στατικές διαδρομές από το quagga του R1 και R2.
3.2 Μπορείτε να κάνετε ping από το PC1 στο PC2;
3.3 Ενεργοποιήστε το RIPng στους δύο δρομολογητές βάζοντας τα κατάλληλα δίκτυα για ανταλλαγή πληροφορίας δρομολόγησης μεταξύ τους.
3.4 Εμφανίστε στον R1 τον πίνακα δρομολόγησης IPv6 για το RIPng. Πόσες δυναμικές εγγραφές βλέπετε;
3.5 Μπορείτε να κάνετε ping από το PC1 στο PC2;
3.6 Απενεργοποιήστε το RIPng στους R1 και R2.
3.7 Ενεργοποιήστε το OSPF6 βάζοντας router-id 1.1.1.1 και 2.2.2.2 στον R1 και R2 αντίστοιχα.
3.8 Στην παραμετροποίηση του OSPF6 δηλώστε τις διεπαφές στην περιοχή 0.0.0.0 στους R1 και R2 και περιμένετε λίγο.
3.9 Εμφανίστε στον R1 τον πίνακα δρομολόγησης IPv6 για το OSPF6. Πόσες δυναμικές εγγραφές βλέπετε;
3.10 Μπορείτε να κάνετε ping από το PC1 στο PC2;
3.11 Απενεργοποιήστε το OSPF6 στους R1 και R2.
3.12 Ενεργοποιήστε στον R1 το BGP χρησιμοποιώντας AS 65010 και router-id 1.1.1.1.
3.13 Δηλώστε τον R2 ως γείτονα με AS 65020.
3.14 Δηλώστε no neighbor activate για τον προηγούμενο γείτονα.
3.15 Από το υπο-μενού “address-family ipv6” του bgp router διαφημίστε το κατάλληλο δίκτυο και ενεργοποιήστε τον γείτονα.
3.16 Επαναλάβατε για τον R2 με το σωστό AS και router-id 2.2.2.2.
3.17 Περιμένετε περίπου 3 λεπτά και εμφανίστε στον R1 τον πίνακα δρομολόγησης IPv6 για το BGP. Πόσες δυναμικές εγγραφές βλέπετε;
3.18 Μπορείτε να κάνετε ping από το PC1 στο PC2;

Άσκηση 4: Μετάβαση στο IPv6

Για την επόμενη άσκηση θα χρειαστεί να χρησιμοποιήσετε μόνο τα 2 PC της προηγούμενης άσκησης όμως *σε δικτύωση NAT, αντί Internal,* αυτή τη φορά.

Απαντήστε τις παρακάτω ερωτήσεις καταγράφοντας παράλληλα, όπου απαιτείται, την ακριβή σύνταξη των εντολών που χρησιμοποιήσατε.

4.1 Ενεργοποιήστε τον DHCP client στις διεπαφές των εικονικών μηχανημάτων και βεβαιωθείτε ότι έχετε πρόσβαση στο Internet. *[Υποδ. Δείτε σελίδες βοήθειας για το dhclient]*.

4.2 Εγκαταστήστε και ενεργοποιήστε το teredo client μέσω των παρακάτω εντολών και στα 2 PC:

```
setenv PACKAGESITE http://ftp.ntua.gr/pub/FreeBSD/ports/i386/packages-
stable/Latest/
pkg_add -r miredo
vi /etc/rc.conf και προσθέστε miredo_enable="YES"
cp /usr/local/share/examples/miredo/miredo.conf
/usr/local/etc/miredo/miredo.conf
και από το κέλυφος "service miredo start"
```

Πόσες διεπαφές δικτύου βλέπετε;

4.3 Πόσες διευθύνσεις IPv6 έχει η διεπαφή teredo;

4.4 Μπορείτε να κάνετε ping από το PC1 στο PC2 χρησιμοποιώντας τις διευθύνσεις IPv6; Γιατί; *[Υποδ. Δείτε περιγραφή λειτουργίας του teredo και ειδικά του teredo relay στην ιστοσελίδα http://en.wikipedia.org/wiki/Teredo_tunneling#Node_types]*.

4.5 Ξεκινήστε καταγραφή πακέτων με το tcpdump στη διεπαφή teredo.

4.6 Σε άλλο παράθυρο δώστε την εντολή "ping6 www.ntua.gr". Τι είδους πακέτα IP και πρωτόκολλα ανωτέρου στρώματος βλέπετε;

4.7 Σταματήστε την προηγούμενη καταγραφή και ξεκινήστε νέα στη διεπαφή που είναι στο δίκτυο NAT.

4.8 Σε άλλο παράθυρο δώστε την εντολή "ping6 www.ntua.gr". Τι είδους πακέτα IP και πρωτόκολλα ανωτέρου στρώματος βλέπετε;

Ονοματεπώνυμο:	**Όνομα PC:**
Ομάδα:	**Ημερομηνία:**
Διεύθυνση IP: . . .	**Διεύθυνση MAC: - - - - -**

Εργαστηριακή Άσκηση 9
Το πρωτόκολλο IPv6

Απαντήστε στα ερωτήματα στον χώρο που σας δίνεται παρακάτω και στην πίσω σελίδα εάν δεν επαρκεί. Το φυλλάδιο αυτό θα παραδοθεί στον επιβλέποντα.

1

1.1 .....

.....

.....

1.2 .....

.....

.....

1.3 .....

.....

.....

1.4 .....

1.5 .....

1.6 .....

1.7 .....

1.8 .....

1.9 .....

1.10 .....

1.11 .....

.....

.....

1.12 .....

1.13 .....

1.14 .....

1.15 .....

1.16 .....

1.17 .....

.....

.....

1.18 .....

1.19 .....

1.20 .....

1.21 .....

.....

1.22 .....

PC1 PC2

2

2.1 .....

2.2 .....

2.3 .....

2.4 .....

2.5 .....

2.6 .....

2.7 .....

2.8 .....

2.9 .....

2.10 .....

.....

2.11 .....

.....

2.12 .....

2.13 .....