Εργαστηριακή Άσκηση 11
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 τη 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, το 1998 ακολούθησε μια πιο ενημερωμένη έκδοση, το RFC 2460, και το 2017 εκδόθηκε στην τελική του μορφή, το RFC 8200. Εντούτοις, η αναμενόμενη εξάντληση των διευθύνσεων IPv4 καθυστέρησε 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 και 192.168.0.0/16, στο εσωτερικό των ιδιωτικών δικτύων καθώς και των 100.64.0.0/10 από παρόχους.

Η IANA (Internet Assigned Numbers Authority) είναι ο αρμόδιος οργανισμός που διαχειρίζεται ομάδες διευθύνσεων σε παγκόσμιο 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 εξάντλησε τις διευθύνσεις, δηλαδή, απέμειναν μόνο οι αναγκαίες για τη μετάβαση σε IPv6, την 19/4/2011, το RIPE NCC την 14/9/2012, το LACNIC την 10/6/2014, το ARIN την 24/9/2015 και το AfriNIC την 31/12/2021. Θα περάσει όμως 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.

Το IPv6 σχεδιάσθηκε για να αντικαταστήσει το IPv4, όχι να διαλειτουργεί με το IPv4. Η απευθείας επικοινωνία με κόμβους IPv4 είναι αδύνατη και αυτό, σε συνδυασμό με την ανάγκη ανάπτυξης μηχανισμών μετάβασης, καθυστέρησε την εισαγωγή του IPv6. Σήμερα, παρά την εξάντληση των διευθύνσεων, η πλειονότητα της διαδικτυακής κίνησης είναι ακόμη IPv4. Στο τέλος του 2014 μόνο το 1% της κίνησης ήταν IPv6. Η κίνηση IPv6 αυξάνει σταδιακά, αλλά υπάρχουν σημαντικές διακυμάνσεις ανά πάροχο, χώρα και γεωγραφική περιοχή. Το AMS IX (Amsterdam Internet exchange) δημοσιεύει στατιστικά που δείχνουν κίνηση IPv6 περί το 6% (δείτε https://stats.ams-ix.net/sflow/ether_type.html). Όμως ο αριθμός χρηστών που χρησιμοποιούν IPv6 αυξάνει πολύ πιο γρήγορα, αφού όλα τα μοντέρνα λειτουργικά συστήματα το υποστηρίζουν εγγενώς. Για παράδειγμα, οι χρήστες των υπηρεσιών της Google που χρησιμοποιούν το IPv6 έχουν ξεπεράσει φέτος το 40%

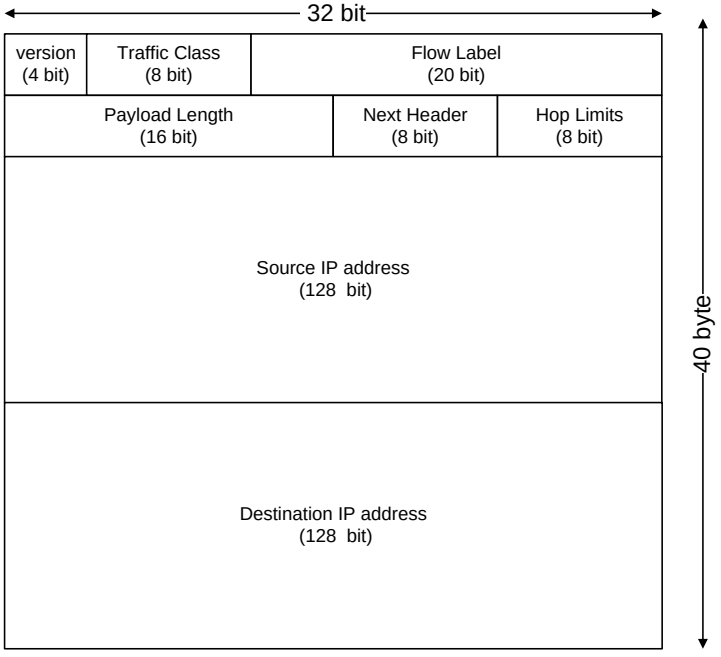
(δείτε ιστοσελίδα https://www.google.com/intl/en/ipv6/statistics.html). Σημαντικό στοιχείο είναι και η διαθεσιμότητα ιστοσελίδων μέσω IPv6. Υπολογίζεται ότι παγκοσμίως περίπου το 25% των ιστοθέσεων στο διαδίκτυο είναι διαθέσιμες και με IPv6 (δείτε https://w3techs.com/technologies/details/ce-ipv6).

Πακέτο 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 τους 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). Προβλέπεται μια ελάχιστη MTU των 1280 byte για τα πακέτα IPv6, τα οποία σε τοπικά δίκτυα (LAN) μεταφέρονται ως πλαίσια Ethernet, και ορίζεται νέος τύπος δεδομένων για τη μεταφορά πακέτων IPv6, το Ethertype 0x86DD αντί για το 0x0800. 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 σχεδίαση της επικεφαλίδας στοχεύει στην αποδοτικότητα και έχει απλούστερη δομή, 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 έχει σταθερό μέγεθος (40 byte) και περιέχει μόνο βασικές πληροφορίες όπως διευθύνσεις και μέγεθος πακέτου.



Επικεφαλίδα πακέτου IPv6

Δεν υπάρχει το 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 σε κάθε βήμα είναι η κύρια πηγή καθυστέρησης κατά την επεξεργασία του πακέτου. Επίσης, έχουν απαλειφτεί τα πεδία που σχετίζονται με τον θρυμματισμό. Εάν απαιτείται θρυμματισμός, αυτός γίνεται από τον αποστολέα, ενώ οι δρομολογητές IPv6 δεν θρυμματίζουν πακέτα. Τέλος δεν υπάρχουν οι επιλογές (options) της επικεφαλίδας IPv4, οι οποίες, αν και επιτρέπονται στο IPv6, βρίσκονται εκτός της επικεφαλίδας IPv6 (δείτε πιο κάτω πεδίο “Next Header”). Τέτοιου είδους πληροφορίες κωδικοποιούνται πιο αποδοτικά σε αλληλουχία Επικεφαλίδων επέκτασης (Extension

headers), οι οποίες προστίθενται σύμφωνα με τις ανάγκες των εφαρμογών ή βάσει άλλων απαιτήσεων, όπως για παράδειγμα, η υποστήριξη κινητικότητας[1]. Η μορφή της βασικής επικεφαλίδας φαίνεται στο προηγούμενο σχήμα. Τα πεδία της επικεφαλίδας είναι:

Version

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

Traffic Class

Νέο όνομα και αλλαγή θέσης, ίδια λειτουργικότητα με το ToS/DiffServ του IPv4. 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).

Flow Label

Ταυτοποιεί μια ομάδα πακέτων που ανήκουν στην ίδια ροή (flow), όμως η έννοια της "ροής" δεν ορίζεται καλώς στο πρότυπο. Αρχικά δημιουργήθηκε ώστε υπηρεσίες πραγματικού χρόνου να απολαμβάνουν ξεχωριστή εξυπηρέτηση (π.χ. τα πακέτα τους να ακολουθούν την ίδια διαδρομή στο δίκτυο). Η ετικέτα ροής μαζί με τις διευθύνσεις πηγής και προορισμού επιτρέπει τον χαρακτηρισμό ροών μόνο βάσει επικεφαλίδων του στρώματος δικτύου. Στα πακέτα IPv4 δεν υπάρχει παρόμοιο πεδίο. Εκεί για τον χαρακτηρισμό ροών απαιτούνται και επικεφαλίδες του στρώματος μεταφοράς (θύρες tcp ή udp), η θέση των οποίων εξαρτάται από το μήκος της επικεφαλίδας IPv4.

Payload Length

Νέο όνομα και αλλαγή θέσης για το μήκος πακέτου, αντίστοιχο του Total Length στο IPv4. Είναι το μέγεθος σε byte του περιεχομένου, δηλαδή, το μήκος πακέτου χωρίς τη βασική επικεφαλίδα, συμπεριλαμβανομένων των επικεφαλίδων επέκτασης, με άνω όριο την τιμή των 64 KB.

Next Header

Ρόλος περίπου ανάλογος του πεδίου Protocol στο IPv4. Καθορίζει το είδος των δεδομένων που έπονται της βασικής επικεφαλίδας, π.χ. πρωτόκολλο στρώματος μεταφοράς (TCP, UDP) ή επικεφαλίδα επέκτασης. Όταν υποδεικνύει πρωτόκολλο ανωτέρου στρώματος π.χ. TCP, UDP, ICMP, χρησιμοποιούνται οι ίδιες τιμές με αυτές του πεδίου Protocol στα πακέτα IPv4. Όταν ακολουθεί επικεφαλίδα επέκτασης, προσδιορίζει το είδος της. Το πλήθος των επικεφαλίδων επέκτασης είναι μεταβλητό και επιτρέπεται ο σχηματισμός αλυσίδας. Κάποιες από τις επόμενες επικεφαλίδες έχουν νόημα από άκρη-σε-άκρη, ενώ άλλες από βήμα-σε-βήμα μιας διαδρομής.

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 (εκτός και εάν έφτασε στον προορισμό του) και αποστέλλεται ένα μήνυμα τύπου ICMP στον αποστολέα. Με αυτό τον τρόπο αποφεύγεται αέναη κίνηση λόγω βρόχων στο δίκτυο.

Source Address

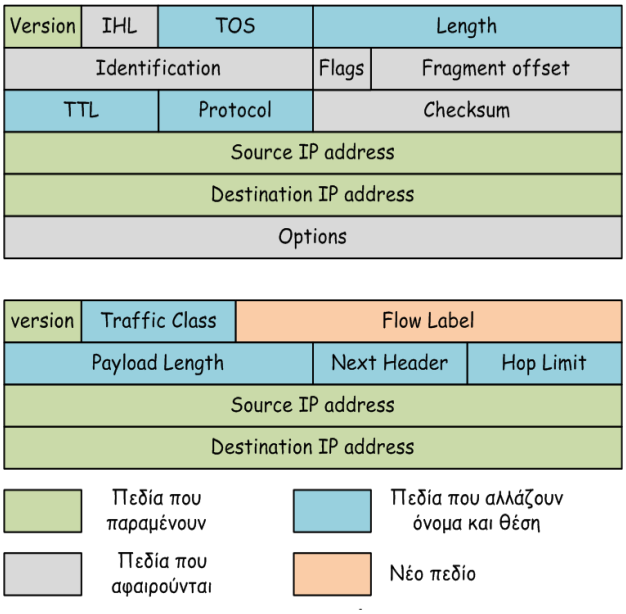
Η διεύθυνση πηγής μήκους 128 bit. Λεπτομέρειες για τη δομή της σε επόμενη παράγραφο.

Destination Address

Η διεύθυνση του παραλήπτη.

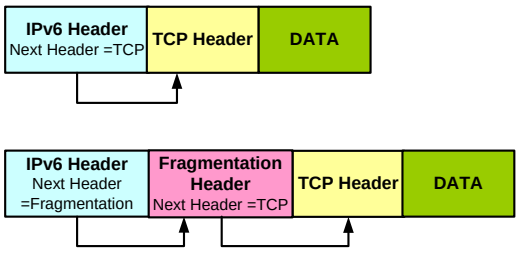
[1] Ένας κινούμενος κόμβος μπορεί να προσθέτει πληροφορίες δρομολόγησης με τη μορφή επιπλέον επικεφαλίδων στα εξερχόμενα πακέτα του και να επηρεάζει με τον τρόπο αυτό το μονοπάτι από το οποίο θα δρομολογούνται.

Στο επόμενο σχήμα βλέπετε παραστατικά τις ομοιότητες και διαφορές των επικεφαλίδων IPv4 και IPv6. 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 καταργήθηκαν ή μετακινήθηκαν σε νέες, άλλου τύπου επικεφαλίδες επέκτασης.



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 επέκτασης “IPv6 fragment” όπως φαίνεται στο ακόλουθο σχήμα.



Παράδειγμα ακολουθίας επικεφαλίδων

Πεδίο Next Header

Όπως προαναφέρθηκε οι τιμές του Next Header στο IPv6 και του Protocol στο IPv4 είναι ίδιες όσον αφορά τα πρωτόκολλα ανωτέρου στρώματος (TCP, UDP, κλπ). Αμφότερα τα πεδία έχουν μήκος 8 bit. Στο IPv6 ορίζονται νέες τιμές για τις επικεφαλίδες επέκτασης. Ο επόμενος πίνακας αναφέρει τις πιο σημαντικές.

Πεδίο (δεκαδική τιμή)	Επικεφαλίδα επέκτασης	Χρήση
0	Hop by Hop	Προαιρετικές επιλογές που πρέπει να εξετασθούν από όλους τους κόμβους της διαδρομής, όπως η υποστήριξη jumbograms ή τα μηνύματα Router Alert.
43	Routing	Μέθοδοι για τον ορισμό ενδιάμεσων κόμβων της διαδρομής από την πηγή (όπως στο source routing του IPv4) και για την υποστήριξη κινητικότητας Mobile IPv6.
44	Fragment	Για πακέτα που έχουν θρυμματισθεί (στην πηγή), οι τιμές που προσδιορίζουν τη θέση του θραύσματος στο αρχικό πακέτο (όπως στο IPv4).
50	Encapsulating Security Payload (ESP)	Κρυπτογραφημένα δεδομένα για ασφαλή επικοινωνία.
51	Authentication Header (AH)	Πληροφορία για την πιστοποίηση αυθεντικότητας του πακέτου.
59	No next header	Το πακέτο IPv6 τελειώνει με αυτή την επικεφαλίδα.
60	Destination Option	Πληροφορίες που πρέπει να εξετασθούν μόνο από τον προορισμό, π.χ. το Home Address για την υποστήριξη Mobile IPv6.
135	Mobility	Παράμετροι για τη δημιουργία και διαχείριση των σχέσεων μεταξύ mobile nodes, correspondent nodes και home agents στο Mobile IPv6.

Αυτός ο μηχανισμός αλληλουχίας επικεφαλίδων ενέχει κάποια πολυπλοκότητα η οποία έγκειται στο ότι απαιτείται συνολική ανάγνωση όλων των επικεφαλίδων για να καταστεί εφικτή η προώθηση του πακέτου IPv6. 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 κόμβων μέσω των οποίων υποχρεούται να περάσει το πακέτο. Έχουν οριστεί δύο τύποι επικεφαλίδων δρομολόγησης (που ταυτοποιούνται από πεδίο εντός της επικεφαλίδας). Ο ορισμός είναι επεκτάσιμος και μπορεί να προστεθούν περισσότεροι τύποι επικεφαλίδων αργότερα εάν χρειαστεί. Ο τύπος 0, η χρήση του οποίου καταργήθηκε διότι δεν αποτρέπει κυκλικές διαδρομές (RFC 5095), ορίζει μια αυθαίρετη διαδρομή από διευθύνσεις IPv6 τις οποίες πρέπει να διασχίσει το πακέτο. Ο τύπος 2 χρησιμοποιείται για υποστήριξη κινητικότητας στο IPv6 (RFC 6275).

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 κόμβοι απομένουν. Ο σταθμός που επιθυμεί να χρησιμοποιήσει το παραπάνω χαρακτηριστικό προσθέτει την επικεφαλίδα δρομολόγησης και τοποθετεί τη διεύθυνση του πρώτου κόμβου στο πεδίο της διεύθυνσης προορισμού της βασικής επικεφαλίδας. Προσθέτει δε την ακολουθία διευθύνσεων των ενδιάμεσων κόμβων στην επικεφαλίδα δρομολόγησης. Ο τελικός προορισμός του πακέτου είναι ο τελευταίος κόμβος στην ακολουθία που περιγράφεται στην επικεφαλίδα δρομολόγησης. Το πεδίο Segments Left δείχνει πόσοι ενδιάμεσοι κόμβοι απομένουν μέχρι την τελική παράδοση του πακέτου. Στη συνέχεια το πακέτο ακολουθεί την τυπική διαδικασία δρομολόγησης. Με την παραλαβή του πακέτου από τον κόμβο που περιγράφεται στο πεδίο Destination Address, ο δρομολογητής εντοπίζει την επικεφαλίδα δρομολόγησης και αντιλαμβάνεται

ότι αποτελεί ενδιάμεσο σταθμό. Ανταλλάσσει τη διεύθυνση προορισμού με τη N-οστή (μετρώντας από το τέλος) διεύθυνση στην ακολουθία κόμβων, όπου N είναι η τρέχουσα τιμή του πεδίου Segments Left. Στη συνέχεια μειώνει κατά ένα την τιμή του πεδίου Segments Left και το πακέτο στέλνεται στο νέο του προορισμό που είναι ο επόμενος κόμβος. Αυτή η διαδικασία εκτελείται σε κάθε ενδιάμεσο κόμβο. 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 περιέχει μία μόνο διεύθυνση, την οικία διεύθυνση (Home address) του κινητού σταθμού. Ο κινητός σταθμός IPv6 που επισκέπτεται ένα νέο υποδίκτυο αποκτά μια νέα διεύθυνση (care of address). Τα πακέτα που προορίζονται για τον κινητό κόμβο προωθούνται στη διεύθυνση care of address αλλά προστίθεται μια επικεφαλίδα δρομολόγησης (τύπου 2) η οποία περιέχει τη διεύθυνση Home Address. Όταν το πακέτο παραδίδεται, ως διεύθυνση προορισμού τίθεται η Home address και έτσι τα ανώτερα 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. Επομένως 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 στις ζεύξεις που υποστηρίζουν IPv6 τα 1280 byte (με συνιστώμενη τιμή τα 1500 byte). Ο αποστολέας ξεκινά να στέλνει πακέτα μεγέθους όσο του επιτρέπει η MTU της ζεύξης. Εάν κάποιος ενδιάμεσος κόμβος δεν μπορεί να προωθήσει το πακέτο εξαιτίας μικρής τιμής της MTU απορρίπτει το πακέτο και στέλνει στον αποστολέα το μήνυμα ICMP τύπου packet too big που περιλαμβάνει την τιμή της MTU της προβληματικής ζεύξης. Ο αποστολέας θα μειώσει την MTU της διαδρομής στην υποδεικνυόμενη τιμή και η διαδικασία μπορεί να επαναληφθεί όσες φορές χρειαστεί (μέχρι το 1280 που υποστηρίζεται από όλους).

Επιλογές (Options)

Οι επικεφαλίδες επέκτασης 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 την έχουν ορίσει μπορούν να ενεργοποιήσουν το ενδιαφέρον όλων των δρομολογητών π.χ. για τη δέσμευση πόρων κατά μήκος της διαδρομής.

Jumbo payload

Επιτρέπει τη μεταφορά πακέτων με περιεχόμενο που είναι μεγαλύτερο από το μέγιστο των 64 KB. Η εν λόγω επιλογή ζητά τη χρήση πακέτων jumbograms με μέγιστο μέγεθος περιεχομένου τα 4 GB.

Home Address

Χρησιμοποιείται από τον κινητό σταθμό για να ενημερώσει τον λήπτη για την οικία διεύθυνσή (home address) του.

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.

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

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. 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.

Η δομή των διευθύνσεων IPv6 ακολουθεί μια ιεραρχία δύο επιπέδων (δίκτυο – διεπαφή) με ένα πρόθεμα δικτύου που χρησιμοποιείται για δρομολόγηση, ένα αριθμό του υποδικτύου, που προσδιορίζει μοναδικά το τελικό δίκτυο (δίκτυο πελάτη), που και αυτό μπορεί να χωρισθεί σε υποδίκτυα όπως γίνεται στο CIDR, και μια ταυτότητα διεπαφής. Οι βασικοί κανόνες της

αριθμοδότησης του IPv6 ορίζονται στο RFC 4291. Συνοδευτικά RFC ορίζουν περιπτώσεις και χρήσεις ειδικού τύπου διευθύνσεων. Υπάρχουν τρεις τύποι διευθύνσεων:

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

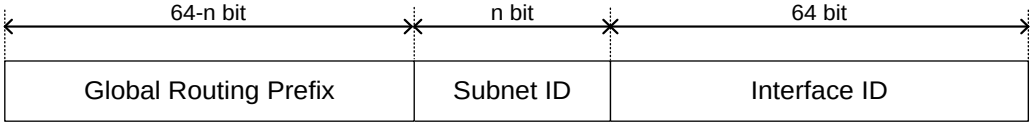
Διευθύνσεις Anycast που προσδιορίζουν μια ομάδα διεπαφών συνήθως σε διαφορετικούς host. Ένα πακέτο που αποστέλλεται σε μια τέτοια διεύθυνση παραδίδεται σε μία μόνο διεπαφή, δρομολογούμενο συνήθως στην πλησιέστερη της ομάδας.

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

Δεν υπάρχουν διευθύνσεις εκπομπής (Broadcast). Η εκπομπή προς όλες τις διεπαφές μπορεί να γίνει με ειδικού τύπου διευθύνσεις multicast.

Διευθύνσεις Unicast

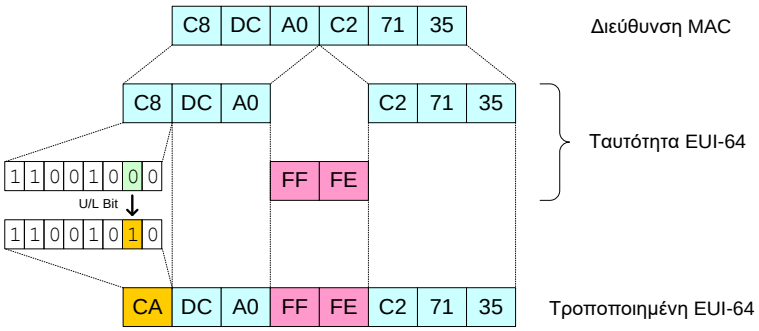
Όλος ο χώρος διευθύνσεων IPv6 πλην των multicast (ff00::/8) είναι διευθύνσεις unicast. Οι διευθύνσεις anycast δεν διαφέρουν συντακτικά από τις unicast. Εξαιρουμένων των link-local (fe80::/10) διευθύνσεων, οι υπόλοιπες διευθύνσεις unicast είναι παγκόσμιες (GUA – Global Unicast Addresses). Από τις διευθύνσεις GUA ένα μικρό μέρος, αυτές με πρόθεμα **2000::/3** του RFC 3587 έχουν διατεθεί για την επικοινωνία μεταξύ κόμβων στο δημόσιο διαδίκτυο. Σύμφωνα με το RFC 4291 όλες οι παγκόσμιες unicast διευθύνσεις, πλην αυτών που ξεκινούν με το δυαδικό 000, έχουν μήκος ταυτότητας διεπαφής 64 bit, με την ταυτότητα διεπαφής (IID –Interface ID) να ακολουθεί τη μορφή τροποποιημένης EUI-64. Η ταυτότητα διεπαφής μπορεί να παράγεται από τη διεύθυνση MAC αυτής, να δίδεται από εξυπηρετητή DHCPv6, να προκύπτει με τυχαίο τρόπο ή να τίθεται χειροκίνητα.



Δομή μιας διεύθυνσης τύπου Global Unicast

Τροποποιημένη EUI-64

Η ταυτότητα EUI-64 είναι μια διεύθυνση IEEE MAC μήκους 64 bit, ανάλογη προς τις συνήθεις διευθύνσεις MAC που είναι τύπου EUI-48. Το RFC 4291 καθορίζει την τροποποιημένη έκδοση της ταυτότητας EUI-64 αντιστρέφοντας το νόημα του 7ο bit του πρώτου byte και έτσι η τιμή 0 σημαίνει τοπικά (local) οριζόμενη και όχι παγκόσμια (universal) ταυτότητα. Ο λόγος αυτής της αλλαγής είναι η διευκόλυνση της χειροκίνητης ανάθεσης. Είναι πιο απλό να ορισθεί μια τοπική IID ως 0:0:0:1, ενώ εάν τηρηθεί η κανονική μορφή θα έπρεπε να είναι 0200:0:0:1.



Μετατροπή της διεύθυνσης MAC σε τροποποιημένη EUI-64

Η αυτόματη παραγωγή μιας ταυτότητας διεπαφής από τη διεύθυνση MAC προκύπτει παρεμβάλλοντας το ff:fe στο μέσο της και αντιστρέφοντας το 7ο bit του πρώτου byte, που στις διευθύνσεις MAC των καρτών δικτύου έχει τιμή 1, παγκόσμια μοναδική (globally unique) διεύθυνση. Έτσι για παράδειγμα η διεύθυνση MAC C8:DC:A0:C2:71:35 μετατρέπεται σε CADC:A0FF:FEC2:7135 όπως φαίνεται στο σχήμα.

Διευθύνσεις Multicast

Οι διευθύνσεις **ff00::/8** προορίζονται για πολλαπλή διανομή (multicast). Μετά το πρόθεμα ff ακολουθεί το πεδίο flags (4 bit), το πεδίο scope (4 bit) που ορίζει την εμβέλειά τους, περιοχή όπου ισχύουν, και η ταυτότητα ομάδας (group ID) μήκους 112 bit. Η τιμή 1 στο πεδίο flags δηλώνει προσωρινές διευθύνσεις, ενώ η τιμή 0 μόνιμες εκχωρούμενες από την IANA. Οι διευθύνσεις **ff01::** αφορούν τη διεπαφή, οι **ff02::** την τοπική ζεύξη και οι **ff05::** το τοπικό site. Εξ αυτών, η **ff01::1** παριστάνει όλους τους κόμβους στη διεπαφή και η **ff02::1** όλους τους κόμβους στη τοπική ζεύξη. Αντίστοιχα, η **ff01::2** παριστάνει όλους τους δρομολογητές στη διεπαφή, η **ff02::2** όλους τους δρομολογητές στη τοπική ζεύξη και η **ff05::2** όλους τους δρομολογητές στο τοπικό site.

Το IPv6 κάνει χρήση διευθύνσεων multicast σε συνδυασμό με τις διευθύνσεις πολλαπλής διανομής του Ethernet. Ένα πλαίσιο τύπου multicast Ethernet είναι αυτό που αποστέλλεται σε περισσότερους από ένα κόμβους. Το σύνολο των παραληπτών χαρακτηρίζεται από μια διεύθυνση τύπου multicast group και προσδιορίζεται από μια διεύθυνση 48-bit, όπως μια τυπική διεύθυνση Ethernet. Μια διεύθυνση MAC τύπου multicast διαφέρει από μια διεύθυνση unicast επειδή έχει ίσο με 1 το τελευταίο bit (το 8ο) του πρώτου byte (που είναι το πρώτο bit που μεταδίδεται στο φυσικό μέσο). Έτσι η MAC διεύθυνση 00-c0-4f-68-12-cb είναι τύπου unicast ενώ η διεύθυνση 33-33-ff-68-12-cb είναι multicast. Αυτό σημαίνει ότι η διεπαφή Ethernet πρέπει να ακούει για πλαίσια τα οποία απευθύνονται στην unicast διεύθυνσή της, αλλά και για πλαίσια των ομάδων multicast των οποίων είναι μέλος. Για την αποστολή πακέτων multicast IPv6 πάνω από Ethernet, δημιουργείται μια MAC διεύθυνση με το πρόθεμα 33-33- να ακολουθείται από τα τελευταία 32 bit της IPv6 διεύθυνσης προορισμού. Ένα πακέτο με διεύθυνση ff02::1:ff68:12cb θα σταλεί στη MAC διεύθυνση 33-33-ff-68-12-cb. Κάθε κόμβος που ενδιαφέρεται για πακέτα με αυτή τη διεύθυνση IPv6 θα πρέπει να διαβάζει πλαίσια Ethernet με την παραπάνω MAC διεύθυνση.

Ειδικές διευθύνσεις IPv6

Στην αριθμοδότητηση IPv6 η διεύθυνση **::/0** είναι η προκαθορισμένη διαδρομή. Η διεύθυνση **::/128** θεωρείται ως ακαθόριστη (Unspecified) και έχει νόημα μόνο σε πακέτα που δημιουργούνται προτού ο host αποκτήσει μια διεύθυνση (π.χ. μέσω DHCP). 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). Οι 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 μπλοκ **fe80::/64** έχει εκχωρηθεί, αντίστοιχο του 169.254.0.0/16 για το IPv4. Οι διευθύνσεις **fc00::/7** (local unicast) προορίζονται για δρομολόγηση στο εσωτερικό ιδιωτικών δικτύων. Το μπλοκ έχει χωρισθεί στα δύο. Το άνω μέρος **fd00::/8** προορίζεται για ψευδοτυχαίες μοναδικές τοπικές διευθύνσεις (ULA – Unique Local Addresses), όπου τα 40 bit μετά τα αρχικά 8 παράγονται τυχαία ώστε να είναι μοναδικά (global ID) και τα επόμενα 16 bit ορίζουν το υποδίκτυο (subnet ID). Μια διεύθυνση με πρόθεμα της μορφής fdxx:xxxx:xxxx::/48 δεν δρομολογείται στο δημόσιο διαδίκτυο και έχει χρήση ανάλογη των 10.0.0.0/8, 172.16.0.0/12 και 192.168.0.0/16 στο IPv4. Η χρήση του κάτω μέρους **fc00::/8** δεν έχει ορισθεί ακόμη.

Απαιτούμενες διευθύνσεις IPv6

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 υπακούν σε πρότυπα. Στο περιβάλλον IPv6, η κατάσταση είναι διαφορετική: η χρήση πολλαπλών διευθύνσεων επιβάλλεται για λόγους λειτουργικότητας. Οι απαιτούμενες διευθύνσεις για κάθε τερματικό κόμβο (που δεν προωθεί πακέτα σε άλλον) είναι:

- η διεύθυνση βρόχου επιστροφής **::1/128**
- μία τοπική στη ζεύξη (link-local) διεύθυνση 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 multicast 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. Η multicast διεύθυνση 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 fd00::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 08:2a:0f:32:5e:d1, συμμετέχει στα υποδίκτυα 2001:a:b:1::/64 και 2001:a:b:2::/64 και είναι μέλος της ομάδας ff15::1:2:3 πρέπει να λαμβάνει δεδομένα στις ακόλουθες διευθύνσεις:

- ::1 (loopback)
- fe80::a2a: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:1:a2a:fff:fe32:5ed1 (unicast κατόπιν ανάθεσης)
- 2001:a:b:2:a2a: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 subnet-router anycast διεύθυνση για κάθε υποδίκτυο όπου δρα ως δρομολογητής, που προσδιορίζει όλους τους δρομολογητές του υποδικτύου, και είναι το πρόθεμα δικτύου της τοπικής ζεύξης ακολουθούμενο από μηδενικά (το αντίστοιχο της διεύθυνσης δικτύου IPv4)
- 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)

Έτσι, εάν ο δρομολογητής διασυνδέει τα παραπάνω υποδίκτυα θα έχει επιπλέον τις διευθύνσεις:

- 2001:a:b:1:: (δρομολογητής υποδικτύου για το πρώτο υποδίκτυο)
- 2001:a:b:2:: (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:1::fdff:ffff:ffff:fffe (home agents στο πρώτο υποδίκτυο)
- 2001:a:b:2::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 τη συμπεριφορά και ως εκ τούτου ο τρόπος επιλογής της είναι σημαντικός. Η σύσταση RFC 6724 ορίζει τους κανόνες. Για διευθύνσεις πηγής ορίζονται κανόνες ταξινόμησης ώστε να προκύψει η "καλύτερη" διεύθυνση πηγής για μια δεδομένη διεύθυνση προορισμού. Ο αλγόριθμος ταξινόμησης σχηματίζει ένα σύνολο υποψηφίων CandidateSource(D) για τον προορισμό D και επιλέγεται η πρώτη διεύθυνση. Οι κανόνες εφαρμόζονται μόνο στις διευθύνσεις IPv6, όχι στις IPv4. Ο αλγόριθμος επιλογής διεύθυνσης προορισμού ξεκινά με μια λίστα διευθύνσεων, που τυπικά λαμβάνεται από το DNS, και διατάσσει τις διευθύνσεις σε μια νέα λίστα. Εδώ ο αλγόριθμος διατάσσει τόσο διευθύνσεις 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 σε όλες τις διεπαφές οι τοπικές στη ζεύξη (link-local) διευθύνσεις έχουν όλες το ίδιο πρόθεμα δικτύου (**fe80::/64**), η διαδικασία δρομολόγησης δεν μπορεί επιλέξει την απερχόμενη διεπαφή όταν ο προορισμός είναι τέτοια διεύθυνση. Για τον λόγο αυτό χρειάζεται επιπλέον πληροφορία δρομολόγησης. Στην αναγραφή των διευθύνσεων χρησιμοποιείται μια ειδική ταυτότητα που αποκαλείται δείκτης ζώνης (zone index). Ο δείκτης ζώνης προσδιορίζει τη διεπαφή 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

Ο πίνακας συνοψίζει τις συνήθως απαντούμενες στην πράξη διευθύνσεις IPv6

::0/128	Ακαθόριστη διεύθυνση
::1/128	Διεύθυνση βρόχου επιστροφής (Loopback)
ff00::/8	Διευθύνσεις πολλαπλής διανομής (Multicast)
fe80::/10	Διευθύνσεις τοπικές στη ζεύξη (Link-local)
fc00::/7	Μοναδικές τοπικές διευθύνσεις (Unique local)
::ffff:0:0/96	Διευθύνσεις IPv4-mapped
64:ff9b::/96	Διευθύνσεις IPv4-IPv6-translated (Well-Known Prefix)
2001::/32	Σήραγγες Teredo
2001:db8::/32	Διευθύνσεις για χρήση σε κείμενα και παραδείγματα
2002::/16	Διευθύνσεις 6to4
2400::/12	Διευθύνσεις που έχουν εκχωρηθεί στο APNIC
2600::/12	Διευθύνσεις που έχουν εκχωρηθεί στο ARIN
2800::/12	Διευθύνσεις που έχουν εκχωρηθεί στο ARIN
2A00::/12	Διευθύνσεις που έχουν εκχωρηθεί στο RIPE
2C00::/12	Διευθύνσεις που έχουν εκχωρηθεί στο AfriNIC

Ανακάλυψη γείτονα (Neighbor Discovery)

Η ανακάλυψη γείτονα αντικαθιστά το πρωτόκολλο ARP και είναι απαραίτητη για τη λειτουργία του IPv6. Υλοποιείται από όλους τους κόμβους και επιτρέπει σε αυτούς (υπολογιστές και δρομολογητές στην ίδια ζεύξη) να συνδεθούν και να διαφημίσουν την ύπαρξη τους στους γείτονες. Οι κόμβοι βρίσκουν τις link-local διευθύνσεις των γειτόνων στη ζεύξη, εντοπίζουν δρομολογητές που μπορούν να προωθήσουν τα πακέτα τους, παρακολουθούν ενεργά ποιοι γείτονες είναι προσβάσιμοι ή όχι, εντοπίζουν αλλαγές διευθύνσεων από αυτούς και διαγράφουν αποθηκευμένες διευθύνσεις όταν αυτές παύουν να ισχύουν. Επιπλέον, από τα μηνύματα που ανταλλάσσονται οι κόμβοι μπορούν να κατασκευάσουν τη διεύθυνσή τους όπως θα περιγραφεί στη συνέχεια. Η διαδικασία ανεύρεσης

γείτονα ορίζεται στο RFC 4861 και βασίζεται στη χρήση του πρωτοκόλλου ICMPv6 που ορίζεται στο RFC 4443. Χρησιμοποιούνται τα ακόλουθα μηνύματα πρωτοκόλλου ICMPv6:

- Router Solicitation (RS)
- Router Advertisement (RA)
- Neighbor Solicitation (NS)
- Neighbor Advertisement (NA)
- Redirect

Αναζήτηση δρομολογητή (Router Solicitation)

Ο κόμβος IPv6 στέλνει μήνυμα RS όταν θέλει να λάβει μηνύματα διαφήμισης δρομολογητών RA, ώστε να μάθει γρήγορα την αναγκαία πληροφορία για τις δικτυακές του ρυθμίσεις. Το μήνυμα RS είναι πακέτο ICMPv6 τύπου 133, με διεύθυνση πηγής αυτή του κόμβου, εάν αυτός ήδη έχει διεύθυνση IPv6, αλλιώς την ακαθόριστη διεύθυνση **::0**. Ως δε διεύθυνση προορισμού έχει τη διεύθυνση πολλαπλής διανομής όλοι οι δρομολογητές σε αυτή τη ζεύξη **ff02::2**. Το RS έχει στο πεδίο Hop Limit την τιμή 255.

Διαφήμιση δρομολογητή (Router Advertisement)

Η ανακάλυψη του πλησιέστερου δρομολογητή γίνεται με τη λήψη μηνυμάτων RA (Router Advertisement) είτε αυτά αποστέλλονται περιοδικά από τον δρομολογητή είτε σε απάντηση μηνυμάτων RS (Router Solicitation). Με βάση την πληροφορία από τα μηνύματα RA που λαμβάνουν, οι κόμβοι σχηματίζουν μια λίστα προκαθορισμένων δρομολογητών (Default Router List) και μια λίστα προθεμάτων (Prefix List). Η λίστα προθεμάτων ζεύξης (on-link) χρησιμεύει κατά την αποστολή πακέτων για να προσδιορισθεί το κατά πόσο ο προορισμός είναι επί της ζεύξης, δηλαδή, τοπικά προσβάσιμος σε αντίθεση με προθέματα εκτός ζεύξης (off-link) όπου απαιτείται η διαμεσολάβηση δρομολογητή. Η λίστα προκαθορισμένων δρομολογητών χρησιμεύει για να επιλεχθεί ο κατάλληλος δρομολογητής για τους εκτός ζεύξης προορισμούς. Για τους δρομολογητές, η λίστα προθεμάτων χρησιμοποιείται για την προώθηση πακέτων. Εάν η διεύθυνση προορισμού ενός πακέτου βρίσκεται εντός των προθεμάτων ζεύξης ο δρομολογητής το στέλνει στην εν λόγω ζεύξη, διαφορετικά το στέλνει σε κάποιο γειτονικό δρομολογητή.

Το μήνυμα RA είναι πακέτο ICMPv6 τύπου 134, με διεύθυνση πηγής την link-local της διεπαφής από όπου πηγάζει και διεύθυνση προορισμού τη διεύθυνση πολλαπλής διανομής όλοι οι κόμβοι σε αυτή τη ζεύξη **ff02::1** ή αυτή του κόμβου που το ζήτησε με RS. Το RA έχει στο πεδίο Hop Limit την τιμή 255. Εάν ο κόμβος λάβει μήνυμα με τιμή Hop Limit μικρότερη του 255, το πακέτο δεν είναι έγκυρο. Έτσι εξασφαλίζεται ότι το πακέτο δεν έχει περάσει μέσα από δρομολογητή. Τα μηνύματα RA περιέχουν την ακόλουθη πληροφορία:

- την τιμή του Hop Limit, που πρέπει να χρησιμοποιούν οι κόμβοι στο τοπικό δίκτυο,
- δύο σημαίες (flags), M και O, που δηλώνουν το κατά πόσο θα χρησιμοποιηθεί DHCPv6 για την αυτόματη ρύθμιση διευθύνσεων και με ποιο τρόπο, τη σημαία H, που δηλώνει ότι δρομολογητής είναι και Home Agent για Mobile IPv6, καθώς και το πεδίο Prf (2-bit), που δηλώνει το κατά πόσο να προτιμηθεί ο δρομολογητής ως προκαθορισμένος,
- τη χρονική διάρκεια ζωής (σε s) του δρομολογητή (router lifetime), μέγιστη τιμή 18,2 ώρες, που εάν είναι 0 αυτός ο δρομολογητής δεν μπορεί να χρησιμοποιηθεί ως προκαθορισμένος,
- την τιμή του Reachable Time (σε ms), διάρκεια χρόνου που ένας κόμβος θεωρείται προσβάσιμος μετά την επιβεβαίωση ύπαρξης επικοινωνίας με αυτόν,
- την τιμή του Retrans Timer (σε ms), το διάστημα αναμετάδοσης μηνυμάτων NS που χρησιμοποιείται από τη διαδικασία ανίχνευσης έλλειψης επικοινωνίας, και
- διάφορες προαιρετικές (options) πληροφορίες.

Από τις προαιρετικές πληροφορίες, το Prefix Information περιλαμβάνει ένα ή περισσότερα προθέματα IPv6 και δύο σημαίες A και L. Όταν τίθεται η σημαία A, οι τοπικοί κόμβοι χρησιμοποιούν τα προθέματα για τη λειτουργία αυτόματης ρύθμισης διευθύνσεων IPv6 (δείτε παρακάτω). Όταν τίθεται, η σημαία L δηλώνει ότι το πρόθεμα είναι on-link στην τοπική ζεύξη. Η προαιρετική πληροφορία Route Information διαφημίζει πιο συγκεκριμένες διαδρομές, απαλείφοντας την ανάγκη για χρήση πρωτοκόλλων δρομολόγησης ειδικά σε δίκτυα (multi-homed) με πολλαπλές συνδέσεις προς το διαδίκτυο. Η προαιρετική πληροφορία Source Link-Layer Address περιλαμβάνεται όταν ο δρομολογητής ξέρει τη διεύθυνση στρώματος 2 (MAC) από όπου στέλνει το μήνυμα RA. Η πληροφορία MTU, εάν υπάρχει, δηλώνει στους κόμβους την MTU του τοπικού δικτύου. Τέλος, οι προαιρετικές πληροφορίες Recursive DNS Server (RDNSS) και DNS Search List (DNSSL) παρέχουν τον εξυπηρετητή DNS και λίστα επιθεμάτων (suffixes) κατά την αναζήτηση ονομάτων.

Αναζήτηση γείτονα (Neighbor Solicitation)

Το μήνυμα αναζήτησης γείτονα NS στέλνεται για να βρεθεί η φυσική διεύθυνση του γείτονα ή για να επιβεβαιωθεί η προσβασιμότητα του γείτονα. Είναι μήνυμα ICMPv6 τύπου 135 multicast όταν χρησιμοποιείται για την ανεύρεση μιας διεύθυνσης και unicast όταν χρησιμοποιείται για επιβεβαίωση προσβασιμότητας. Ως διεύθυνση πηγής έχει είτε αυτήν της διεπαφής από όπου πηγάζει είτε την ακαθόριστη **::0**. Η διεύθυνση προορισμού του είναι είτε η διεύθυνση πολλαπλής διανομής solicited-node που αντιστοιχεί στον προορισμό είτε η unicast του αναζητούμενου γείτονα. Το Hope Limit τίθεται 255 ώστε να μην διέρχεται από δρομολογητές.

Διαφήμιση γείτονα (Neighbor Advertisement)

Το μήνυμα διαφήμισης γείτονα NA στέλνεται σε απάντηση μηνυμάτων NS είτε χωρίς να ζητηθεί ώστε να διαδοθεί νέα πληροφορία, όπως η αλλαγή της φυσικής διεύθυνσης του κόμβου. Είναι μήνυμα ICMPv6 τύπου 136 με διεύθυνση πηγής αυτή της διεπαφής από όπου πηγάζει. Η δε διεύθυνση προορισμού του είναι η διεύθυνση πηγής του NS είτε η ομαδική διεύθυνση όλοι οι κόμβοι σε αυτή τη ζεύξη **ff02::1**. Το Hope Limit τίθεται 255 ώστε να μην διέρχεται από δρομολογητές.

Αυτόματη ρύθμιση διευθύνσεων (Automatic Address Configuration)

Ένας κόμβος μπορεί να ρυθμίσει αυτόματα (χωρίς παρέμβαση του διαχειριστή) τη διεύθυνση IPv6 που χρησιμοποιεί για επικοινωνία στο δίκτυο. Ο κόμβος μπορεί να χρησιμοποιεί ταυτόχρονα και τους δύο διαθέσιμους μηχανισμούς ρύθμισης διευθύνσεων stateless και stateful. Η συγκεκριμένη μέθοδος μπορεί να ρυθμιστεί με χρήση σημαιών (flags) στα μηνύματα RA. Φυσικά είναι δυνατό ο κόμβος να ρυθμιστεί και χειροκίνητα.

Stateless Address Autoconfiguration (SLAAC)

Η stateless διαδικασία της αυτόματης ρύθμισης που ορίζεται στο RFC 4862 περιλαμβάνει την παραγωγή τοπικών στη ζεύξη (link-local) και παγκοσμίων (global) διευθύνσεων καθώς και τη διαδικασία ανίχνευσης ταυτόσημων διευθύνσεων ώστε να εξασφαλισθεί η μοναδικότητά τους σε μια ζεύξη. Οι κόμβοι ορίζουν αυτόματα διευθύνσεις για κάθε διεπαφή τους επιθέτοντας την ταυτότητα διεπαφής, μήκους 64 bit, στο πρόθεμα. Υπάρχουν διάφοροι τρόποι με τους οποίους ο κόμβος μπορεί να δημιουργήσει την ταυτότητα διεπαφής (π.χ. από τη διεύθυνση MAC ως τροποποιημένη EUI-64, με τυχαίο τρόπο ή κρυπτογραφικά). Οι τοπικές στη ζεύξη διευθύνσεις σχηματίζονται με το πρόθεμα **fe80::/64**. Οι παγκόσμιες διευθύνσεις σχηματίζονται χρησιμοποιώντας τα προθέματα στο Prefix Information εντός του μηνύματος RA εάν υπάρχει η σημαία ‘A’ (autonomous). Εάν το μήνυμα RA περιέχει τη σημαία ‘O’ (other configuration), τότε ο κόμβος μετά την αυτόματη ρύθμιση της διεύθυνσής του, θα ζητήσει επιπλέον πληροφορία με stateless DHCPv6. Η μέθοδος αποκαλείται stateless γιατί ο εξυπηρετητής DHCPv6 δεν διαχειρίζεται τις αναθέσεις διευθύνσεων και τη διάρκειά τους, παρέχει μόνο όποια επιπλέον πληροφορία ζητηθεί, όπως π.χ. τους εξυπηρετητές DNS.

Stateful Address Configuration και DHCPv6

Κατά την αυτόματη ρύθμιση διευθύνσεων οι προαιρετικές πληροφορίες του μηνύματος RA επιτρέπουν στους κόμβους, ιδιαίτερα, στους κινητούς, να δικτυωθούν και επικοινωνήσουν χωρίς καμία παρέμβαση από τον χρήστη. Σε πιο σταθερά όμως περιβάλλοντα, όπως τα εταιρικά, πιθανόν αυτή η λειτουργία να μην είναι επιθυμητή. Επίσης, συχνά θέλουμε ένας κόμβος να έχει διεύθυνση ανεξάρτητη από τη φυσική του διεύθυνση (όπως αυτή προκύπτει με την μέθοδο SLAAC σε δίκτυα Ethernet). Σε αυτές τις περιπτώσεις οι διευθύνσεις μπορεί να παρασχεθούν μέσω DHCPv6. Παρότι η αποθήκευση κατάστασης στη 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. Σε αυτό μπορεί να προστεθεί και η ανάγκη για εγγραφές PTR στη ρύθμιση του DNS για αντίστροφη επίλυση.

Η ρύθμιση με DHCPv6 συμβαίνει εάν το μήνυμα RA έχει τη σημαία ‘M’ (Managed address configuration). Η διαδικασία δεν είναι διαφορετική από αυτήν του DHCP για το IPv4. Ο εξυπηρετητής DHCPv6 αποδίδει τόσο τη διεύθυνση IPv6 όσο και τις άλλες απαραίτητες πληροφορίες για τη δικτύωση του κόμβου. Το DHCPv6 όμως έχει διαφορετικούς τύπους μηνυμάτων και χρησιμοποιεί ταυτότητες DUID (DHCP Unique Identifier) εκεί που το DHCPv4 χρησιμοποιεί διευθύνσεις MAC. Να σημειωθεί ότι και στους δύο τρόπους, stateless και stateful, ο εξυπηρετητής DHCPv6 δεν παρέχει πληροφορία για τον προκαθορισμένο δρομολογητή όπως στην περίπτωση του DHCPv4. Αυτός προκύπτει από τα μηνύματα RA.

Ανίχνευση ταυτόσημων διευθύνσεων (Duplicate Address Detection – DAD)

Από την στιγμή που ένας κόμβος έχει ρυθμίσει μια διεύθυνση πρέπει να προχωρήσει στη διαδικασία DAD για να αποτραπεί η χρήση ταυτόσημων διευθύνσεων στο τοπικό υποδίκτυο. Αυτό γίνεται ανεξάρτητα του τρόπου σχηματισμού της διεύθυνσης stateless, stateful ή χειροκίνητου. Ο κόμβος δεν επιτρέπεται να χρησιμοποιήσει μια διεύθυνση εάν δεν ολοκληρωθεί η διαδικασία DAD επιτυχώς. Μέχρι να ολοκληρωθεί επιτυχώς η διαδικασία DAD, η διεύθυνση βρίσκεται σε δοκιμαστική (tentative) κατάσταση που σημαίνει ότι μπορεί να χρησιμοποιηθεί μόνο για λειτουργίες αναζήτησης γείτονα. Με την επιτυχή ολοκλήρωση της διαδικασίας DAD η διεύθυνση μεταπίπτει στην προτιμώμενη κατάσταση (preferred) και μπορεί να χρησιμοποιηθεί μέχρις ότου αυτή λήξει.

Στη διαδικασία DAD, ο κόμβος στέλνει ένα μήνυμα NS με τη δικιά του διεύθυνση στο πεδίο target address. Ως διεύθυνση πηγής θέτει την ακαθόριστη διεύθυνση **::0** και ως διεύθυνση προορισμού τη διεύθυνση πολλαπλής διανομής solicited node που προκύπτει από την target address. Εάν υπάρχει και άλλος κόμβος που χρησιμοποιεί τη διεύθυνση στο πεδίο target address δύο ενδεχόμενα μπορεί να συμβούν:

- Ο κόμβος που θα λάβει το μήνυμα NS να απαντήσει με μήνυμα NA στη διεύθυνση πολλαπλής διανομής all-nodes **ff02::1** εκθέτοντας με αυτό τον τρόπο την ταυτόσημη διεύθυνση στον αιτούντα,
- Ο κόμβος να πάρει ένα μήνυμα NS με τη δικιά του διεύθυνση στο πεδίο target address από ένα άλλο κόμβο ο οποίος προσπαθεί να ολοκληρώσει τη 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 του διεύθυνση ως μοναδική εάν δεν ληφθούν ενδείξεις ταυτόσημης διεύθυνσης μετά από έλευση χρόνου ίσου με την Retrans Timer (που δηλώνουν τα μηνύματα RA) αφότου έστειλε αριθμό Dup_Addr_Detect_Transmits πακέτων NS. Οι τυπικές τιμές των παραπάνω μεταβλητών είναι 1.000 msec και 1, αντίστοιχα. Κατά συνέπεια σε τυπικές συνθήκες χρειάζεται περίπου 1 sec συν την επιπλέον καθυστέρηση για τη μετάδοση πακέτων και τους υπολογισμούς. Επιπλέον, ένας κόμβος πρέπει να καθυστερήσει την αποστολή NS για ένα τυχαίο χρονικό διάστημα μεταξύ 0 και Max_Rtr_Solicitation_Delay 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 κόμβος 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 αναζήτησης δρομολογητή. Ο κόμβος ξεκινά τη διαδικασία DAD με την link-local διεύθυνση χωρίς να περιμένει απάντηση στο αίτημα RS που ίσως αργήσει.

Προσδιορισμός επόμενου βήματος (Next-hope determination)

Το επόμενο βήμα για μια unicast διεύθυνση προσδιορίζεται σε στάδια. Πρώτα, ο αποστολέας αναζητεί το μεγαλύτερο ταίριασμα σε μια λίστα on-link προθεμάτων δικτύου. Εάν βρεθεί, ο προορισμός βρίσκεται στην ίδια ζεύξη και διεύθυνση IPv6 του επόμενου βήματος είναι η διεύθυνση προορισμού. Εάν ο προορισμός είναι off-link, ο αποστολέας διαλέγει τον καλύτερο δρομολογητή από τη λίστα προκαθορισμένων δρομολογητών. Το αποτέλεσμα αποθηκεύεται στον πίνακα προορισμών (Destination Cache). Αφού βρεθεί το επόμενο βήμα, αναζητείται η φυσική του διεύθυνση στον πίνακα γειτόνων (Neighbor Cache).

Επίλυση διευθύνσεων

Ο πίνακας γειτόνων (Neighbor Cache) περιέχει αντιστοιχίσεις διευθύνσεων IPv6 σε φυσικές διευθύνσεις και πληροφορία κατάστασης. Εάν δεν υπάρχει εγγραφή για τον ζητούμενο γείτονα, δημιουργείται μία ως *Incomplete*, και ο αποστολέας αποθηκεύει προσωρινά τα πακέτα. Για να μάθει τη φυσική διεύθυνση του προορισμού στέλνει μήνυμα NS στην ομαδική διεύθυνση solicited node που προκύπτει από την IPv6 διεύθυνση προορισμού. Το μήνυμα περιλαμβάνει και τη δική του φυσική διεύθυνση στην οποία ο γείτονας απαντά με μήνυμα NA. Όταν λάβει απάντηση, ενημερώνει τον πίνακα γειτόνων, σημαδεύει τη φυσική διεύθυνση ως *Reachable* και μεταδίδει τα αποθηκευμένα πακέτα.

Ανίχνευση Έλλειψης Επικοινωνίας (Neighbor Unreachability Detection)

Μια εγγραφή με το χαρακτηριστικό Reachable σημαίνει ότι ο κόμβος είναι προσβάσιμος. Στο IPv6 ένας κόμβος 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. Εάν δεν επιβεβαιωθεί η προσβασιμότητα κάποιας εγγραφής του πίνακα γειτόνων για περισσότερο από 30 sec η κατάσταση μεταπίπτει σε *Stale*. Σε μια σύνδεση υπάρχει πρόοδος εάν λαμβάνονται πακέτα από τον προορισμό σε απάντηση αυτών που στέλνονται. Σε συνδέσεις TCP για κάθε τεμάχιο που στέλνεται, ο προορισμός στέλνει επιβεβαίωση. Άρα ο on-link προορισμός ή ο δρομολογητής (επόμενου βήματος για off-link προορισμούς) είναι προσβάσιμος. Σε πακέτα UDP δεν αναμένονται επιβεβαιώσεις και ο κόμβος επιβεβαιώνει την προσβασιμότητα των γειτόνων στέλνοντας μηνύματα NS και αναμένοντας απαντήσεις NA. Αυτό γίνεται σε συνδυασμό με την ύπαρξη κίνησης. Εάν δεν υπάρχει κίνηση, δεν στέλνονται NS.

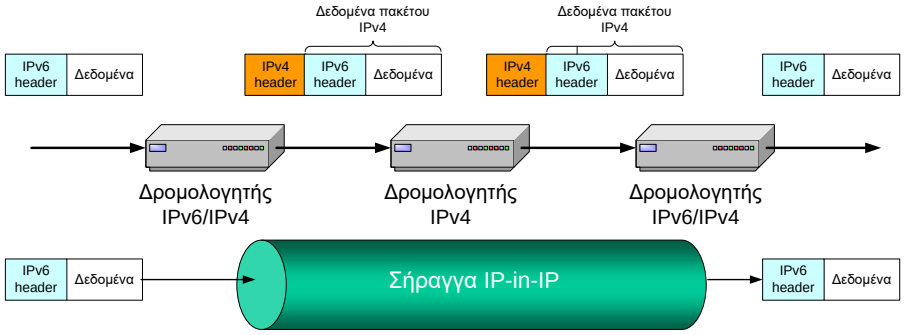
Μηχανισμοί Μετάβασης

Κατά τη 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, υπολογιστές) στο νέο πρωτόκολλο ήταν εντελώς διαφορετική. Για τους υπολογιστές 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 τη 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 (6to4, 6rd, 6in4, teredo, …) καθώς και τεχνικές μετάφρασης διευθύνσεων IPv4/IPv6 (SIIT, NAT64/DNS64, 464XLAT).

Μηχανισμός Ενθυλάκωσης 6in4

Ο μηχανισμός 6in4, RFC 2473, είναι ένα πρωτόκολλο ενθυλάκωσης πακέτων IPv6 σε ζεύξεις IPv4. Το πακέτο 6in4 περιλαμβάνει το αρχικό πακέτο IPv6 και μια επικεφαλίδα IPv4 μήκους 20 byte. Τα άκρα της σήραγγας πρέπει να ορισθούν χειροκίνητα και πρέπει να διαθέτουν δημόσιες διευθύνσεις IPv4. Εξ αιτίας αυτού δεν είναι ιδιαίτερα κατάλληλος για τυπικά οικιακά περιβάλλοντα που βρίσκονται σε νησίδες NAT.



Μηχανισμός Ενθυλάκωσης 6to4

Ο μηχανισμός 6to4, RFC 3056, χρησιμοποιεί την ενθυλάκωση 6in4 για την επικοινωνία μεταξύ νησίδων IPv6 μέσω του διαδικτύου IPv4 χωρίς την ανάγκη ρητής εγκατάστασης σηράγγων από τους κόμβους IPv6. Για τον σκοπό αυτό χρησιμοποιούνται ενδιάμεσοι (relays) ή δρομολογητές 6to4 και διευθύνσεις 6to4 που δημιουργούνται από το πρόθεμα **2002::/16** προσθέτοντας τα 32 bit της διεύθυνσης IPv4 (π.χ. η διεύθυνση 192.0.2.4 αντιστοιχεί στο 6to4 πρόθεμα 2002:c000:0204::/48) καθώς και 16 bit για τον ορισμό υποδικτύων IPv6. Με αυτόν τον τρόπο δημιουργείται ένας παράλληλο δίκτυο όπου πακέτα IPv6 με προορισμό διεύθυνση 6to4 ενθυλακώνονται σε πακέτα IPv4 με τη διεύθυνση προορισμού IPv4 να προκύπτει από τη διεύθυνση 6to4, ενώ από τα πακέτα 6to4 που φτάνουν σε διεπαφές IPv4 εξάγεται το περιεχόμενο πακέτο IPv6. Έτσι κόμβοι με διευθύνσεις 6to4 μπορούν να επικοινωνήσουν με κόμβους 6to4 μέσω των ενδιαμέσων. Για να επικοινωνήσουν με άλλους κόμβους IPv6 ο ενδιάμεσος πρέπει να δρομολογεί μεταξύ κανονικών διευθύνσεων IPv6 και διευθύνσεων 6to4.

Μηχανισμός Ενθυλάκωσης Teredo

Μεταξύ των μηχανισμών μετάβασης, ο Teredo, RFC 4380, είναι μια ενδιαφέρουσα λύση, ικανή να διασχίζει τις νησίδες NAT που συναντιούνται στα οικιακά περιβάλλοντα. Εδώ ο υπολογιστής πελάτης ενθυλακώνει τα πακέτα IPv6 σε πακέτα IPv4 ως μηνύματα πρωτοκόλλου UDP. Η επιλογή του UDP έγινε για να μην παρουσιάζονται προβλήματα με το NAT. Ο μηχανισμός teredo υποστηρίζεται σε σύγχρονα λειτουργικά συστήματα ως εικονική διεπαφή (pseudo interface) μέσω της οποίας διέρχονται ενθυλακωμένα πακέτα IPv6. Χρησιμοποιεί διευθύνσεις από το πρόθεμα **2001::/32** που σχηματίζονται ως εξής:

Bit 0 έως 31	το Teredo prefix (2001:0000::/32)
Bit 32 έως 63	η IPv4 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($3ffffdd2_h$)

Ο πελάτης επικοινωνεί με τον εξυπηρετητή Teredo στέλνοντας ενθυλακωμένα σε UDP μηνύματα ICMPv6 RS και λαμβάνοντας ICMPv6 RA ώστε να διατηρείται η αντιστοίχιση του πίνακα NAT. Ο εξυπηρετητής Teredo δεν χρειάζεται να προωθεί κίνηση πλην μηνυμάτων ICMPv6 και Teredo bubbles (πακέτα IPv6 μηδενικού περιεχομένου για τη δημιουργία αντιστοιχίσεων στους πίνακες NAT). Η κίνηση IPv6 προωθείται από αναμεταδότες Teredo relays. Για την ανεύρεσή τους ο πελάτης στέλνει μέσω του εξυπηρετητή Teredo ένα ICMPv6 echo request προς τον προορισμό. Ο προορισμός απαντά με ICMPv6 echo reply που δρομολογείται προς τον πλησιέστερο αναμεταδότη Teredo, που με τη σειρά του το προωθεί προς τον πελάτη.

Μηχανισμός μετάφρασης SIIT

Το Stateless IP/ICMP Translation (SIIT), όπως ορίσθηκε στο RFC 2765, είναι κανόνες μετάφρασης μεταξύ επικεφαλίδων πακέτων IPv4 και IPv6 (περιλαμβανομένων των πακέτων ICMP/ICMPv6). Ο μεταφραστής για εισερχόμενα πακέτα IPv4 αφαιρεί την επικεφαλίδα τους και την αντικαθιστά με επικεφαλίδα IPv6. Πλην των πακέτων ICMP, τα δεδομένα και οι επικεφαλίδες στρώματος μεταφοράς δεν τροποποιούνται. Το αντίστροφο συμβαίνει για εισερχόμενα πακέτα IPv6. Κεντρικό σημείο του μηχανισμού είναι η χρήση των αποκαλούμενων αντιστοιχημένων-IPv4 (IPv4-mapped) διευθύνσεων IPv6 για την αναπαράσταση κόμβων IPv4 εντός ενός δικτύου IPv6. Για τις IPv4-mapped διευθύνσεις IPv6 έχει διατεθεί το πρόθεμα **::ffff:0:0/96**. Στην εν λόγω μετάφραση η διεύθυνση IPv4 a.b.c.d αντιστοιχεί στη διεύθυνση IPv6 ::ffff:a.b.c.d. Οι διευθύνσεις αυτές δεν είναι δρομολογήσιμες στο δημόσιο δίκτυο, επιτρέπουν όμως, στην περίπτωση κόμβων διπλής στοίβας, την παράδοση πακέτων IPv4 σε εφαρμογές IPv6.

Αλγόριθμος μετάφρασης IP/ICMP

Το IP/ICMP Translation Algorithm αποτελεί γενίκευση του SIIT. Ορίσθηκε αρχικά στο RFC 6145 που στη συνέχεια αντικαταστάθηκε από το RFC 7915. Στη μετάφραση IP/ICMP υποτίθεται ένας κόμβος με διεύθυνση IPv4, αλλά χωρίς διεύθυνση IPv6, που επικοινωνεί με ένα κόμβο με διεύθυνση IPv6, αλλά χωρίς διεύθυνση IPv4, είτε δύο συστήματα που δεν διαθέτουν συμπαγή (contiguous) όσον αφορά τη δρομολόγηση συνδεσιμότητα.

Η μετάφραση των διευθύνσεων IPv4/IPv6 ορίζεται αλλού, στο RFC 6052, και μπορεί να είναι stateless ή stateful. Εκεί περιγράφεται το μορφότυπο ενσωματωμένων-IPv4 (embedded-IPv4) διευθύνσεων, δηλαδή, ένας γενικός τρόπος χρήσης διευθύνσεων IPv6 για την αναπαράσταση διευθύνσεων IPv4 σε ένα δίκτυο IPv6.

Στην stateless περίπτωση, μια ομάδα διευθύνσεων IPv6, οι αποκαλούμενες μετατρεμμένες-IPv4 (IPv4-converted) διευθύνσεις IPv6 χρησιμεύουν για την αναπαράσταση των κόμβων IPv4 στο δίκτυο IPv6. Οι δε κόμβοι IPv6 έχουν μία μεταφράσιμη-IPv4 (IPv4-translatable) διεύθυνση που αντιστοιχεί αλγοριθμικά σε κάποιο υποσύνολο των διευθύνσεων IPv4.

Στην stateful περίπτωση και πάλι μια συγκεκριμένη ομάδα μετατρεμμένων-IPv4 διευθύνσεων IPv6 διατίθεται για την αναπαράσταση των κόμβων IPv4. Όμως οι κόμβοι IPv6 μπορούν να έχουν οποιαδήποτε διεύθυνση IPv6 εκτός αυτής της ομάδας. Η αντιστοιχία διευθύνσεων IPv6 και IPv4 τηρείται σε πίνακες όπου εμπλέκονται παράμετροι στρώματος μεταφοράς (όπως στο stateful NAT).

Μηχανισμός μετάφρασης NAT64/DNS64

Το stateless NAT64 είναι εφαρμογή της μετάφρασης IP/ICMP κατάλληλη μόνο για την περίπτωση που η πύλη NAT64 χρησιμοποιείται εμπρός από εξυπηρετητές IPv4, ώστε αυτοί να είναι προσβάσιμοι από πελάτες IPv6. Ορίζονται στατικά α) μετατρεμμένες-IPv4 διευθύνσεις IPv6 για την αναπαράσταση των κόμβων IPv4 εντός του δικτύου IPv6 και β) μεταφράσιμες-IPv4 διευθύνσεις IPv6 που αντιστοιχούν στους κόμβους IPv6 ένα υποσύνολο διευθύνσεων IPv4. Η αντιστοίχιση γίνεται σύμφωνα με τους κανόνες του RFC 6052. Για τη λειτουργία αυτή διατίθεται είτε το πασίγνωστο πρόθεμα **64:ff9b::/96** (WKP – Well-Known Prefix) είτε ένα συγκεκριμένο δημόσιο /32, /40, /48, /64 ή /96 πρόθεμα υποδικτύου IPv6 (NSP – Network Specific Prefix).

Στο stateless NAT64 ο κόμβος IPv6 (H6) για την επικοινωνία του με τον κόμβο IPv4 (H4) χρησιμοποιεί ως διεύθυνση πηγής την IPv4-translatable και ως προορισμό την IPv4-converted. Ο μηχανισμός μετάφρασης εξάγει αλγοριθμικά από τα πακέτα του H6 τις αντίστοιχες διευθύνσεις πηγής και προορισμού IPv4, μεταφράζει τις επικεφαλίδες και προωθεί τα μεταφρασμένα πακέτα στον H4. Ο H4 απαντά στη διεύθυνση IPv4 που αντιστοιχεί στην IPv4-translatable του H6, ο μηχανισμός μεταφράζει τις επικεφαλίδες και προωθεί στον H6 Η αντιστοίχιση αυτή είναι 1:1, δηλαδή, για κάθε κόμβο H6 που θέλει να επικοινωνήσει με κόμβο H4, πρέπει να διατεθεί μία διεύθυνση IPv4 στο μηχανισμό μετάφρασης, όπως ακριβώς και στην περίπτωση διπλής στοίβας.

Το stateful NAT64 (RFC 6146) είναι μηχανισμός NAT για επικοινωνία που ξεκινά αποκλειστικά από κόμβους IPv6. Με την τεχνική αυτή, υπολογιστές με διεύθυνση IPv6, που δεν διαθέτουν δημόσια διεύθυνση IPv4, μπορούν να επικοινωνήσουν με υπολογιστές που διαθέτουν μόνο διεύθυνση IPv4, χρησιμοποιώντας μονο-εκπομπή (unicast) UDP, TCP και ICMP. Η επικοινωνία γίνεται μέσω πύλης NAT64 που διατηρεί πίνακες με την αντιστοιχία διευθύνσεων IPv4/IPv6 και συνόδων UDP, TCP, ICMP που έχουν εγκατασταθεί μέσω αυτής. Για την αναπαράσταση των κόμβων IPv4 εντός ενός δικτύου IPv6 χρησιμοποιείται είτε το WKP είτε ένα συγκεκριμένο NSP.

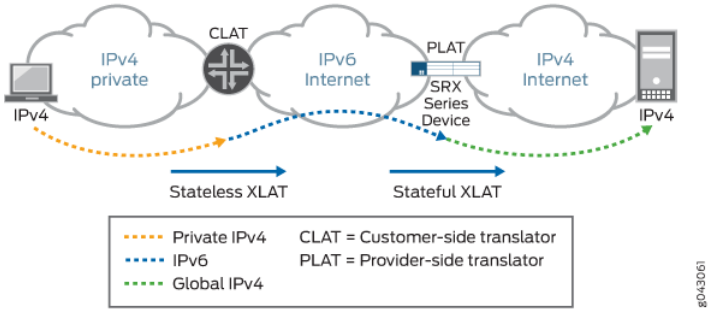
Στο stateful NAT64 ο κόμβος IPv6 (H6) για την επικοινωνία του με τον κόμβο IPv4 (H4) χρησιμοποιεί ως διεύθυνση πηγής την IPv6 διεύθυνσή του και ως προορισμό την IPv4-converted. Ο μηχανισμός μετάφρασης αντιστοιχεί δυναμικά στον H6 μία από τις διαθέσιμες σε αυτόν διευθύνσεις IPv4, εξάγει με αλγοριθμικό τρόπο την IPv4 διεύθυνση προορισμού, μεταφράζει τις επικεφαλίδες, προωθεί τα μεταφρασμένα πακέτα στον H4 διατηρώντας τη θύρα προορισμού TCP ή UDP και καταγράφει την αντιστοίχιση διευθύνσεων και θυρών σε πίνακα. Ο H4 απαντά στη διεύθυνση IPv4 πηγής, ο μηχανισμός μεταφράζει τις επικεφαλίδες σύμφωνα με την πληροφορία που διατηρεί στον πίνακα κατάστασης και προωθεί το πακέτο στον H6. Στο stateful NAT64 η αντιστοίχιση είναι 1:N, πολλαπλοί κόμβοι IPv6 μπορούν να έχουν πρόσβαση σε απομακρυσμένους κόμβους IPv4 μέσω μίας ή περισσότερων διευθύνσεων IPv4.

Για την επικοινωνία με τον εξυπηρετητή IPv4, τυπικά ο πελάτης IPv6 θα αναζητήσει μέσω DNS τη διεύθυνση IPv6. Όμως ο εξυπηρετητής DNS δεν αναμένεται να διαθέτει εγγραφή τύπου AAAA για ένα κόμβο IPv4. Το DNS64 (RFC 6147), που χρησιμοποιείται σε συνδυασμό με το stateful NAT64, περιγράφει έναν εξυπηρετητή DNS ο οποίος, όταν ερωτάται για εγγραφές AAAA, αλλά βρίσκει μόνο εγγραφές A, συνθέτει απαντήσεις AAAA από αυτές. Το πρώτο μέρος της συνθετικής διεύθυνσης IPv6 αντιστοιχεί σε ένα μεταφραστή IPv6/IPv4 (τυπικά την πύλη NAT64) και το δεύτερο μέρος είναι η ενσωματωμένη-IPv4 διεύθυνση.

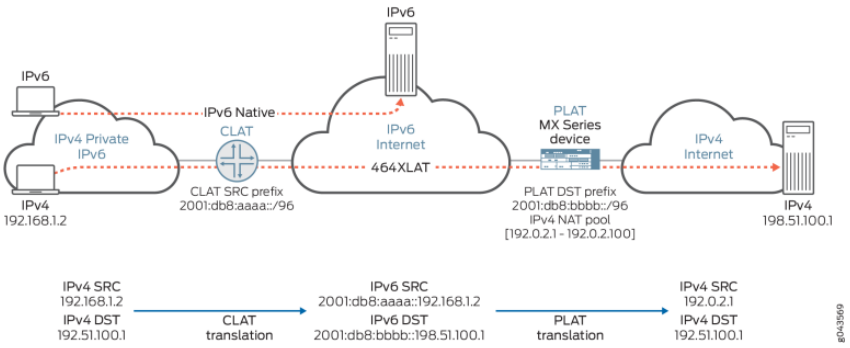
Με NAT64 δεν είναι δυνατή η πρόσβαση σε οποιαδήποτε υπηρεσία. Πρωτόκολλα ή εφαρμογές που ενσωματώνουν στα μηνύματά τους διευθύνσεις IPv4, όπως SIP και SDP, FTP, Skype, Webex MSN, κλπ αποκλείονται. Για τέτοιες περιπτώσεις απαιτούνται είτε πληρεξούσιοι διπλής στοίβας (dual-stack proxies) είτε, για τα SIP, FTP, πύλες ALG (Application-Level Gateways). Όμως για συνδέσεις μόνο πάνω από IPv6 μπορεί να χρησιμοποιηθεί το 464XLAT ένας υβριδικός μηχανισμός NAT64 που συνδυάζει τις δύο (stateless και stateful) προσεγγίσεις.

Μηχανισμός μετάφρασης 464XLAT

Ο μηχανισμός 464XLAT, RFC 6877, χρησιμοποιείται από πελάτες με IPv4 ιδιωτικές διευθύνσεις για πρόσβαση μέσω δικτύων IPv6 σε υπηρεσίες IPv4 (όπως το Skype). Το 464XLAT υποστηρίζει μόνο το μοντέλο πελάτη-εξυπηρετητή IPv4, όχι ισότιμη επικοινωνία IPv4 ή εισερχόμενες συνδέσεις IPv4. Ο πελάτης χρησιμοποιεί μετάφραση IP/ICMP (stateless) για να μετατρέψει πακέτα IPv4 σε IPv6 και να τα στείλει μέσω δικτύου IPv6 σε πύλη NAT64 (stateful), η οποία θα τα μεταφράσει πίσω σε IPv4 και θα τα στείλει στον εξυπηρετητή IPv4, όπως στο σχήμα. Λόγω του NAT64 οι συνδέσεις προς τον εξυπηρετητή περιορίζονται στα πρωτόκολλα UDP, TCP και ICMP.



Ο μηχανισμός 464XLAT είναι ιδιαίτερα χρήσιμος σε παρόχους κινητής τηλεφωνίας. Επιτρέπει την ανάπτυξη υποδομής αποκλειστικά δικτύου IPv6 και την παροχή υπηρεσιών IPv4 στις κινητές συσκευές. Ο μεταφραστής στην πλευρά του πελάτη CLAT (Customer-side transLATor) τυπικά υλοποιείται ως ειδικό λογισμικό (στον πελάτη). Ο μεταφραστής NAT64 στην πλευρά του παρόχου PLAT (Provider-side transLATor) είναι δικτυακή συσκευή και πρέπει να έχει πρόσβαση τόσο στον εξυπηρετητή όσο και στον πελάτη (μέσω του CLAT).



Προετοιμασία στο σπίτι

Οδηγίες εγκατάστασης δυναμικών πρωτοκόλλων δρομολόγησης RIPng και OSPFv3 για το IPv6

Στην άσκηση αυτή θα χρησιμοποιήσετε ως PC και δρομολογητή το FRR. Ως άσκηση για το σπίτι, θα ενεργοποιήσετε στο FreeBSD 13.2 με FRR, που δημιουργήσατε στην Εργαστηριακή Άσκηση 9, τη δρομολόγηση IPv6 καθώς και τα πρωτόκολλα δρομολόγησης RIPng και OSPFv3. Να έχετε μαζί σας αυτήν την εικόνα του FreeBSD, ώστε να μην χρειαστεί να επαναλάβετε την εγκατάσταση του FRR στο εργαστήριο.

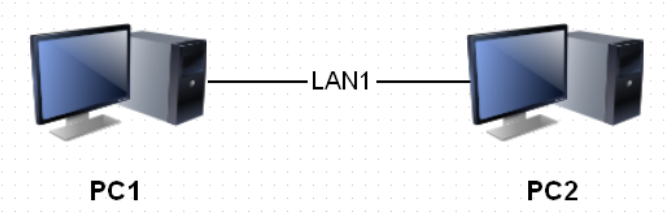
1. Κλείστε την υπηρεσία frr με “service frr stop”.
2. Στο αρχείο παραμετροποίησης /etc/rc.conf προσθέστε το ripngd και ospf6d τη γραμμή frr_daemons=“zebra staticd ripd ospfd bgpd”, ώστε να γίνει frr_daemons=“zebra staticd ripd ripngd ospfd ospf6d bgpd”.

3. Ξεκινήστε την υπηρεσία frr ξανά με “service frr start”.
4. Κλείστε το εικονικό μηχάνημα με την εντολή poweroff και από τη διαδρομή *File→Export Appliance…* στο VirtualBox δημιουργήστε ένα αρχείο frr.ova.
5. Αποθηκεύστε το αρχείο frr.ova για να μπορείτε να δημιουργείτε στη συνέχεια εικονικά μηχανήματα και δρομολογητές.

Στο FRR η παραμετροποίηση των πρωτοκόλλων RIPng και OSPF3 γίνεται μέσω του ενιαίου περιβάλλοντος που παρέχει το vtysh. Στο Quagga ο πιο απλός τρόπος είναι μέσω του cli (ισοδύναμο με το vtysh). Εναλλακτικά, μπορείτε να συνδεθείτε με telnet (στη θύρα 2603/tcp για το RIPng και θύρα 2606/tcp για το OSPFv3), αφού πρώτα ορίσετε συνθηματικό πρόσβασης.

Άσκηση 1: Εισαγωγή στο IPv6

Κατασκευάστε στο VirtualBox το παρακάτω δίκτυο όπου ως PC χρησιμοποιήστε τα εικονικά μηχανήματα FreeBSD 13.2 με το FRR που κατασκευάσατε (frr.ova).



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 Στα PC η λειτουργία αυτόματης απόδοσης διευθύνσεων IPv6 είναι απενεργοποιημένη και θα πρέπει να την ενεργοποιήσετε. Με τη βοήθεια της κατάλληλης εντολής προσθέσετε στο αρχείο /etc/rc.conf τη γραμμή ifconfig_em0_ipv6=“inet6 accept_rtadv” για ενεργοποίηση της αποδοχής μηνυμάτων Router Advertisement στη διεπαφή em0.

1.2 Μετά επανεκκινήσετε την υπηρεσία δικτύου netif.

1.3 Ποια διεύθυνση IPv6 έχει αποδοθεί στη διεπαφή em0 του PC1;

1.4 Ποια διεύθυνση IPv6 έχει αποδοθεί στη διεπαφή em0 του PC2;

1.5 Τι είδους είναι αυτές οι διευθύνσεις IPv6; Πώς παράγονται από τη διεύθυνση MAC της κάρτας δικτύου;

1.6 Σε κάποιο από τα δύο PC εμφανίστε τον πίνακα δρομολόγησης μόνο για το IPv6. Πόσες εγγραφές υπάρχουν;

1.7 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;

1.8 Ποιες εγγραφές σχετικές με το πρόθεμα δικτύου fe80::/64 περιέχει ο πίνακας δρομολόγησης και ποιες οι αντίστοιχες διεπαφές εξόδου;

1.9 Από το PC1 κάντε ping6 στη διεύθυνση ::1. Ποιο PC απαντά;

1.10 Από το PC1 κάντε ping6 στη link-local διεύθυνση αυτού; Τι πρέπει να προσθέσετε στη διεύθυνση για να επιτύχει η εκτέλεση της εντολής;

1.11 Από το PC1 κάντε ping στην link-local διεύθυνση του PC2. Εάν αποτυγχάνει τι πρέπει να προσθέσετε;

1.12 Εκτελέστε την εντολή “*ping6 ff01::1%em0*”. Ποιο PC απαντά;

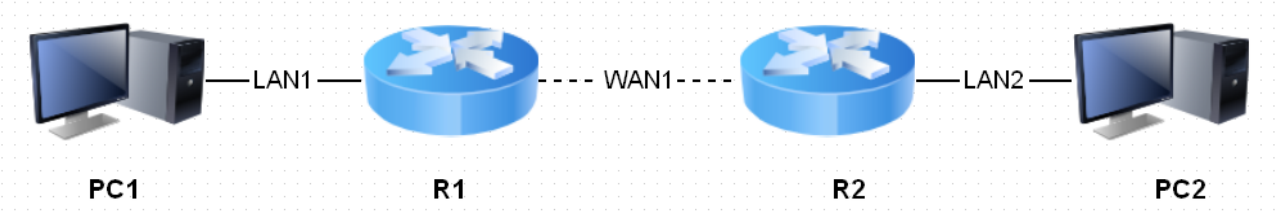
1.13 Εκτελέστε την εντολή “*ping6 ff02::1%em0*”. Τι παρατηρείτε;

1.14 Ορίστε στη διεπαφή του PC1 στο LAN1 τη στατική διεύθυνση fd00:1::2/64. *[Δείτε σελίδες man για τη σύνταξη της εντολής ifconfig.]*
1.15 Ορίστε στη διεπαφή του PC2 στο LAN1 τη στατική διεύθυνση fd00:1::3/64.
1.16 Τι είδους διευθύνσεις IPv6 είναι οι προηγούμενες; Ποιες είναι οι ανάλογες με αυτές IPv4 διευθύνσεις;
1.17 Πόσες διευθύνσεις υπάρχουν στις διεπαφές em0 των PC;
1.18 Εμφανίστε ξανά τον πίνακα δρομολόγησης μόνο για το IPv6. Πόσες νέες εγγραφές προστέθηκαν;
1.19 Τι πρέπει να προσθέσετε και σε ποια αρχεία για να μπορείτε να χρησιμοποιείτε τα ονόματα των μηχανημάτων αντί των IPv6 διευθύνσεών τους στις διάφορες δικτυακές εντολές;
1.20 Μετά την αλλαγή αυτή μπορείτε να κάνετε ping από το PC1 στο PC2 χρησιμοποιώντας το όνομά του;
1.21 Στο PC1 εμφανίστε τον πίνακα ARP. Πόσες εγγραφές βλέπετε;
1.22 Εμφανίστε τη βοήθεια της εντολής *ndp* και μελετήστε τη χρήση της.
1.23 Ποια είναι η σύνταξη της παραπάνω εντολής για να εμφανίσετε τον πίνακα γειτόνων (neighbor cache) του PC1;
1.24 Πόσες εγγραφές βλέπετε και σε ποια κατάσταση βρίσκονται;*[Υποδ. Δείτε σελίδα man για ndp για τις καταστάσεις των εγγραφών και τις συντομογραφίες τους.]*
1.25 Δείτε τη λίστα προθεμάτων IPv6 στο PC1. Υπάρχουν εγγραφές για κάποια προθέματα;
1.26 Καθαρίστε τον πίνακα γειτόνων σε αμφότερα τα PC.
1.27 Στο PC2 ξεκινήστε μια καταγραφή πακέτων σε χωριστό παράθυρο με εμφάνιση λεπτομερειών και απενεργοποιημένη την επίλυση ονομάτων και διευθύνσεων.
1.28 Στο PC1 εκτελέστε την εντολή "*ping6 –c 1 PC2*". Σταματήστε την καταγραφή. Πόσα πακέτα IPv6 βλέπετε;
1.29 Μηνύματα ποιου πρωτοκόλλου μεταφέρουν τα πακέτα IPv6 της καταγραφής και ποια είναι η τιμή του πεδίου Next header της επικεφαλίδας που το προσδιορίζει;
1.30 Σχεδιάστε ένα διάγραμμα που να δείχνει τη σειρά αποστολής και τον τύπο των μηνυμάτων που καταγράψατε προηγουμένως.
1.31 Τι είδους διεύθυνση είναι ο προορισμός του πρώτου πακέτου NS που καταγράψατε και πώς προκύπτει αυτή;
1.32 Τι είδους διεύθυνση είναι ο προορισμός του δεύτερου πακέτου NS που καταγράψατε και πώς προκύπτει;
1.33 Ποια είναι η κατάσταση της εγγραφής για το PC1 στον πίνακα γειτόνων του PC2 και ποια η διάρκεια ζωής της σχετικής εγγραφής;
1.34 Ξεκινήστε ένα ping6 από το PC1 στο PC2 και αφήστε το να τρέχει. Παρατηρήστε διαδοχικά αρκετές φορές για περίπου 1 min την κατάσταση της εγγραφής για το PC1 στον πίνακα γειτόνων του PC2. Ποιες καταστάσεις παρατηρήσατε;
1.35 Ποια είναι η διάρκεια της κατάστασης "(R) Reachable"; Τι συμβαίνει όταν λήξει η διάρκειά της;
1.36 Ποια είναι η διάρκεια της κατάστασης "(S) Stale".
1.37 Σταματήστε το ping και συνεχίστε να παρατηρείτε διαδοχικά αρκετές φορές για περίπου άλλο 1 min την κατάσταση της εγγραφής για το PC1 στον πίνακα γειτόνων του PC2. Ποιες καταστάσεις παρατηρήσατε;

1.38 Ξεκινήστε και πάλι ένα ping6 από το PC1 στο PC2 και αφήστε το να τρέχει. Στο PC2 ξεκινήστε μια καταγραφή πακέτων με απενεργοποιημένη την επίλυση ονομάτων και διευθύνσεων. Παρατηρείτε την παραγωγή άλλων πακέτων πλην των ICMPv6 Echo Request και Echo Reply; Εάν ναι, για ποιο λόγο και κάθε πότε περίπου παράγονται.

Άσκηση 2: SLAAC και Στατική δρομολόγηση IPv6

Κατασκευάστε στο VirtualBox το παρακάτω δίκτυο. Κρατήστε τα PC από την προηγούμενη άσκηση. Ως δρομολογητές θα χρησιμοποιήσετε εικονικά μηχανήματα FreeBSD 13.2 FRR (frr.ova) με δύο διεπαφές όπου θα ενεργοποιήσετε τη λειτουργία δρομολόγησης.



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

2.1 Με τη βοήθεια της κατάλληλης εντολής προσθέστε στο αρχείο εκκίνησης /etc/rc.conf των R1 και R2 την εντολή ipv6_gateway_enable="YES" ώστε να ενεργοποιηθεί η προώθηση πακέτων IPv6 και επανεκκινήστε την υπηρεσία routing.
2.2 Στο PC2 διαγράψτε τη διεύθυνση fd00:1::3/64 και ορίστε στατική διεύθυνση fd00:2::2/64.
2.3 Στον R1 ορίστε μέσω vtysh τη διεύθυνση fd00:1::1/64 για τη διεπαφή του στο LAN1.
2.4 Στον R1 ορίστε μέσω vtysh τη διεύθυνση fd00:3::1/126 για τη διεπαφή του στο WAN1.
2.5 Στον R2 ορίστε μέσω vtysh τη διεύθυνση fd00:2::1/64 για τη διεπαφή του στο LAN2.
2.6 Στον R2 ορίστε μέσω vtysh τη διεύθυνση fd00:3::2/126 για τη διεπαφή του στο WAN1.
2.7 Ορίστε τη σωστή προεπιλεγμένη πύλη στο PC1. *[Υποδ. Δείτε σελίδες man για εντολή route.]*
2.8 Ορίστε τη σωστή προεπιλεγμένη πύλη στο PC2.
2.9 Ενεργοποιήστε μια καταγραφή πακέτων στη διεπαφή του R1 στο LAN1.
2.10 Στο PC1 καθαρίστε τον πίνακα γειτόνων και εκτελέστε την εντολή ping6 στέλνοντας ακριβώς ένα πακέτο προς το PC2; Είναι το ping6 επιτυχές; Αιτιολογήστε.
2.11 Τι είδους μηνύματα παράγονται και ποια είναι η IPv6 διεύθυνση προορισμού καθένα εξ αυτών;
2.12 Στον R1 μέσω vtysh προσθέστε την κατάλληλη στατική εγγραφή για το LAN2.
2.13 Από το PC1 μπορείτε να κάνετε ping στο PC2; Αιτιολογήστε.
2.14 Στον R2 μέσω vtysh προσθέστε την κατάλληλη στατική εγγραφή για το LAN1.
2.15 Μπορείτε τώρα να κάνετε ping από το PC1 στο PC2;
2.16 Στο FRR η λειτουργία διαφήμισης δρομολογητή είναι απενεργοποιημένη για όλες τις διεπαφές. Ενεργοποιήστε την στη διεπαφή em0 του R1. *[Δείτε υπο-εντολή ipv6 για ρυθμίσεις παραμέτρων ανεύρεσης γειτόνων (nd) στη διεπαφή em0.]*
2.17 Στον R1 για τη διεπαφή του στο LAN1 ορίστε ως πρόθεμα δικτύου για τη διαδικασία ανεύρεσης γειτόνων το fd00:1::/64.
2.18 Στον R2 ενεργοποιήστε τη διαφήμιση δρομολογητή για τη διεπαφή στο LAN2.
2.19 Στον R2 για τη διεπαφή του στο LAN2 ορίστε ως πρόθεμα δικτύου για τη διαδικασία ανεύρεσης γειτόνων το fd00:2::/64.
2.20 Στο PC1 διαγράψτε την προκαθορισμένη διαδρομή.

2.21 Ξεκινήστε μια καταγραφή πακέτων ICMPv6 στον R1 στη διεπαφή του στο LAN1, χωρίς επίλυση ονομάτων και εμφανίζοντας τις επικεφαλίδες Ethernet.
2.22 Επανεκκινήστε την υπηρεσία δικτύου στο PC1. *[Υποδ. /etc/rc.d/netif]*
2.23 Ποια μηνύματα ανταλλάσσονται κατά τις διαδικασίες αυτόματης απόδοσης διεύθυνσης (SLAAC) και ανίχνευσης ταυτόσημων διευθύνσεων (DAD);
2.24 Για ποιο σκοπό παράγει μήνυμα NS το PC1;
2.25 Ποια διεύθυνση πηγής χρησιμοποιεί στο μήνυμα NS και γιατί;.
2.26 Ποια διεύθυνση πηγής χρησιμοποιεί το PC1 στο μήνυμα RS;
2.27 Ποιες είναι οι διευθύνσεις IPv6 προορισμού των μηνυμάτων NS, RS και RA που στάλθηκαν; Αιτιολογήστε.
2.28 Ποιες είναι οι διευθύνσεις MAC προορισμού των πλαισίων Ethernet που τα μεταφέρουν και πως προκύπτουν αυτές;
2.29 Δείτε πάλι τη λίστα προθεμάτων στο PC1. Ποιες σημαίες σχετικές με τον μηχανισμό αυτόματης απόδοσης διευθύνσεων (SLAAC) δηλώνονται για το πρόθεμα fd00:1::/64; *[Υποδ. Δείτε χρήση σημαιών L,A,O]*.
2.30 Ποιες διευθύνσεις έχει λάβει το PC1 αυτόματα μέσω του SLAAC;
2.31 Δείτε τον πίνακα δρομολόγησης για IPv6 στο PC1. Υπάρχει προκαθορισμένη διαδρομή; Εάν ναι, πώς προέκυψε η προκαθορισμένη πύλη;
2.32 Ποιες από τις διευθύνσεις μπορείτε να χρησιμοποιήσετε για να κάνετε ping στο PC1 από το PC2 και ποιες από τον R1;

Άσκηση 3: Δυναμική δρομολόγηση IPv6

Θα χρησιμοποιήσετε το δίκτυο της προηγούμενης άσκησης. Για τη δυναμική δρομολόγηση στο IPv6 τα αντίστοιχα των πρωτοκόλλων RIP και OSPF του IPv4 είναι τα RIPng και OSPFv3. Το BGP κατά τη διάρκεια της εγκατάστασης γειτονίας μπορεί να διαπραγματευτεί επιλογές για πολλαπλά πρωτόκολλα (multiprotocol extensions). Εάν ενεργοποιηθούν αυτές κατά τη διάρκεια της εγκατάστασης σύνδεσης με τον γείτονα, οι διαφημίσεις διαδρομών περιλαμβάνουν και ένα πρόθεμα για την οικογένεια διευθύνσεων (address family prefix). Οι οικογένειες διευθύνσεων περιλαμβάνουν την IPv4 (προκαθορισμένη), IPv6, IPv4/IPv6 VPNs και πολλαπλή διανομή BGP.

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

3.1 Μέσω vtysh διαγράψτε τις στατικές διαδρομές στους R1 και R2.
3.2 Στους R1 και R2 εισέλθετε σε router configuration mode για το πρωτόκολλο RIPng. Ενεργοποιήστε το RIPng στις διεπαφές των δρομολογητών στο WAN και τα αντίστοιχα LAN. Περιμένετε λίγο.
3.3 Εμφανίστε στον R1 τον πίνακα δρομολόγησης IPv6 για το RIPng. Πόσες εγγραφές βλέπετε;
3.4 Ποια και τι είδους είναι διεύθυνση του επόμενου κόμβου για το δίκτυο fd00:2::/64;
3.5 Μπορείτε να κάνετε ping από το PC1 στο PC2;
3.6 Ξεκινήστε καταγραφή πακέτων IPv6 με το tcpdump στη διεπαφή του R1 στο WAN1, εμφανίζοντας λεπτομερείς πληροφορίες για τα πακέτα χωρίς επίλυση ονομάτων και περιμένετε τουλάχιστον ένα λεπτό.
3.7 Τι είδους πακέτα RIPng παρατηρείτε και ποιος είναι ο προορισμός τους; *[Υποδ. Αναζητήστε πληροφορίες στο διαδίκτυο για την IPv6 διεύθυνση προορισμού που βλέπετε]*.
3.8 Τι τιμή έχει το Hop Limit των πακέτων IPv6 που τα μεταφέρουν και γιατί;

3.9 Ποιο πρωτόκολλο στρώματος μεταφοράς και ποια θύρα χρησιμοποιεί το RIPng; Είναι τα ίδια με αυτά που χρησιμοποιεί το RIP;
3.10 Απενεργοποιήστε το RIPng στους R1 και R2.
3.11 Αποθηκεύστε την παραμετροποίηση του FRR. *[Υποδ. Δείτε εντολή write.]*
3.12 Επανεκκινήστε την υπηρεσία FRR.
3.13 Στους R1 και R2 εισέλθετε σε router configuration mode για το πρωτόκολλο OSPF6. Ορίστε router-id 1.1.1.1 και 2.2.2.2 στους R1 και R2, αντίστοιχα.
3.14 Ενεργοποιήστε το OSPF6 στον R1 δηλώνοντας τις διεπαφές του στα LAN1 και WAN1 στην περιοχή 0.0.0.0.
3.15 Παρόμοια στον R2 για τις διεπαφές του στα LAN2 και WAN1. Περιμένετε περίπου ένα λεπτό.
3.16 Εμφανίστε στον R2 τον πίνακα δρομολόγησης IPv6 για το OSPF6. Πόσες εγγραφές βλέπετε; Πώς προέκυψε το κόστος τους;
3.17 Ποια και τι είδους είναι διεύθυνση του επόμενου κόμβου για το δίκτυο fd00:1::/64;
3.18 Ξεκινήστε καταγραφή πακέτων IPv6 με το tcpdump στη διεπαφή του R2 στο WAN1, εμφανίζοντας λεπτομερείς πληροφορίες για τα πακέτα χωρίς επίλυση ονομάτων και περιμένετε τουλάχιστον ένα λεπτό.
3.19 Τι είδους πακέτα OSPFv3 παρατηρείτε και ποια είναι η διεύθυνση προορισμού τους;
3.20 Τι τιμή έχει το Hop Limit των πακέτων IPv6 που τα μεταφέρουν;
3.21 Ποιο αριθμό πρωτοκόλλου (next header) ανωτέρου στρώματος χρησιμοποιεί το OSPFv3; Είναι ίδιος με αυτόν του OSPFv2;
3.22 Μπορείτε να κάνετε ping6 από το PC2 στο PC1;
3.23 Απενεργοποιήστε το OSPF6 στους R1 και R2.
3.24 Επανεκκινήστε την υπηρεσία FRR.
3.25 Στον R1 ορίστε ως router-id 1.1.1.1 και εισέλθετε σε router configuration mode για το BGP δηλώνοντας αυτόνομο σύστημα AS 65010.
3.26 Στην τυπική του χρήση για δρομολόγηση το FRR απαιτεί την εφαρμογή φίλτρων στις συνόδους eBGP για συμβατότητα με το RFC 8212. Χωρίς φίλτρο εισόδου καμία διαδρομή δεν γίνεται δεκτή και χωρίς φίλτρο εξόδου δεν ανακοινώνονται διαδρομές. Για τη συνέχεια ακυρώστε την απαίτηση αυτή. *[Υποδ. Δείτε εντολή bgp ebgp-requires-policy.]*
3.27 Στο BGP η σχέση γειτονίας από προεπιλογή (default) ενεργοποιείται για την οικογένεια διευθύνσεων IPv4. Στη συγκεκριμένη περίπτωση όμως δεν έχουμε ορίσει διευθύνσεις IPv4 στις διεπαφές του δρομολογητή, οπότε πρέπει να απενεργοποιηθεί η χρήση της. Αυτό όμως συνεπάγεται ότι θα πρέπει να ενεργοποιείται ρητά για την εκάστοτε χρησιμοποιούμενη οικογένεια διευθύνσεων με κάθε γείτονα. Δηλώστε ότι δεν θέλουμε να χρησιμοποιήσουμε την οικογένεια διευθύνσεων IPv4 unicast για τη δημιουργία γειτονίας. *[Υποδ. Δείτε εντολή bgp default.]*
3.28 Δηλώστε τον R2 ως γείτονα στο αυτόνομο σύστημα AS 65020.
3.29 Εισέλθετε στο υπο-μενού του R1 για την οικογένεια διευθύνσεων (address-family) IPv6 προκειμένου να ορίσετε τα διαφημιζόμενα δίκτυα και ενεργοποιήσετε τη σχέση γειτονίας.
3.30 Διαφημίστε το δίκτυο του LAN1.
3.31 Ενεργοποιήστε για IPv6 τη σχέση γειτονίας με τον R2 και εξέλθετε με exit. *[Υποδ. Δείτε υπο-εντολή activate της εντολής neighbor.]*
3.32 Επαναλάβατε τα προηγούμενα για τον R2 με router-id 2.2.2.2 στο αυτόνομο σύστημα AS 65020, απενεργοποιώντας την πολιτική φίλτρων eBPG και την οικογένεια διευθύνσεων IPv4

και ορίζοντας τον R1 ως γείτονα IPv6 στο αυτόνομο σύστημα AS 65010. Στην οικογένεια διευθύνσεων IPv6, διαφημίστε το δίκτυο LAN2, ενεργοποιήστε για IPv6 τη σχέση γειτονίας με τον R1 και εξέλθετε με exit.

3.33 Περιμένετε περίπου δύο λεπτά. Με ποια εντολή vtysh μπορείτε να επιβεβαιώσετε ότι έχει εγκατασταθεί σύνοδος BGP μεταξύ των R1 και R2;

3.34 Εμφανίστε στον R1 τον πίνακα δρομολόγησης IPv6 για το BGP. Πόσες δυναμικές εγγραφές βλέπετε;

3.35 Ποια και τι είδους είναι διεύθυνση του επόμενου κόμβου για το δίκτυο fd00:2::/64;

3.36 Ποιες διαδρομές διαφημίζει προς τον R2 και με ποιο επόμενο βήμα;

3.37 Ξεκινήστε καταγραφή πακέτων με το tcpdump στη διεπαφή του R1 στο WAN1, εμφανίζοντας λεπτομερείς πληροφορίες για τα πακέτα, χωρίς επίλυση ονομάτων, χωρίς να συλλαμβάνετε μηνύματα ICMPv6 και περιμένετε τουλάχιστον ένα λεπτό.

3.38 Τι είδους μηνύματα BGP παρατηρείτε; Ποιο πρωτόκολλο μεταφοράς και ποια θύρα χρησιμοποιείται;Είναι ίδια με τα αντίστοιχα σε IPv4;

3.39 Τι τιμή έχει το Hop Limit των πακέτων IPv6 που τα μεταφέρουν;

3.40 Μπορείτε να κάνετε ping6 από το PC1 στο PC2;

3.41 Αφού επανεκκινήσετε το PC1, εισέλθετε στο περιβάλλον του frr, ορίστε ως router-id 1.1.0.0 και στατική διεύθυνση fd00:1::2/64 για τη διεπαφή του στο LAN1.

3.42 Στο PC1 εισέλθετε σε router configuration mode για το BGP δηλώνοντας αυτόνομο σύστημα AS 65010.

3.43 Δηλώστε ότι δεν θα χρησιμοποιήσετε την οικογένεια διευθύνσεων IPv4 unicast για τη δημιουργία γειτονίας.

3.44 Δηλώστε τον R1 ως γείτονα στο αυτόνομο σύστημα AS 65010 καθορίζοντας έτσι σύνοδο τύπου iBGP.

3.45 Εισέλθετε στο υπο-μενού για την οικογένεια διευθύνσεων IPv6, ενεργοποιήστε για IPv6 τη σχέση γειτονίας με τον R1 και εξέλθετε με exit.

3.46 Στον R1 σε router configuration mode για το BGP δηλώστε το PC1 ως γείτονα στο ίδιο αυτόνομο σύστημα.

3.47 Αφού εισέλθετε στο υπο-μενού για την οικογένεια διευθύνσεων IPv6, ενεργοποιήσετε για IPv6 τη σχέση γειτονίας με το PC1, δηλώστε ότι για τις διαφημίσεις προς το PC1 το επόμενο βήμα είναι ο εαυτός του και εξέλθετε με exit.

3.48 Με ποια εντολή vtysh μπορείτε να επιβεβαιώσετε ότι έχει εγκατασταθεί σύνοδος iBGP μεταξύ των PC1 και R1;

3.49 Εμφανίστε στο PC1 τον πίνακα δρομολόγησης IPv6 για το BGP. Πόσες εγγραφές βλέπετε;

3.50 Γιατί δεν είναι επιλεγμένη η διαδρομή προς το δίκτυο fd00:1::/64;

3.51 Ποια και τι είδους είναι διεύθυνση του επόμενου κόμβου για το δίκτυο fd00:2::/64;

3.52 Μπορείτε να κάνετε ping6 από το PC2 στο PC1;

Άσκηση 4: Μηχανισμός μετάβασης 464 XLAT

Θα χρησιμοποιήσετε την τοπολογία της προηγούμενης άσκησης για να εφαρμόσετε το μηχανισμό μετάβασης 464 XLAT. Προς τούτο θα δώσετε διευθύνσεις IPv4 στα PC1 και PC2 και θα ορίσετε μετάφραση NAT64 ώστε τα πακέτα IPv4 να μετατρέπονται σε πακέτα IPv6 και αντιστρόφως. Για τον μηχανισμό 464 XLAT, ο R1 θα επιτελεί τη λειτουργία CLAT, ενώ ο R2 τη λειτουργία PLAT.

Το FreeBSD από την έκδοση 11 υποστηρίζει ενσωματωμένο μηχανισμό NAT64, αντίστοιχο του in-kernel NAT, που μπορεί να χρησιμοποιηθεί σε συνδυασμό με το τείχος προστασίας ipfw. Για τη λειτουργία μετάφρασης διευθύνσεων IPv6/IPv4 πρέπει πρώτα να δημιουργηθεί στο τείχος προστασίας ένας πίνακας NAT64 (δείτε πιο κάτω) και μετά να προστεθεί στο τείχος προστασίας κανόνας μέσω της εντολής "ipfw add" ώστε η κίνηση που ταιριάζει σε αυτόν να ωθείται στον πίνακα NAT64 προκειμένου να υποστεί την οριζόμενη εκεί μετάφραση διευθύνσεων. Ορίζονται διάφοροι τρόποι stateful και stateless μετάφρασης. Εδώ θα χρησιμοποιήσετε το stateful NAT64 για τη λειτουργία PLAT και το stateless XLAT464 για τη λειτουργία CLAT. Οι εντολές ορισμού της μετάφρασης είναι:

ipfw nat64lsn *name* **create** *options* για τη λειτουργία PLAT και **ipfw nat64clat** *name* **create** *options* για τη λειτουργία για τη λειτουργία CLAT.

όπου *name* είναι το όνομα του πίνακα NAT, π.χ. nat64, και *options* οι σχετικοί με την μετάφραση nat64 κανόνες.

Στο stateful NAT64 μπορείτε να ορίσετε ως options τα

prefix6 ***ipv6_prefix/length*** για τις IPv4-embedded IPv6 διευθύνσεις που θα χρησιμοποιηθούν κατά τη μετάφραση για να αναπαραστήσουν διευθύνσεις IPv4, και
prefix4 ***ipv4_prefix/length*** για τις IPv4 διευθύνσεις που θα χρησιμοποιηθούν κατά τη μετάφραση.

Στο XLAT464 πρέπει να ορίσετε ως options τα

clat_prefix ***ipv6_prefix/length*** για τις IPv4-embedded IPv6 διευθύνσεις που θα χρησιμοποιηθούν κατά τη μετάφραση για να αναπαραστήσουν διευθύνσεις IPv4 πηγής, και
plat_prefix ***ipv6_prefix/length*** για τις IPv4-embedded IPv6 διευθύνσεις που θα χρησιμοποιηθούν κατά τη μετάφραση για να αναπαραστήσουν διευθύνσεις IPv4 προορισμού.

Και στους δύο τρόπους με

allow_private επιτρέπεται η χρήση ιδιωτικών διευθύνσεων κατά τη μετάφραση (που απαγορεύονται σε πραγματικά δίκτυα)
log επιτρέπεται η καταγραφή στη διεπαφή ipfwlog0, που προηγουμένως πρέπει να δημιουργηθεί.

Με τις εντολές ***ipfw nat64lsn/nat64clat*** name ***show*** μπορείτε να δείτε την τρέχουσα διάρθρωση του πίνακα NAT64/CLAT64 με όνομα name. Με την εντολή ***ipfw nat64lsn*** name ***show states*** μπορείτε να δείτε την κατάσταση του πίνακα NAT64 με όνομα name. Για περισσότερες λεπτομέρειες δείτε παράγραφο IPv6/IPv4 NETWORK ADDRESS AND PROTOCOL TRANSLATION της σελίδας man του ipfw στην ιστοσελίδα https://www.freebsd.org/cgi/man.cgi?query=ipfw.

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

4.1 Ορίστε μέσω vtysh του R1 την IPv4 διεύθυνση 192.168.1.1/24 για τη διεπαφή του στο LAN1.

4.2 Ορίστε μέσω vtysh του R2 την IPv4 διεύθυνση 192.168.2.1/24 για τη διεπαφή του στο LAN2.

4.3 Ορίστε μέσω vtysh του PC1 την IPv4 διεύθυνση 192.168.1.2/24 για τη διεπαφή του στο LAN1 και ως προκαθορισμένη διαδρομή την 192.168.1.1.

4.4 Ορίστε μέσω vtysh του PC2 την IPv4 διεύθυνση 192.168.2.2/24 για τη διεπαφή του στο LAN1 και ως προκαθορισμένη διαδρομή την 192.168.2.1.

4.5 Στο αρχείο εκκίνησης /etc/rc.conf του R1 προσθέστε τις ακόλουθες εντολές firewall_enable="YES" να ενεργοποιηθεί το τείχος προστασίας ipfw, firewall_nat64_enable="YES" για να ενεργοποιηθεί η ενσωματωμένη λειτουργία NAT64, firewall_type="open" για ανοικτό τύπο τείχους προστασίας και firewall_logif="YES" για να ενεργοποιηθεί η δυνατότητα καταγραφής πακέτων της λειτουργίας NAT64.

4.6 Εκκινήστε την υπηρεσία ipfw του τείχους προστασίας.
4.7 Πόσους κανόνες περιέχει το τείχος προστασίας του R1;
4.8 Μπορείτε να κάνετε ping6 από το PC1 στο PC2. Εάν όχι ελέγξτε για λάθη στο /etc/rc.conf.
4.9 Δημιουργήστε πίνακα nat64clat με όνομα nat64 ώστε κίνηση με clat_prefix fd00:3:1::/96 να μεταφράζεται σε plat_prefix 64:ff9b::/96, να επιτρέπεται η χρήση ιδιωτικών διευθύνσεων καθώς και η καταγραφή.
4.10 Προσθέστε στο τείχος προστασίας του R1 κανόνα με αύξοντα αριθμό 2000 ώστε να ωθείται προς μετάφραση στον πίνακα nat64clat με όνομα nat64 η κίνηση IPv4, ανεξάρτητα διεύθυνσης πηγής και με προορισμό εκτός του R1, που λαμβάνεται από τη διεπαφή του στο LAN1.
4.11 Προσθέστε κανόνα στο τείχος προστασίας του R1 με αύξοντα αριθμό 3000 ώστε να ωθείται προς μετάφραση στον πίνακα nat64clat με όνομα nat64 η κίνηση IPv6, με πηγή το δίκτυο 64:ff9b::/96 και προορισμό το δίκτυο fd00:3:1::/96, που λαμβάνεται από τη διεπαφή του στο WAN1.
4.12 Μέσω vtysh του R1 προσθέστε διαδρομή προς το δίκτυο 64:ff9b::/96 μέσω του R2.
4.13 Επαναλάβατε τις ρυθμίσεις της ερώτησης 4.5 στον R2 και εκκινήστε την υπηρεσία του τείχους προστασίας.
4.14 Δημιουργήστε πίνακα nat64lsn με όνομα nat64 ώστε κίνηση με πρόθεμα IPv4 2.2.2.0/24 να μεταφράζεται σε πρόθεμα IPv6 64:ff9b::/96, να επιτρέπεται η χρήση ιδιωτικών διευθύνσεων καθώς και η καταγραφή.
4.15 Προσθέστε κανόνα στο τείχος προστασίας του R2 με αύξοντα αριθμό 2000 ώστε να ωθείται προς μετάφραση στον πίνακα nat64lsn με όνομα nat64 η κίνηση IPv6, με πηγή το δίκτυο fd00:3:1::/96 και προορισμό το δίκτυο 64:ff9b::/96, που λαμβάνεται από τη διεπαφή του στο WAN1.
4.16 Προσθέστε κανόνα στο τείχος προστασίας του R2 με αύξοντα αριθμό 3000 ώστε να ωθείται προς μετάφραση στον πίνακα nat64lsn με όνομα nat64 η κίνηση IPv4, ανεξάρτητα διεύθυνσης πηγής και με προορισμό το δίκτυο 2.2.2.0/24, που λαμβάνεται από τη διεπαφή του στο LAN2.
4.17 Μέσω vtysh του R2 προσθέστε διαδρομή προς το δίκτυο fd00:3:1::/96 μέσω του R1.
4.18 Στη συνέχεια προσθέστε ως προκαθορισμένη διαδρομή IPv4 την 192.168.2.2.
4.19 Μπορείτε να κάνετε ping από το PC1 στα R1 και PC2 χρησιμοποιώντας τις IPv4 διευθύνσεις του; Εάν όχι, ελέγξτε τους κανόνες του τείχους προστασίας και τους ορισμούς των στατικών διαδρομών.
4.20 Στο R1 δημιουργήστε την ψευδο-διεπαφή ipfwlog0 και ξεκινήστε μια καταγραφή.
4.21 Παρομοίως στο R2.
4.22 Στο PC1 δώστε την εντολή "*ping –c 1 192.168.2.2*". Ποια πακέτα παρατηρείτε στις καταγραφές στους R1 και R2;
4.23 Μέσω vtysh του PC2 ορίστε τις 172.17.17.2/24 και 10.0.0.2/24 ως δευτερεύουσες διευθύνσεις IPv4 στη διεπαφή του στο LAN2.
4.24 Στο PC1 μπορείτε να κάνετε ping στις προηγούμενες διευθύνσεις IPv4;
4.25 Ξεκινήστε μια καταγραφή στο PC2 και επαναλάβετε τα ping στις IPv4 διευθύνσεις του PC2. Με ποια διεύθυνση IPv4 εμφανίζεται το PC1 στα μηνύματα ICMP;
4.26 Στον R2 δείτε την κατάσταση του nat64lsn.
4.27 Στο PC1 κάντε ping σε δύο από τις IPv4 διευθύνσεις του PC2 και στη συνέχεια ελέγξτε την κατάσταση του nat64lsn. Τι παρατηρείτε; Πόσο διαρκούν οι σχετικές εγγραφές;

4.28 Μπορείτε να συνδεθείτε με ssh από το PC1 στο PC2 χρησιμοποιώντας κάποια από τις IPv4 διευθύνσεις του; Γιατί; *[Υποδ. Δείτε καταγραφές στην ipfwlog0.]*

4.29 Ορίστε το 1480 ως μέγεθος της MTU της διεπαφής em0 των PC. Επιτυγχάνει τώρα το προηγούμενο ssh;

Άσκηση 5: Μηχανισμός μετάβασης Teredo

Για αυτό το μέρος της άσκησης θα χρησιμοποιήσετε απλά εικονικά μηχανήματα FreeBSD 13.2 για να κατασκευάσετε δύο νέα PC *σε δικτύωση NAT (όχι NAT Network).* Απαντήστε τις παρακάτω ερωτήσεις καταγράφοντας παράλληλα, όπου απαιτείται, την ακριβή σύνταξη των εντολών που χρησιμοποιήσατε.

5.1 Ενεργοποιήστε τον DHCP client στις διεπαφές των εικονικών μηχανημάτων και βεβαιωθείτε ότι έχετε πρόσβαση στο Internet.

5.2 Εγκαταστήστε σε αυτά το teredo client κατεβάζοντας το πακέτο miredo.

5.3 Προσθέστε την εντολή miredo_enable="YES" στο κατάλληλο αρχείο ώστε να ξεκινά η υπηρεσία teredo.

5.4 Στο αρχείο /usr/local/etc/miredo/miredo.cong αφαιρέστε τον χαρακτήρα # από τη γραμμή ServerAddress teredo.iks-jena.de (για να επιλεχθεί αυτός ο εξυπηρετητής) και προσθέστε το στη γραμμή ServerAddress teredo.remlab.de (που πλέον δεν λειτουργεί). Στη συνέχεια εκκινήστε την υπηρεσία miredo.

5.5 Ποια νέα διεπαφή δικτύου βλέπετε στο PC1 και ποια η IPv6 διεύθυνσή της; *[Ίσως χρειαστεί να περιμένετε λίγο μέχρι να δημιουργηθεί η διεύθυνση].*

5.6 Στο PC2 ξεκινήστε μια καταγραφή χωρίς επίλυση ονομάτων και διευθύνσεων στη διεπαφή em0.

5.7 Ποια είναι η διεύθυνση IPv4 του εξυπηρετητή Teredo με τον οποίο επικοινωνεί το PC2;

5.8 Ποιο πρωτόκολλο μεταφοράς χρησιμοποιείται και ποια θύρα αντιστοιχεί στον εξυπηρετητή Teredo;

5.9 Ξεκινήστε με Wireshark μια καταγραφή πακέτων στη φυσική κάρτα του υπολογιστή σας εφαρμόζοντας φίλτρο απεικόνισης teredo και αφήστε τη να τρέχει. Ποιου πρωτοκόλλου μηνύματα παρατηρείτε;

5.10 Ποιο πρόθεμα δικτύου IPv6 διαφημίζει ο εξυπηρετητής Teredo και πώς σχετίζεται με την IPv4 διεύθυνσή του;

5.11 Από το PC1 μπορείτε να κάνετε ping6 στα www.ntua.gr, www.ibm.com ή www.amazon.com; *[Υποδ. Περιμένετε λίγο για την απάντηση.]*

5.12 Από το PC1 κάντε ping6 σε κάποιον από τους προηγούμενους προορισμούς που απάντησε και αφήστε το να τρέχει.

5.13 Ποια νέα μηνύματα παρατηρείτε στην καταγραφή στο Wireshark;

5.14 Παρατηρείτε μηνύματα ICMPv6 Echo request/reply στην καταγραφή στο Wireshark;

5.15 Σε νέο παράθυρο του PC1 ξεκινήστε μια καταγραφή χωρίς επίλυση ονομάτων και διευθύνσεων στη διεπαφή em0. Ποιο πρωτόκολλο ανωτέρου στρώματος παρατηρείτε, ποια είναι η διεύθυνση IPv4 και ποια η θύρα που αντιστοιχεί στον αναμεταδότη Teredo;

5.16 Ξεκινήστε στο PC1 νέα καταγραφή χωρίς επίλυση ονομάτων και διευθύνσεων στη διεπαφή teredo. Τι είδους πακέτα και πρωτόκολλα ανωτέρου στρώματος βλέπετε;

5.17 Μπορείτε να κάνετε ping6 από το PC1 στο PC2 χρησιμοποιώντας τη διεύθυνση IPv6 της διεπαφής teredo; *[Υποδ. Το αποτέλεσμα εξαρτάται από την ύπαρξη και το είδος τείχους προστασίας]*.

5.18 Παράγονται μηνύματα ICMPv6 στη διεπαφή teredo;

5.19 Σταματήστε την καταγραφή στη διεπαφή teredo και ξεκινήστε νέα στην em0. Παράγονται δεδομενογράμματα UDP αντίστοιχα με τα ICMPv6 μηνύματα στη διεπαφή του PC1; Εάν ναι, προς ποια διεύθυνση στέλνονται;

5.20 Κάντε ping6 www.quad9.net και μετά ping6 www.f5.com. Επιλέγεται ο ίδιος teredo relay;

Ονοματεπώνυμο:	**Όνομα PC:**
Ομάδα:	**Ημερομηνία:**

Εργαστηριακή Άσκηση 11
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 .....