ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΔΥΤΙΚΗΣ ΕΛΛΑΔΑΣ

ΣΧΟΛΗ: ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΟΙΚΟΝΟΜΙΑΣ

ΤΜΗΜΑ: ΔΙΟΙΚΗΣΗ ΕΠΙΧΕΙΡΗΣΕΩΝ (ΠΡΩΗΝ ΕΠΙΧΕΙΡΗΜΑΤΙΚΟΥ ΣΧΕΔΙΑΣΜΟΥ ΚΑΙ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ)

ΤΙΤΛΟΣ ΠΤΥΧΙΑΚΗΣ ΕΡΓΑΣΙΑΣ:

ΜΕΛΕΤΗ ΤΩΝ ΜΗΧΑΝΙΣΜΩΝ ΜΕΤΑΒΑΣΗΣ ΣΤΟ IPv6

ΟΝΟΜΑΤΕΠΩΝΥΜΟ ΣΠΟΥΔΑΣΤΡΙΑΣ:

ΧΑΤΖΗΜΑΡΚΟΥ ΕΥΑΓΓΕΛΙΑ, Α.Μ.: 11493

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ:

ΣΤΑΜΟΣ ΚΩΝΣΤΑΝΤΙΝΟΣ

ΠΑΤΡΑ, ΙΑΝΟΥΑΡΙΟΣ 2015

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΠΡΟΛΟΓΟΣ

Η παρούσα πτυχιακή εργασία με θέμα **«Μελέτη των μηχανισμών μετάβασης στο IPv6»**, έχει ως σκοπό να παρουσιάσει τους μηχανισμούς μετάβασης από το IPv4 (Internet Protocol version 4) στο IPv6 (Internet Protocol version 6). Το IPv6 αποτελεί το νέο πρωτόκολλο δικτύου και έχει σκοπό να επιλύσει τον περιορισμένο χώρο διευθύνσεων του IPv4. Για να γίνει ομαλά η μετάβαση από το ένα πρωτόκολλο στο άλλο, είναι απαραίτητη η χρήση κάποιων μηχανισμών μετάβασης.

Την πτυχιακή εργασία την επιμελήθηκε η σπουδάστρια Χατζημάρκου Ευαγγελία του τμήματος Διοίκηση Επιχειρήσεων (πρώην τμήμα Επιχειρηματικού Σχεδιασμού και Πληροφοριακών Συστημάτων) της σχολής Διοίκησης και Οικονομίας του Τεχνολογικού Εκπαιδευτικού Ιδρύματος Δυτικής Ελλάδας. Η ανάθεση του θέματος έγινε τον Ιούνιο του 2014 και η ολοκλήρωσή της έγινε τον Ιανουάριο του 2015. Εισηγητής του θέματος είναι ο κ. Στάμος Κωνσταντίνος, τον οποίο ευχαριστώ για τη βοήθεια και την καθοδήγηση του. Η κυριότερη πηγή άντλησης πληροφοριών ήταν το Διαδίκτυο, καθώς πρόκειται για τεχνολογία που συνεχώς εξελίσσεται και προκύπτουν νέα δεδομένα.

Κεφάλαιο 1: ΠΡΩΤΟΚΟΛΛΑ IP

ΕΙΣΑΓΩΓΗ

Το Διαδίκτυο (Internet) έχει μπει για τα καλά στην καθημερινότητα μας και ολοένα και περισσότεροι το χρησιμοποιούν ως πολύτιμο εργαλείο στην εργασία τους, ως μέσο επικοινωνίας και πληροφόρησης, ως τρόπος απασχόλησης στον ελεύθερο χρόνο τους.

Ένα δομικό στοιχείο του Διαδικτύου είναι το πρωτόκολλο επικοινωνίας που επιτρέπει τη διασύνδεση όλων των συστημάτων. Αυτό είναι το Πρωτόκολλο Διαδικτύου (Internet Protocol-IP).

Όμως, η ιλιγγιώδης εξέλιξη της τεχνολογίας στον τομέα των ηλεκτρονικών υπολογιστών, που αντικαθιστούν τις παραδοσιακές μορφές επικοινωνίες, φανέρωσε την αδυναμία του υπάρχοντος Πρωτοκόλλου Διαδικτύου IPv4 να διαχειριστεί τον ολοένα αυξανόμενο αριθμό των χρηστών και των δικτύων που αποτελούν σήμερα το Internet, αλλά και να εκμεταλλευτεί τον μεγάλο όγκο των νέων εφαρμογών που συνεχώς εμφανίζονται με αυξανόμενες απαιτήσεις.

Η έκδοση 4 του Πρωτοκόλλου IP είναι η πλέον διαδεδομένη σήμερα. Όμως οι σύγχρονες ανάγκες του Διαδικτύου απαιτούν τη χρήση μιας νέας βελτιωμένης έκδοσης του Πρωτοκόλλου IP.

Η νέα αυτή έκδοση είναι το Πρωτόκολλο Διαδικτύου έκδοση 6 (Internet Protocol version 6- IPv6), το οποίο σχεδιάστηκε με σκοπό να ξεπεραστούν οι υπάρχοντες περιορισμοί και αδυναμίες και να προσφερθούν νέα χαρακτηριστικά.

Η μετάβαση στο νέο πρωτόκολλο δεν είναι απλό εγχείρημα και δεν μπορεί να γίνει μέσα σε μια στιγμή. Για να διευκολυνθεί η μετάβαση από το IPv4 στο IPv6 και να ελαχιστοποιηθούν τα προβλήματα κατά την μεταβατική περίοδο, έχει αναπτυχθεί μια σειρά από τεχνικές μετάβασης.

1.1 IPv4 Πρωτόκολλο

Το ήδη υπάρχον Πρωτόκολλο Internet IPv4 ήταν η πρώτη χρησιμοποιημένη δημόσια έκδοση του Πρωτοκόλλου Internet (RFC791). Το IPv4 σχεδιάστηκε στις αρχές της δεκαετίας του ΄80 χωρίς να αλλάξει ιδιαίτερα στη συνέχεια. Έχει αποδεχτεί ένα ικανοποιητικό πρωτόκολλο και έχει καλύψει τις ανάγκες της διευθυνσιοδότησης για δεκαετίες. Το IPv4 χρησιμοποιείται για να εντοπίσει τις συσκευές σε ένα δίκτυο μέσω ενός συστήματος διευθυνσιοδότησης. Το Πρωτόκολλο Internet έχει σχεδιαστεί για χρήση σε διασυνδεδεμένα συστήματα των πακέτων μεταγωγής των δικτύων επικοινωνίας υπολογιστών.

Το IPv4 χρησιμοποιεί ένα σύστημα διευθυνσιοδότησης μήκους 32 bits (4 byte). Οι διευθύνσεις αυτές εμφανίζονται συνήθως ως δεκαδικές τιμές σε τέσσερις οκτάδες χωρισμένες με τελείες, το καθένα με εύρος 0 έως 255, ή 8 bits ανά αριθμό. Έτσι, το IPv4 περιορίζει το χώρο διευθύνσεων σε 2^{32} διευθύνσεις (μόλις πάνω από 4 δισεκατομμύρια). Η εξάντληση των διευθύνσεων δεν ήταν αρχικά μια ανησυχία του IPv4. Η αύξηση της χρήσης του Internet οδήγησε στην εξάντληση του χώρου διευθύνσεων. Ο τεράστιος αριθμός των νέων διασυνδεδεμένων υπολογιστών και δικτύων, και γενικότερα η επέκταση του Internet σήμερα, πέρα από κάθε αρχική προσδοκία οδήγησαν σε εξάντληση των IPv4 διευθύνσεων. Το πρόβλημα είχε αρχίσει να διαφαίνεται πριν ακόμη το 1994, ακόμα και μετά τον ανασχεδιασμό του συστήματος διευθυνσιοδότησης έγινε σαφές ότι αυτό δεν αρκεί για να αποτρέψει την εξάντληση των διευθύνσεων IPv4, και ότι απαιτούνται περαιτέρω αλλαγές στην υποδομή του Διαδικτύου.

1.2 IPv6 Πρωτόκολλο

Το IPng (IP next generation- επόμενη γενιά) γνωστό ως IPv6 (Internet Protocol version 6- Πρωτόκολλο Διαδικτύου έκδοση 6), είναι η τελευταία έκδοση του Internet Protocol (IP), είναι ένα σύνολο πρωτοκόλλων, το οποίο χρησιμοποιούν οι υπολογιστές για να ανταλλάσουν πληροφορίες μέσω Internet και μέσω δικτύων. Σκοπός του είναι να αντικαταστήσει την παλαιότερη έκδοση του IPv4, το οποίο εξακολουθεί να ασκεί περισσότερο από το 96% της κίνησης του Internet σε παγκόσμιο επίπεδο από το Μάιο του 2014. Το IPv6 αναπτύχθηκε το 1994 από το Internet Engineering Task Force (IETF- Ομάδα δράσης μελέτης τεχνολογιών Internet) για να ασχοληθεί με την αδυναμία του IPv4 να ακολουθήσει τις εξελίξεις.

Σε κάθε συσκευή στο Διαδίκτυο έχει εκχωρηθεί μια IP διεύθυνση για την ταυτοποίηση και τον ορισμό τοποθεσίας. Με την ταχεία ανάπτυξη του Διαδικτύου, μετά την εμπορευματοποίηση της δεκαετίας του 1990, έγινε εμφανές ότι περισσότερες διευθύνσεις από το διαθέσιμο χώρο διευθύνσεων του IPv4 ήταν απαραίτητο να συνδεθούν με νέες συσκευές στο μέλλον. Το IPv6 είχε σχεδιαστεί ως μια εξελικτική αναβάθμιση του Πρωτοκόλλου Internet ενώ, στην πραγματικότητα συνυπάρχει με το ήδη υπάρχον IPv4 για κάποιο χρονικό

διάστημα. Έχει σχεδιαστεί για να επιτρέψει στο Διαδίκτυο να αυξάνεται σταθερά, τόσο όσον αφορά τον αριθμό των συνδεδεμένων host όσο και το σύνολο των δεδομένων κυκλοφορίας που διαβιβάζονται.

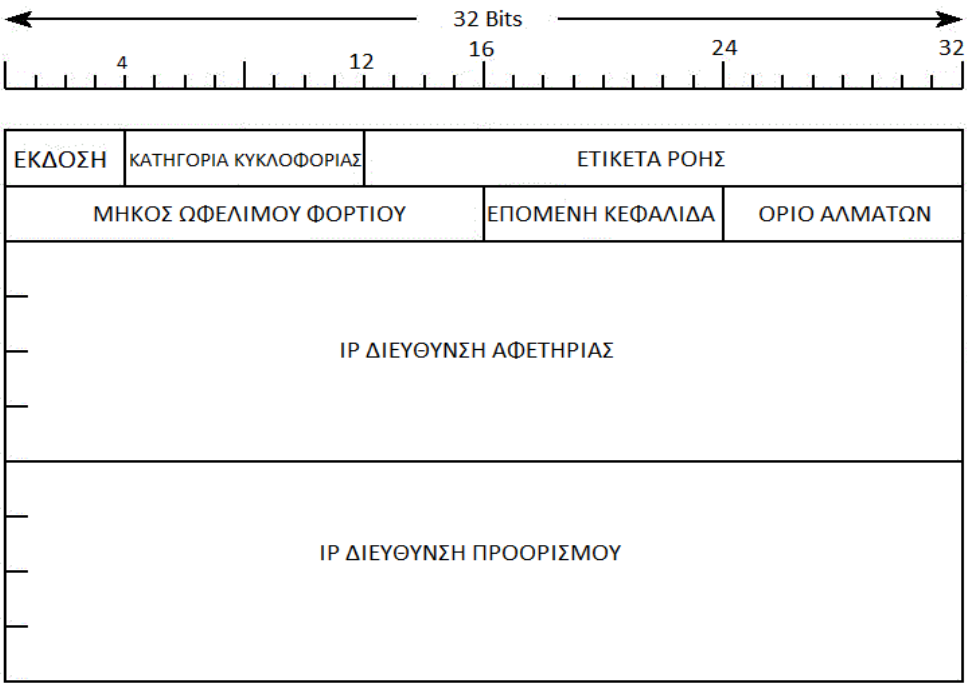
Το IPv6 χρησιμοποιεί 128 bit για μια διεύθυνση ή 2^{128} διευθύνσεις ή $3,4*10^{38}$ διευθύνσεις ή περισσότερο από $7,9*10^{28}$ διευθύνσεις από ότι χρησιμοποιεί το IPv4 και παρέχει περίπου 4,3 δισεκατομμύρια διευθύνσεις. Οι διευθύνσεις IPv6 είναι γραμμένες σε οκτώ ομάδες των τεσσάρων δεκαεξαδικών ψηφίων χωρισμένες με άνω και κάτω τελεία. Ένα παράδειγμα μιας IPv6 διεύθυνσης θα μπορούσε να είναι 3ffe: 1900: 4545: 3: 200: f8ff: fe21: 67CF. Τα δύο πρωτόκολλα δεν έχουν σχεδιαστεί για να είναι δυσλειτουργικά, περιπλέκοντας τη μετάβαση στο IPv6. Ωστόσο, αρκετοί μηχανισμοί μετάβασης έχουν επινοηθεί για να επιτρέψουν την επικοινωνία μεταξύ των IPv4 και IPv6 hosts.

1.2.1 Μορφή Πακέτων IPv6

Ένα πακέτο IPv6 είναι η μικρότερη οντότητα που ανταλλάσσονται μέσω του Πρωτοκόλλου Internet στο IPv6 του δικτύου. Τα πακέτα αποτελούνται από πληροφορίες ελέγχου για τη διευθυνσιοδότηση και τη δρομολόγηση. Ένα πακέτο IPv6 έχει δυο μέρη: μια επικεφαλίδα και το ωφέλιμο φορτίο, το οποίο αποτελείται από τα δεδομένα του χρήστη. Το ωφέλιμο φορτίο είναι συνήθως ένα datagram ή τμήμα του υψηλότερου επιπέδου του πρωτοκόλλου Transport Layer (Επίπεδο μεταφοράς), αλλά μπορεί να είναι δεδομένα για ένα Internet Layer (Επίπεδο Διαδικτύου) ή Link Layer (Επίπεδο συνδέσμου).

Ένα πακέτο IPv6 αρχίζει με μια βασική επικεφαλίδα (base header), που ακολουθείται από καμία, μια ή περισσότερες κεφαλίδες επέκτασης (extension header) , οι οποίες ακολουθούνται από τα δεδομένα. Τα πεδία ενός πακέτου δεν είναι σχεδιασμένα με κλίμακα. Συγκεκριμένα, οι κεφαλίδες επέκτασης μπορεί να είναι μεγαλύτερες ή μικρότερες από τη βασικά κεφαλίδα, ενώ το μέγεθος της περιοχής των δεδομένων μπορεί να είναι μεγαλύτερο από το μέγεθος των κεφαλίδων.

Η βασική κεφαλίδα του IPv6 είναι διπλάσια σε μέγεθος από ότι η κεφαλίδα του IPv4, αλλά περιέχει λιγότερες πληροφορίες. Η βασική κεφαλίδα καταλαμβάνει τις πρώτες 40 οκτάδες (320 bits) του πακέτου IPv6. Η μορφή της βασικής κεφαλίδας του IPv6 φαίνεται στην Εικόνα 1.



Εικόνα 1 Μορφή βασικής κεφαλίδας
(Πηγή: http://el.wikipedia.org)

Το πεδίο ΕΚΔΟΣΗ (4 bits) προσδιορίζει την έκδοση του πρωτοκόλλου, δηλαδή έχει την τιμή 6. Το πεδίο ΚΑΤΗΓΟΡΙΑ ΚΥΚΛΟΦΟΡΙΑΣ (8 bits) καθορίζει κάποια γενικά χαρακτηριστικά τα οποία χρειάζεται το πακέτο και καθορίζει την προτεραιότητα για το κάθε πακέτο που δρομολογείται. Η προκαθορισμένη τιμή του είναι 0. Το πεδίο ΕΤΙΚΕΤΑ ΡΟΗΣ (20 bits) χρησιμοποιείται για τον προσδιορισμό μιας συγκεκριμένης διαδρομής του πακέτου μέσω του δικτύου. Το πεδίο ΜΗΚΟΣ ΩΦΕΛΙΜΟΥ ΦΟΡΤΙΟΥ(16 bits) καθορίζει το μέγεθος των δεδομένων που μεταφέρονται, εξαιρείται δηλαδή η βασική κεφαλίδα. Το πεδίο ΕΠΟΜΕΝΗ ΚΕΦΑΛΙΔΑ (8 bits) καθορίζει το τύπο των πληροφοριών που ακολουθούν μετά την τρέχουσα κεφαλίδα. Αν, για παράδειγμα, το πακέτο περιλαμβάνει κεφαλίδα επέκτασης τότε το πεδίο καθορίζει το τύπο της κεφαλίδας επέκτασης, και αν δεν υπάρχει κεφαλίδα επέκτασης , το πεδίο καθορίζει το τύπο των δεδομένων που μεταφέρονται. Το πεδίο ΟΡΙΟ ΑΛΜΑΤΩΝ (8 bits) μειώνεται κατά ένα κάθε φορά που το πακέτο προωθείται στον επόμενο κόμβο. Αν η τιμή του φτάσει στο μηδέν τότε το πακέτο απορρίπτεται πριν φτάσει στον προορισμό του. Όπως φαίνεται στην Εικόνα 1, ο περισσότερος χώρος της κεφαλίδας είναι αφιερωμένος σε δύο πεδία που προσδιορίζουν τον αποστολέα και τον παραλήπτη. Το πεδίο ΔΙΕΥΘΥΝΣΗ ΑΦΕΤΗΡΙΑΣ (128 bits) περιέχει την IP διεύθυνση του αποστολέα του πακέτου. Τέλος, το πεδίο ΔΙΕΥΘΥΝΣΗ ΠΡΟΟΡΙΣΜΟΥ (128 bits) περιέχει την IP διεύθυνση του τελικού παραλήπτη του πακέτου.
Οι κεφαλίδες επέκτασης φέρουν προαιρετικές πληροφορίες του επιπέδου δικτύου που βρίσκονται σε ξεχωριστές επικεφαλίδες, οι οποίες τοποθετούνται ανάμεσα στην βασική επικεφαλίδα του IPv6 και στη επικεφαλίδα του επιπέδου μεταφοράς. Κάθε μια από τις κεφαλίδες επέκτασης προσδιορίζεται από μια τιμή του πεδίου

ΕΠΟΜΕΝΗ ΚΕΦΑΛΙΔΑ της προηγούμενης επικεφαλίδας. Ένα πακέτο IPv6 μπορεί να έχει καμία, μια ή περισσότερες επικεφαλίδες επέκτασης. Η κάθε επικεφαλίδα επέκτασης έχει μέγεθος ακέραιο πολλαπλάσιο των 8 bytes. Όλες οι κεφαλίδες επέκτασης είναι προαιρετικές και πρέπει να εμφανίζονται μόνο μια φορά το πολύ, εκτός από την Destination Options Header (Επικεφαλίδα Επιλογών Προορισμού) που μπορεί να εμφανιστεί δύο φορές.

Κεφαλίδα επέκτασης	Τύπος
Hop-by-Hop	0
Routing Header	43
Fragment Header	44
Authentication Header	51
Encapsulation Security Payload	52
Destination Options Header	60
Mobility Header	135

Πίνακας 1 Κεφαλίδες Επέκτασης

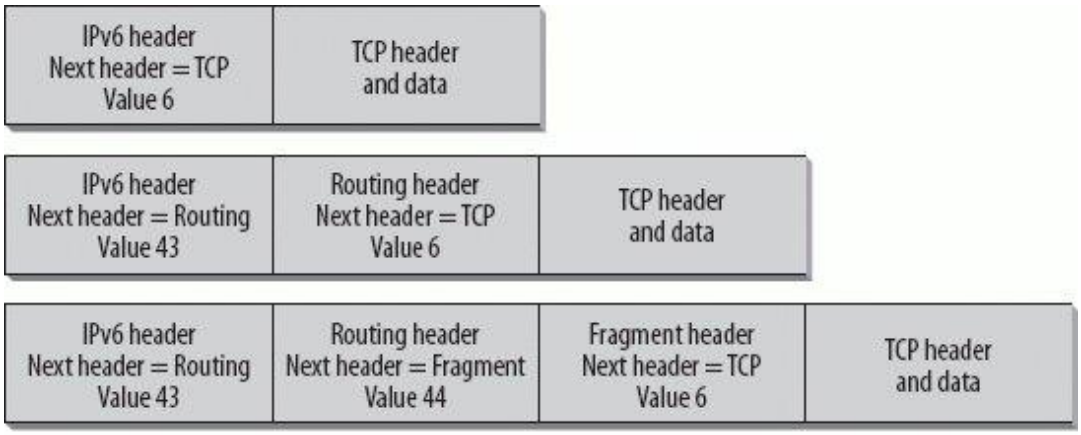
(Πηγή: Μπούρας, Χ. Εισαγωγή Στην IPv6 Τεχνολογία.[pdf]Διαθέσιμο στο: http://www.ebusinessforum.gr/old/content/downloads/Introduction_IPv6.pdf)

Όταν ένας κόμβος επεξεργάζεται ένα πακέτο IPv6 και δεν μπορεί να μεταφράσει το πεδίο ΕΠΟΜΕΝΗ ΚΕΦΑΛΙΔΑ της προηγούμενης κεφαλίδας, τότε πρέπει να απορρίψει το πακέτο (Σε αυτή τη περίπτωση, πρέπει να στείλει ένα ICMPv6 μήνυμα στον αποστολέα του πακέτου). Ομοίως, αν ένας κόμβος συναντήσει την τιμή 0 στο πεδίο ΕΠΟΜΕΝΗ ΚΕΦΑΛΙΔΑ κάποιας άλλης επικεφαλίδας και όχι της βασικής. Αν το πεδίο της βασικής επικεφαλίδας έχει την τιμή 59, τότε δεν υπάρχει επόμενη επικεφαλίδα.

Οι κεφαλίδες επέκτασης πρέπει να εξετάζονται και να υποβάλλονται σε επεξεργασία με το προορισμό του πακέτου, εκτός από την Hop-by-Hop (Βήμα-προς-Βήμα). Η Hop-by-Hop περιέχει προαιρετικές πληροφορίες που πρέπει να επεξεργαστούν από κάθε ενδιάμεσο κόμβο στο μονοπάτι του πακέτου, συμπεριλαμβανομένων και των κόμβων αφετηρίας και προορισμού. Όταν υπάρχει, πρέπει να ακολουθεί αμέσως μετά από τη βασική κεφαλίδα του IPv6. Όπως φαίνεται και στον Πίνακα 1, δηλώνεται με την τιμή 0 στο πεδίο ΕΠΟΜΕΝΗ ΚΕΦΑΛΙΔΑ της βασικής επικεφαλίδας.

Το Routing Header (Επικεφαλίδα Δρομολόγησης) χρησιμοποιείται όταν η πηγή θέλει το πακέτο να περάσει από έναν ή περισσότερους ενδιάμεσους κόμβους στην πορεία του προς τους προορισμούς. Το Fragment Header (Επικεφαλίδα Διάσπασης) χρησιμοποιείται από την πηγή για να στείλει μεγαλύτερα πακέτα από το MTU (Maximum Transmission Unit-Μέγιστη μονάδα μετάδοσης) του μονοπατιού. Η διάσπαση γίνεται μόνο από τη πηγή και όχι από τους δρομολογητές που βρίσκονται πάνω στη διαδρομή. Οι δρομολογητές δεν σπάνε πακέτα κατά την

διαδρομή αν είναι μεγάλα. Το Authentication Header (Επικεφαλίδα Πιστοποίησης) προσφέρει ένα μηχανισμό ενός κρυπτογραφικού αθροίσματος ελέγχου πάνω σε κάποια μέρη της επικεφαλίδας του IPv6, των επικεφαλίδων επέκτασης και των δεδομένων. Παρέχει, επίσης , επιβεβαίωση της αυθεντικότητας της προέλευσης των δεδομένων και προστασία από τις επαναλήψεις. Το Encapsulation Security Payload (Επικεφαλίδα Ενσωματωμένης Ασφάλειας) είναι η τελευταία και μη κρυπτογραφημένη επικεφαλίδα του πακέτου και δείχνει ότι το υπόλοιπο μέρος του πακέτου είναι κρυπτογραφημένο και προσφέρει πληροφορίες για να αποκρυπτογραφήσει ο προορισμός χωρίς έλεγχο ταυτότητας. Το Destination Options Header χρησιμοποιείται για να μεταφέρει προαιρετικές πληροφορίες που χρειάζεται να εξεταστούν μόνο από τον κόμβο προορισμού του πακέτου. Η δομή του είναι παρόμοια με εκείνη της Hop-by-Hop. Τέλος, το Mobility Header (Επικεφαλίδα Υποστήριξης Κινητών Χρηστών) χρησιμοποιείται για την υποστήριξη κινητών χρηστών του IPv6 δικτύου.



Εικόνα 2 Παράδειγμα κεφαλίδας επέκτασης

(Πηγή: http://flylib.com)

1.2.2 Πρωτόκολλα Δικτύου του IPv6

ICMPv6

Το ICMPv6 (Internet Control Message Protocol version 6) είναι η εφαρμογή του Πρωτόκολλου μηνυμάτων ελέγχου διαδικτύου (ICMP) του IPv6 που ορίζεται από το RFC4443. Το ICMPv6 αποτελεί αναπόσπαστο κομμάτι του IPv6, το οποίο εκτελεί την αναφορά των σφαλμάτων, τις διαγνωστικές λειτουργίες, και έχει ένα πλαίσιο για επεκτάσεις των μελλοντικών αλλαγών. Ένα τύπος μηνύματος του ICMPv6 είναι το Neighbor Discovery Protocol(NDP), το οποίο είναι ένα πρωτόκολλο εντοπισμού του κόμβου στο IPv6 και αντικαθιστά τις λειτουργίες του ARP (Address Resolution Protocol- Πρωτόκολλο αναγωγής διευθύνσεων). Τα

μηνύματα ICMPv6 μπορούν να ταξινομηθούν σε δύο κατηγορίες: τα μηνύματα λάθους και τα μηνύματα πληροφοριών. Τα μηνύματα ICMPv6 μεταφέρονται από τα IPv6 πακέτα, τα οποία έχουν την τιμή 58 στο πεδίο ΕΠΟΜΕΝΗ ΚΕΦΑΛΙΔΑ.

DHCPv6

Το DHCPv6 (Dynamic Host Configuration Protocol version 6- Πρωτόκολλο δυναμικής διευθέτησης υπολογιστών υπηρεσίας έκδοση 6) είναι ένα πρωτόκολλο δικτύου για την διαμόρφωση των IPv6 hosts με τις IP διευθύνσεις, τα προθέματα και άλλα δεδομένα διαμόρφωσης που απαιτούνται για να λειτουργήσει ένα IPv6 δίκτυο. Τα IPv6 hosts μπορούν να δημιουργήσουν IP διευθύνσεις χρησιμοποιώντας auto-configuration (αυτόματη διευθέτηση) ή μπορεί να ανατεθούν δεδομένα διαμόρφωσης με DHCPv6. Τα IPv6 hosts που χρησιμοποιούν auto-configuration μπορούν να ζητήσουν πληροφορίες σχετικά με μια διεύθυνση ή τη διαδρομή. Το DHCPv6 μπορεί να χρησιμοποιηθεί για να αποκτήσει αυτές τις πληροφορίες, ακόμα και αν αυτό δεν χρησιμοποιείται για να ρυθμιστούν οι IP διευθύνσεις. Δεν είναι απαραίτητο για τη διαμόρφωση των hosts με τις διευθύνσεις του DNS (Domain Name System- Σύστημα ονομάτων περιοχών), αλλά μπορεί να ρυθμιστεί χρησιμοποιώντας το NDP.

Κεφάλαιο 2: ΣΥΓΚΡΙΣΗ ΜΕ ΤΟ IPv4

2.1 Κυριότερες διαφορές

Το IPv6 διατηρεί πολλά από τα χαρακτηριστικά της σχεδίασης του IPv4. Το IPv6 διατηρεί τις περισσότερες γενικές λειτουργίες που παρέχονται από το IPv4. Το IPv4 και το IPv6 είναι ασυνδεσμικά, δηλαδή κάθε αυτοδύναμο πακέτο περιέχει μια διεύθυνση προορισμού και δρομολογείται ανεξάρτητα. Το IPv6 αλλάζει όλες τις λεπτομέρειες, διατηρώντας τις βασικές έννοιες του IPv4. Ωστόσο, στις περισσότερες περιπτώσεις, το IPv6 είναι μια συντηρητική επέκταση του πρωτοκόλλου IPv4.

Τα κύρια νέα χαρακτηριστικά του IPv6 μπορούν να είναι τα εξής:

- Διευθυνσιοδότηση
  Το IPv6 χρησιμοποιεί μεγαλύτερο χώρο διευθύνσεων μεγέθους 128 bit, αντί για 32 bit. Ο χώρος διευθύνσεων που προκύπτει είναι τόσο μεγάλος ώστε να ανταποκρίνεται στην συνεχιζόμενη ανάπτυξη του Internet σε όλο τον κόσμο. Έτσι ο κάθε χρήστης μπορεί να έχει πολλαπλές IP διευθύνσεις στις προσωπικές συσκευές του (π.χ. προσωπικοί υπολογιστές, σταθεροί υπολογιστές, κινητά τηλέφωνα),οικιακές συσκευές (π.χ. τηλεοράσεις, συστήματα θέρμανσης), συστήματα πλοήγησης σε μέσα μεταφοράς (π.χ. τρένα, αυτοκίνητα) κλπ.

Όμως, το σημαντικό είναι η κατανομή των διευθύνσεων και όχι η παραγωγή πολλών διευθύνσεων σε αριθμό. Το IPv6 κατανέμει τις διευθύνσεις με ιεραρχικό τρόπο δίχως τα προβλήματα του IPv4, το οποίο παράγει μεγάλο όγκο πληροφοριών για τη δρομολόγηση πάνω στα συστήματα και τις διευθύνσεις που έμειναν αχρησιμοποίητες.

- Απόδοση
  Η δικτυακή απόδοση έχει άμεση σχέση με τη δρομολόγηση των πακέτων. Ο όγκος της πληροφορίας αυξάνεται συνεχώς και σε αυτό συντελούν οι νέες εφαρμογές. Επειδή όμως οι ταχύτητες που υποστηρίζουν τα LAN (Local Area Network- Τοπικό δίκτυο) και τα WAN (Wide Area Network- Δίκτυο ευρείας περιοχής) αυξάνονται, έτσι πρέπει οι λειτουργίες επεξεργασίας και προώθησης των IP πακέτων από τους δρομολογητές να γίνονται ταχύτερα.
  Η απόδοση του IPv6 βελτιώνεται με τη χρήση του πεδίου ΕΤΙΚΕΤΑ ΡΟΗΣ της βασικής κεφαλίδας, το οποίο ζητά συγκεκριμένες απαιτήσεις από τους δρομολογητές για μια διαδρομή. Οι απαιτήσεις αυτές σχετίζονται με την προτεραιότητα, τη καθυστέρηση ή το εύρος ζώνης που ζητούν κάποιες εφαρμογές.

- Ασφάλεια
  Η ανάπτυξη και η εκτεταμένη χρήση του Internet φέρνει καινούργιες απαιτήσεις από τους χρήστες, οι οποίοι ζητούν οι συναλλαγές τους και η πρόσβαση στις πηγές τους να γίνονται με ασφάλεια.
  Το IPv6 διευκολύνει την ομαλή ανταλλαγή πληροφοριών μεταξύ των δικτυακών συσκευών. Ο κάθε κόμβος υποστηρίζει κρυπτογραφικές δυνατότητες κατά την μεταφορά δεδομένων. Ειδικά, το πρωτόκολλο IPsec (IP security- Ασφάλεια IP) είναι υποχρεωτική λειτουργία για κάθε κόμβο του IPv6. Αντίθετα, η υποστήριξη του IPsec είναι προαιρετική για τους κόμβους του IPv4 και απαιτεί την εγκατάσταση κατάλληλου εξοπλισμού. Ακόμη, σε αντίθεση με ότι συμβαίνει σε δίκτυα IPv4, οι μηχανισμοί ασφάλειας σε ένα δίκτυο IPv6 δεν αναιρούνται από τη χρήση άλλων μηχανισμών. Για παράδειγμα, σε δίκτυα IPv4 η χρήση λειτουργιών NAT (Network Address Translation- Μετάφραση διευθύνσεων δικτύου) καταργεί την από άκρο σε άκρο ασφάλεια κατά την ανταλλαγή πληροφοριών

- Αυτόματη Διευθέτηση (Autoconfiguration)
  Οι ρυθμίσεις των IPv4 συστημάτων είναι συνήθως δύσκολες και προβληματικές. Το IPv6 προσφέρει δύο τρόπους αυτόματης διευθέτησης των δικτυακών υπολογιστικών συστημάτων: την stateful και την stateless. Με την stateful οι hosts μπορούν να καθορίζουν διευθύνσεις στα υπολογιστικά συστήματα τις οποίες παίρνουν πριν από μια βάση δεδομένων.

Με την stateless δεν είναι απαραίτητη η παρουσία του host. Κατά την stateless τα συστήματα μπορούν να ρυθμίσουν μόνα τους τις διευθύνσεις με τη βοήθεια του τοπικού IPv6 δρομολογητή.
Η αυτόματη διευθέτηση μειώνει πάρα πολύ το βάρος της εργασίας του διαχειριστή ενός δικτύου και ωφελεί τους χρήστες. Για παράδειγμα, στον τομέα του mobile computing παρέχει τη δυνατότητα στους κινητούς υπολογιστές να αποκτήσουν αυτόματα IP διεύθυνση από οπουδήποτε και αν συνδέονται στο δίκτυο.

- Μετάβαση
  Η τεχνολογία του IPv6 έχει να προσφέρει πολλά στο χώρο των δικτύων και να εξελίξει το Internet δίνοντας του εφόδια για να αντιμετωπίσει τις μελλοντικές προκλήσεις. Η μεγαλύτερη του πρόκληση είναι η μετάβαση του Internet από το πρωτόκολλο IPv4 στο IPv6. Το μεγάλο μέγεθος του Internet καθιστά βέβαιο ότι η μετάβαση δεν θα πραγματοποιηθεί σε μια στιγμή, αλλά θα υπάρχει μια περίοδος συνύπαρξης του IPv4 με το IPv6. Έτσι, το IETF δίνει την δυνατότητα στους διαχειριστές δικτύων να αναβαθμίσουν τα δίκτυά τους. Η συνύπαρξη των δύο πρωτοκόλλων είναι δεδομένη, οπότε δεν είναι απαραίτητη η άμεση και ολοκληρωμένη αναβάθμιση όλων των δικτύων. Κατά την αναβάθμιση θα πρέπει να κρατούνται πολλές λειτουργίες του IPv4 για την επικοινωνία με δίκτυα στα οποία δεν έχει πραγματοποιηθεί η μετάβαση.

2.2 Μοντέλο Διευθυνσιοδότησης

Όπως, και το IPv4, έτσι και το IPv6 αποδίδει μια μοναδική τιμή σε κάθε σύνδεση μεταξύ ενός υπολογιστή και ενός φυσικού δικτύου. Αν ένας υπολογιστής συνδέει τρία φυσικά δίκτυα τότε αποδίδονται σε αυτόν τρεις διευθύνσεις.

Η διευθυνσιοδότηση του IPv6 διαφέρει από τη διευθυνσιοδότηση του IPv4 σε κάποια σημαντικά σημεία, ακόμα και αν έχουν την ίδια προσέγγιση για να αποδίδουν διευθύνσεις υπολογιστών. Πρώτον, αντίθετα από το IPv4, το IPv6 έχει σχεδιαστεί για ιεραρχημένη διευθυνσιοδότηση και CIDR (Classless Inter-Domain Routing- Δρομολόγηση μεταξύ περιοχών χωρίς κλάσεις), ο συνδυασμός των οποίων επιτρέπει την απόδοση διευθύνσεων σε κομμάτια ανάλογα με τις απαιτήσεις του κάθε δικτύου χωρίς σπατάλες. Ένα είδος ιεραρχίας είναι η απόδοση διευθύνσεων ανάλογα με τη γεωγραφική θέση του δικτύου, όμως ο διαχωρισμός αυτός δεν είναι πάντα εφικτός γιατί πολλά δίκτυα παροχής Internet αλλά και εταιριών απλώνονται και σε διαφορετικές ηπείρους. Δεύτερον, το IPv6 υπάρχουν τρεις βασικές κατηγορίες διευθύνσεων, οι οποίες διαφέρουν σημαντικά από τις ειδικές διευθύνσεις του IPv4:

- Unicast διευθύνσεις (Διευθύνσεις μονοεκπομπής)

Είναι ο πιο ευρέως χρησιμοποιούμενος τύπος διεύθυνσης. Η διεύθυνση αντιστοιχεί σε ένα μεμονωμένο υπολογιστή. Ένα πακέτο που στέλνεται σε αυτή τη διεύθυνση δρομολογείται μέσω της συντομότερης διαδρομής προς τον υπολογιστή.

- Multicast διευθύνσεις (Διευθύνσεις πολυεκπομπής)

Μια διεύθυνση τύπου multicast χαρακτηρίζει ένα σύνολο από interfaces (διεπαφή), τα οποία ανήκουν συνήθως σε διαφορετικούς κόμβους. Ένα πακέτο με προορισμό μια τέτοια διεύθυνση παραδίδεται σε όλα τα interfaces. Τέτοιες διευθύνσεις χρησιμοποιούν συνήθως οι εφαρμογές πολυμέσων (π.χ. εφαρμογές τηλεδιάσκεψης).

- Anycast διευθύνσεις (Διευθύνσεις γενικής εκπομπής)

Και αυτός ο τύπος διεύθυνσης χαρακτηρίζει μια ομάδα από interfaces. Οι διευθύνσεις τύπου anycast μοιράζονται τον ίδιο χώρο διευθυνσιοδότησης με τις unicast. Το κύριο χαρακτηριστικό του είναι ότι ένα πακέτο με προορισμό μια τέτοια διεύθυνσης δεν θα αποσταλεί σε όλα τα interfaces, αλλά σε αυτό που βρίσκεται πιο κοντά στον αποστολέα (σύμφωνα με τον υπολογισμό απόστασης των πρωτοκόλλων δρομολόγησης).

Επίσης, οι παρακάτω τρεις τύπου διευθύνσεων είναι Unicast IPv6 διευθύνσεις:

- Global Unicast Address (Παγκόσμια διεύθυνση μονοεκπομπής)

  Η Global Unicast διεύθυνση έχει σχεδιαστεί για να παράγει μια αποτελεσματική υποδομή δρομολόγησης.
- Link-Local Unicast Address (Διεύθυνση μονοεκπομπής τοπικής σύνδεσης)

  Πρόκειται για διευθύνσεις που χρησιμοποιούνται για επικοινωνία μεταξύ των IPv6 κόμβων σε ένα τοπικό δίκτυο. Δεν είναι δρομολογήσιμες και ποτέ ένα router δεν τις προωθεί προς τα έξω. Οι πιθανοί χρήστες τέτοιων διευθύνσεων είναι όσοι συνδέονται σε δίκτυα των οργανισμών μέσω τηλεφωνικών γραμμών.
- Site-Local Unicast Address (Διεύθυνση μονοεκπομπής τοπικού δικτύου)

  Πρόκειται για διευθύνσεις που μπορούν να χρησιμοποιηθούν από ένα οργανισμό χωρίς να υπάρχει η ανάγκη να αποκτήσουν ένα μοναδικό πρόθεμα. Πρόκειται για διευθύνσεις αντίστοιχες με τις NAT διευθύνσεις στο IPv4. Οι Site-Local Unicast διευθύνσεις δεν είναι προσβάσιμες από άλλους δικτυακούς τόπους, χρησιμοποιείται μόνο για τοπική επικοινωνία, και δεν μπορούν να δρομολογηθούν εκτός του site.

2.3 Ασφάλεια στο IPv6

Ο αρχικός σχεδιασμός του IPv4 δεν είχε λάβει υπόψη κάποιο θέμα ασφάλειας γιατί ήθελε να συνδέσει ακαδημαϊκά ιδρύματα. Μετά την μεγάλη εξάπλωση του Διαδικτύου και τη σημασία που απέκτησε από τις επιχειρήσεις και του ηλεκτρονικού εμπορίου, η ασφάλεια έγινε από τις πιο σημαντικές απαιτήσεις του διαδικτύου. Για το λόγο αυτό, η IETF δημιούργησε το IP Security Working Group, γνωστό και ως IPsec (RFC1825), με στόχο να σχεδιάσει μια αρχιτεκτονική ασφάλειας και πρωτόκολλα ασφάλειας, ώστε να παρέχεται ασφάλεια βασισμένη στην κρυπτογραφία για το IPv6.

Το IPsec ορίζει τους μηχανισμούς ασφάλειας που μπορούν να χρησιμοποιηθούν από το IP πρωτόκολλο ανεξαρτήτως έκδοσης ώστε να επιτυγχάνεται η ασφάλεια στο δίκτυο. Ένα σύστημα χρησιμοποιεί το IPsec για να ζητήσει από τους κόμβους να κάνουν χρήση αλγορίθμων και πρωτοκόλλων ασφάλειας. Το IPsec παρέχει τα εργαλεία με τα οποία ένα σύστημα μπορεί να διαπραγματευτεί με άλλα συστήματα, για παράδειγμα, για να έχουν κοινή χρήση σε ένα αλγόριθμο κωδικοποίησης.

Στο IPv6 η ασφάλεια βασίζεται στο επίπεδο IP (IP level Security), δηλαδή οι διαδικασίες ασφάλειας έχουν σκοπό την προστασία του πακέτου από κάθε είδος επίθεσης κατά την πορείας του μέσα στο δίκτυο. Η ασφάλεια που παρέχει το IPv6 δεν μπορεί να καλύψει όλες τις περιπτώσεις επιθέσεων.

Η ασφάλεια στο IPv6 παρέχει τις εξής δυνατότητες:

1) Πιστοποίηση: Πιστοποίηση είναι η ικανότητα να γνωρίζουμε ότι τα δεδομένα που έλαβε ο παραλήπτης είναι αυτά που έστειλε ο αποστολέας και ότι ο αποστολέας είναι αυτός που ισχυρίζεται.
2) Ακεραιότητα πληροφορίας: Η ακεραιότητας της πληροφορίας είναι η δυνατότητα να ανιχνεύεται οποιαδήποτε αλλαγή των δεδομένων στην ενδιάμεση διαδρομή από τον αποστολέα στον παραλήπτη.
3) Απόρρητο της πληροφορίας: Το απόρρητο της πληροφορίας είναι όταν η πληροφορία είναι διαθέσιμη και σε κατανοητή μορφή μόνο από τους πραγματικούς παραλήπτες. Έτσι, είναι σχεδόν ασήμαντο ποιοι μπορούν να υποκλέψουν την πληροφορία κατά την διάρκεια της πορείας της προς τον τελικό προορισμό.
4) Απόδειξη αποστολής των δεδομένων από τον αποστολέα: Με την απόδειξη της αποστολής των δεδομένων από τον αποστολέα δεν γίνεται να αρνηθεί ένας αποστολέας το γεγονός της αποστολής των δεδομένων. Η δυνατότητα αυτή είναι διαθέσιμη μόνο όταν χρησιμοποιείται ένας ασύμμετρος αλγόριθμος κρυπτογράφησης.

2.3.1 Μηχανισμοί ασφάλειας του IPv6

Το IPv6 χρησιμοποιεί δύο μηχανισμούς για να παρέχει τις υπηρεσίες ασφάλειας που αναφέραμε παραπάνω. Οι μηχανισμοί αυτοί βασίζονται κυρίως σε εξωτερικούς μηχανισμούς κρυπτογράφησης για να παρέχουν ασφάλεια. Οι μηχανισμοί αυτοί είναι:

1) IP Authentication Header (IP Επικεφαλίδα Πιστοποίησης)
2) IP Encapsulation Security Payload (IP Επικεφαλίδα Επιλογών Προορισμού)

Κρυπτογραφία θεωρείται η κωδικοποίηση των πληροφοριών με χρήση ενός αλγορίθμου και ενός μυστικού κλειδιού για τη δημιουργία μιας σειράς χαρακτήρων οι οποίοι είναι μη αναγνώσιμοι. Το μυστικό κλειδί είναι ένας μυστικός κωδικός που χρησιμοποιείται για κρυπτογράφηση και αποκρυπτογράφηση ενός μηνύματος. Με τη μέθοδο αυτή, οι χρήστες μπορούν να ανταλλάσουν δεδομένα χωρίς να υπάρχει ο φόβος για κλοπή των δεδομένων τους από τρίτους.

IP Authentication Header

Ο μηχανισμός του IP Authentication Header παρέχει τις εξής δυνατότητες ασφάλειας:

- Πιστοποίηση
- Ακεραιότητα πληροφορίας
- Απόδειξη αποστολής των δεδομένων από τον αποστολέα

Ο μηχανισμός αυτός στο IPv6 προστίθεται ως μια έξτρα επικεφαλίδα όπως φαίνεται στην Εικόνα 3. η επικεφαλίδα αυτή περιέχει μια τιμή η οποία είναι το αποτέλεσμα της εφαρμογής του αλγόριθμου κρυπτογράφησης στο πακέτο.

Βασική επικεφαλίδα IPv6	Επικεφαλίδες επέκτασης	Authentication Header	Επικεφαλίδα Destination Option	TCP επικεφαλίδα	Δεδομένα

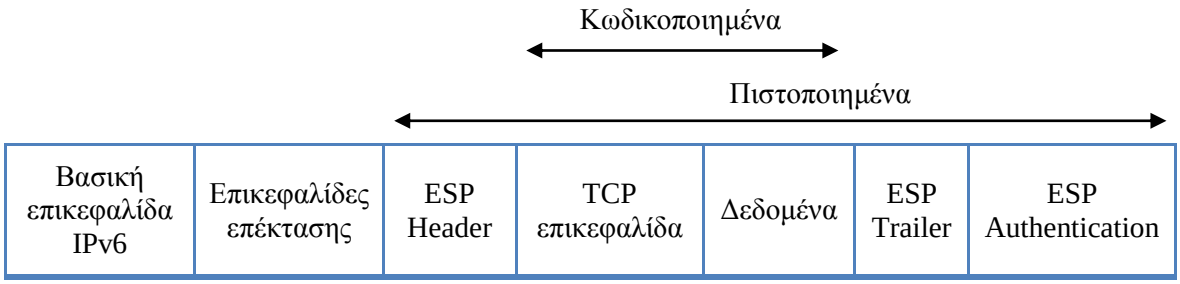
Εικόνα 3 Μορφή IP πακέτου με Authentication Header
(Πηγή: http://www.islab.demokritos.gr)

IP Encapsulation Security Payload

Ο μηχανισμός του IP Encapsulation Security Payload μπορεί να παρέχει τις εξής δυνατότητες ασφάλειας:

- Ακεραιότητα πληροφορίας
- Απόρρητο της πληροφορίας
- Απόδειξη αποστολής των δεδομένων από τον αποστολέα

Η λειτουργία αυτού του μηχανισμού βασίζεται στην κρυπτογράφηση της πληροφορίας που μεταδίδεται. Με αυτό τον τρόπο μόνο ο παραλήπτης που έχει στη κατοχή του το κλειδί μπορεί να αποκρυπτογραφήσει την πληροφορία. Η γενική μορφή ενός πακέτου που χρησιμοποιεί IP Encapsulation Security Payload φαίνεται στην Εικόνα 4.



Εικόνα 4 Μορφή IP πακέτου με IP Encapsulation Security Payload
(Πηγή: http://www.islab.demokritos.gr)

Ο μηχανισμός του Encapsulation Security Payload μπορεί να χρησιμοποιηθεί με δύο τρόπους:

1. Εφαρμογή σε Transport επίπεδο (επίπεδο μεταφοράς)
   Σε αυτή την περίπτωση, μόνο το φορτίο του πακέτου IP είναι συνήθως κρυπτογραφημένο ή/και επικυρωμένο. Η δρομολόγηση του πακέτου είναι άθικτη, αφού η βασική επικεφαλίδα δεν είναι κρυπτογραφημένη και τροποποιημένη, αλλά όταν η Authentication Header χρησιμοποιείται, οι διευθύνσεις IP δεν μπορούν να μεταφραστούν, γιατί θα ακυρωθεί η τιμή κατακερματισμού.
2. Εφαρμογή σε Tunnel επίπεδο (επίπεδο σήραγγας)
   Στο Tunnel επίπεδο ολόκληρο το πακέτο IP είναι κρυπτογραφημένο ή/και επικυρωμένο. Είναι ενθυλακωμένο σε ένα νέο πακέτο IP με μια νέα επικεφαλίδα. Χρησιμοποιείται για τη δημιουργία ιδιωτικών εικονικών δικτύων για επικοινωνίες network-to-network (δίκτυο-σε-δίκτυο), επικοινωνίες host-to-network (δρομολογητής-σε-δίκτυο) και επικοινωνίες host-to-host (δρομολογητής-σε-δρομολογητή).

Οι μηχανισμοί ασφάλειας χρησιμοποιούν την έννοια του Security Association (Ενωση Ασφάλειας). Το Security Association είναι η δέσμη των αλγορίθμων κρυπτογράφησης, πιστοποίησης και παραμέτρων (όπως τα κλειδιά κρυπτογράφησης), που χρησιμοποιείται για την κρυπτογράφηση και τον έλεγχο ταυτότητας μιας ροής σε μια κατεύθυνση. Το Security Association είναι σύνδεση μιας κατεύθυνσης (one-way channel) και υποστηρίζει και παρέχει μια ασφαλή σύνδεση δεδομένων μεταξύ των συσκευών του δικτύου.

Η αύξηση της ασφάλειας αυξάνει και τον υπολογιστικό φόρτο για κάθε πακέτο που δρομολογείται. Σαν αποτέλεσμα έχουμε τη μεγάλη καθυστέρηση της μετάδοσης της πληροφορίας. Ειδικά, η μείωση της απόδοσης του δικτύου είναι μεγαλύτερη για το IP Encapsulation Security Payload. Η μείωση αυτή δεν επηρεάζει τους δρομολογητές που δεν συμμετέχουν στον μηχανισμό ασφάλειας.

2.4 Η απόδοση στο IPv6

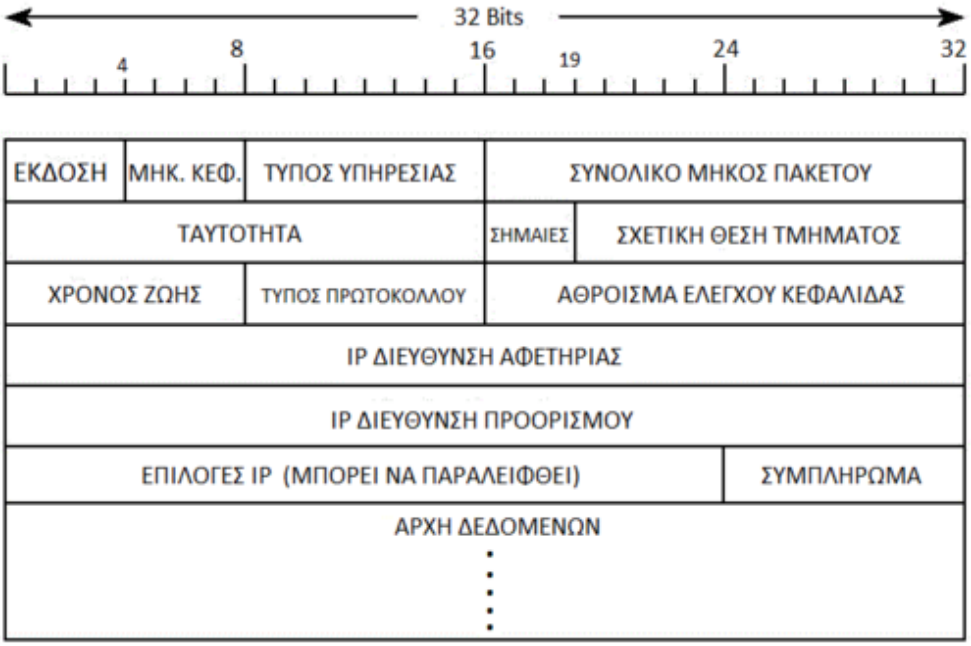
Η αύξηση της απόδοσης του IPv6 έχει δύο βασικές κατευθύνσεις:

- Βελτίωση στην εσωτερική σχεδίαση του πρωτοκόλλου
  Η σχεδίαση του πρωτοκόλλου IPv6 από την αρχή και όχι απλά εξελίσσοντας τον ήδη υπάρχον κώδικα του IPv4 παρέχει πλεονεκτήματα στον τομέα της απόδοση του IPv6.
- Πρόβλεψη για εγγυημένη ποιότητα υπηρεσιών από το δίκτυο Q.o.S. (Quality of Service- Ποιότητα εξυπηρέτησης)
  Η απαίτηση για Q.o.S εμφανίζεται κυρίως λόγω των δικτυακών εφαρμογών πολυμέσων. Οι εφαρμογές αυτές περιλαμβάνουν ήχο, εικόνα και αλληλεπίδραση ανάμεσα στους χρήστες, το οποίο απαιτεί επικοινωνία πραγματικού χρόνου. Αυτό σε σχέση με το δίκτυο μπορεί να σημαίνει δύο πράγματα: α) Ο όγκος των πληροφοριών είναι μεγάλος και στο μεγαλύτερο μέρος τους έχουν ένα σταθερό αριθμό bit κατά την διάρκεια της μετάδοσης και β) η ποιότητα του αποτελέσματος επηρεάζεται σε μεγάλο βαθμό από την καθυστέρηση που μπορεί να υπάρχει στην μεταφορά της πληροφορίας.

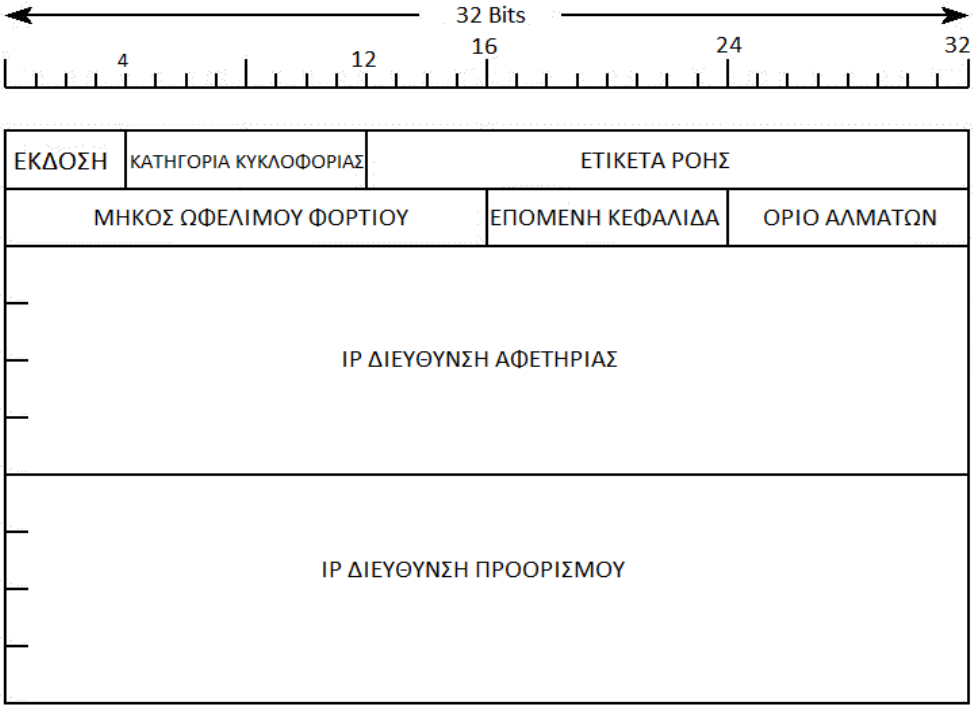
Αυτά τα δύο σημεία κάνουν δύσκολη την χρησιμοποίηση του IPv4, το οποίο έχει σχεδιαστεί για μεταφορά πληροφοριών πραγματικού χρόνου. Τέτοιες εφαρμογές είναι επιθυμητό να χρησιμοποιούν κανάλια με μικρή καθυστέρηση.

2.4.1 Βελτίωση στην εσωτερική σχεδίαση του πρωτοκόλλου

Η πολύχρονη χρήση και βελτίωση του IPv4 οδήγησαν στην απόρριψη χαρακτηριστικών που αποδείχτηκαν μη αποδοτικά ή δεν χρειάζονταν άλλο. Αυτές οι αλλαγές φαίνονται στην Εικόνα 5 και 6 , όπου φαίνεται η καινούργια μορφή της επικεφαλίδας του IPv6 σε σχέση με την υπάρχουσα επικεφαλίδα του IPv4.



Εικόνα 5 Μορφή επικεφαλίδας IPv4
(Πηγή: www.el.wikipedia.org)



Εικόνα 6 Μορφή επικεφαλίδας IPv6
(Πηγή: www.el.wikipedia.org)

Συγκρίνοντας την επικεφαλίδα του IPv6 με την επικεφαλίδα του IPv4 παρατηρούμε την απλοποίηση που έχει γίνει στη μορφή της κρατώντας μόνο τις απαραίτητες πληροφορίες. Έχουμε διπλάσιο μήκος σε bit της επικεφαλίδας IPv6 σε σχέση με το IPv4. Οι επιλογές μπαίνουν σαν επιπλέον επικεφαλίδες που ακολουθούν τη βασική επικεφαλίδα του IPv6 .

Οι σχεδιαστές για να μειώσουν τον χρόνο που ένας δρομολογητής χρειάζεται για να επεξεργαστεί ένα πακέτο φρόντισαν ώστε οι δρομολογητές να επεξεργαστούν το πολύ μια επιλογή και οι υπόλοιπες να ελέγχονται από τον παραλήπτη του πακέτου. Επίσης, το πακέτο πρέπει να ξεκινάει από τον αποστολέα με το κατάλληλο μέγεθος ώστε να είναι δυνατή η μετάδοσή του.

Τέλος, ένας κόμβος IPv6 μπορεί να χειριστεί τα μεγάλα πακέτα IP (Jumbograms) πάνω από το όριο των 65Kb που θέτει το IPv4 και επιτρέπει την καλύτερη εκμετάλλευση των νέων τεχνολογικών δικτύων υψηλών ταχυτήτων, όπως ATM. Η χρήση των Jumbograms μπορεί να βελτιώσει την απόδοση στις συνδέσεις MTU (Μέγιστη μονάδα μετάδοσης).

2.4.2 Ποιότητα εξυπηρέτησης Q.o.S.

Το IPv6 λαμβάνει υπόψη τις νέες απαιτήσεις των νέων εφαρμογών και περιλαμβάνει ειδικές τεχνικές για την επίτευξη της ποιότητας εξυπηρέτησης που επιθυμεί η εφαρμογή αυτή. Το Q.o.S. μπαίνει στην επικεφαλίδα στα πεδία ΚΑΤΗΓΟΡΙΑ ΚΥΚΛΟΦΟΡΙΑΣ και ΕΤΙΚΕΤΑ ΡΟΗΣ.

Το IPv6 χωρίζει την πληροφορία σε κατηγορίες με απαιτήσεις για ποιότητα εξυπηρέτησης και για προτεραιότητα. Τα επίπεδα προτεραιότητας χωρίζονται σε δύο βασικές κατηγορίες:

- Πληροφορίες που έχουν μηχανισμούς αποτροπής κορεσμού του δικτύου (congestion controlled traffic) και περιγράφονται στον Πίνακα 2.
- Πληροφορίες που δεν έχουν μηχανισμούς αποτροπής κορεσμού του δικτύου (non-congestion controlled traffic).
  Αυτή η πληροφορία έχει αριθμούς προτεραιότητας από 8 έως 15. Η μικρότερη προτεραιότητα χρησιμοποιείται για πληροφορία που η απώλεια της θα επηρεάσει λιγότερο σε περίπτωση κορεσμού του δικτύου.

Προτεραιότητα	Τύπος πληροφορίας
0	Μη χαρακτηρισμένη πληροφορία
1	“filler” traffic
2	Μη παρακολουθούμενη μεταφορά μεγάλης ποσότητας δεδομένων
3	Μελλοντική χρήση
4	Παρακολουθούμενη μεταφορά μεγάλης ποσότητας δεδομένων
5	Μελλοντική χρήση
6	Αλληλεπιδραστική πληροφορία
7	Πληροφορία έλεγχου Internet

Πίνακας 2 Επίπεδα προτεραιότητας
(Πηγή: http://www.islab.demokritos.gr)

2.5 Αυτόματη Διευθέτηση (Autoconfiguration)

Το IPv6 προσφέρει την δυνατότητα σε ένα κόμβο να συνδεθεί αυτόματα στο δίκτυο μέσου του σχεδιασμού και των δυνατοτήτων που προσφέρονται για αυτόματη ρύθμιση παραμέτρων μέσω του DHCPv6. Η δυνατότητα αυτή προσφέρεται ακόμα και μέσω της stateless address autoconfiguration. Στο IPv4 η διευθυνσιοδότηση γινόταν χειροκίνητα ή αυτόματα με τη χρήση ενός DHCP. Η διαδικασία της autoconfiguration στο IPv6 περιλαμβάνει τη δημιουργία μιας τοπικής διεύθυνσης και επαλήθευση της μοναδικότητας της σε μια σύνδεση.

Οι hosts του IPv6 μπορούν να ρυθμιστούν αυτόματα όταν συνδέονται σε ένα δίκτυο IPv6 χρησιμοποιώντας το Neighbor Discovery Protocol (NDP) μέσω του ICMPv6. Όταν συνδεθεί σε ένα δίκτυο, ο host στέλνει ένα Link-Local multicast αίτημα σύναψης για τις παραμέτρους διαμόρφωσης του, μετά οι δρομολογητές ανταποκρίνονται στο αίτημα με ένα πακέτο δημοσίευση που περιέχει παραμέτρους διαμόρφωσης Layer Internet (Επίπεδο Διαδικτύου).

Το IPv6 προσφέρει δύο τεχνικές αυτόματης διευθέτησης, οι οποίες παρουσιάζονται πιο αναλυτικά παρακάτω:

- Η stateful address autoconfiguration. Σε αυτό το μοντέλο οι κόμβοι λαμβάνουν τις διευθύνσεις των interfaces (διεπαφών) ή/και τις πληροφορίες διαμόρφωσης από ένα κεντρικό δρομολογητή (DHCPv6). Η stateful χρησιμοποιείται όταν απαιτείται αυστηρός έλεγχος για αναθέσεις διευθύνσεων, αντίθετα με την stateless που χρησιμοποιείται όταν δεν έχει ιδιαίτερα σημασία η ακριβής ανάθεση διευθύνσεων, αφού αυτές είναι μοναδικές. Η stateful χρησιμοποιείται για τη ρύθμιση διευθύνσεων μη τοπικού συνδέσμου μέσω της χρήσης του DHCPv6, το οποίο δεν απαιτεί ρύθμιση παραμέτρων από τον χρήστη.
- Η stateless address autoconfiguration. Οι IPv6 κόμβοι χρησιμοποιούν αυτή τη διαδικασία για να ρυθμίσουν αυτόματα τις IPv6 διευθύνσεις για τα interfaces. Η stateless δημιουργεί κατάλληλα multicast interfaces όταν ο τύπος συνδέσμου multicast είναι ικανός. Δεν απαιτεί καμία χειροκίνητη διαμόρφωση των κόμβων, σχεδόν καθόλου διαμόρφωση των δρομολογητών και κανένα πρόσθετο server. Επιτρέπει σε ένα IPv6 κόμβο να παράγει τη διεύθυνσή του συνδυάζοντας απλά τοπικές διαθέσιμες πληροφορίες και πληροφορίες που διαφημίζονται από τους δρομολογητές.

Οι δύο αυτές τεχνικές αυτόματης διευθέτησης των IP διευθύνσεων μπορούν όμως να αλληλοσυμπληρώνονται. Για παράδειγμα, ένας κόμβος μπορεί να χρησιμοποιεί την stateful προσέγγιση για να λάβει επιπρόσθετες πληροφορίες και τον stateless μηχανισμό για την απόκτηση και διαμόρφωσης της διεύθυνσης του.

Κεφάλαιο 3: ΜΗΧΑΝΙΣΜΟΙ ΜΕΤΑΒΑΣΗΣ

Η μετάβαση από το πρωτόκολλο IPv4 στο πρωτόκολλο IPv6 δεν είναι εύκολη υπόθεση, ειδικά αν αναλογίσει κανείς το μέγεθος του Internet σήμερα, τον τεράστιο αριθμό των χρηστών και των sites. Σε πολλές εταιρίες και οργανισμούς σήμερα είναι αδύνατο να γίνει η μετάβαση στο IPv6 με το κατέβασμα των συστημάτων τους έστω και για λίγο για να γίνει η μετάβαση, γιατί στηρίζονται σημαντικά στο Internet για τη λειτουργία τους και την παροχή των υπηρεσιών.

Η μετάβαση στο IPv6 μπορεί να γίνει σταδιακά. Θα υπάρξει αναγκαστικά ένα μεγάλο χρονικό διάστημα όπου τα δύο πρωτόκολλα θα συνυπάρχουν. Αυτός ήταν άλλωστε και ένας από τους στόχους του IPv6. Οι επιπλέον στόχοι του IPv6 είναι η σταδιακή αναβάθμιση των κόμβων, η σταδιακή εξάπλωση των IPv6 δικτύων, η ευκολία στη διευθυνσιοδότηση των IPv4 κόμβων που αναβαθμίζονται ώστε να υποστηρίζουν και το IPv6, και το χαμηλό κόστος της μετάβασης του IPv4 συστήματος στο IPv6. Έτσι στο διάστημα της μετάβασης οι διαχειριστές θα προχωρούν σταδιακά στην αντικατάσταση του λογισμικού, στις δικτυακές τους συσκευές και κατόπιν στους κόμβους τους. Παράλληλα ο εξοπλισμός αντικαθίσταται από νέα τεχνολογία που θα υποστηρίζει εξαρχής το IPv6.

Η μετάβαση στο IPv6 πρωτόκολλο παραμένει μια χρονοβόρα διαδικασία. Το IPv4 και το IPv6 πρέπει να συνυπάρξουν πολλά χρόνια ακόμα μέχρι να αντικατασταθεί πλήρως το IPv4. Η IETF (Internet Engineering Task Force) έχει αναπτύξει πολλούς μηχανισμούς, σήραγγες και πρωτόκολλα μετάφρασης για να είναι δυνατή η επικοινωνία κατά την διάρκεια της φάσης της μετάβασης που υπολογίζεται ότι θα διαρκέσει αρκετά χρόνια ακόμα, αφού δεν έχει οριστεί η αρχική και η τελική ημερομηνία υλοποίησης της μετάβασης.

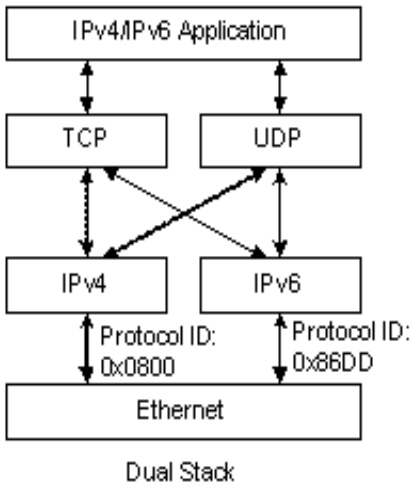
Οι μηχανισμοί μετάβασης είναι τρεις και είναι οι εξής:

1. Dual Stack (Διπλής Στοίβας)
2. Tunneling (Σήραγγας)
3. Protocol translation (Πρωτόκολλο Μετάφρασης)

3.1 Ο Μηχανισμός Dual Stack

Καθώς κατά τη μεταβατική περίοδο οι κόμβοι θα πρέπει να υποστηρίζουν και το IPv4 και το IPv6, στο μηχανισμό Dual Stack (Διπλής Στοίβας), οι κόμβοι του δικτύου υλοποιούν και τις δύο στοίβες των δύο πρωτοκόλλων, δηλαδή συνυπάρχουν πάνω στο ίδιο δίκτυο. Έτσι μπορεί να επιτευχθεί η επικοινωνία τόσο στο IPv4 όσο και στο IPv6.

Για την επιτυχή μετάβαση με το μηχανισμό της Dual Stack, είναι απαραίτητο σε ένα δίκτυο να ενεργοποιηθεί ο μηχανισμός αυτός πρώτα στους δρομολογητές του δικτύου για να εξασφαλίζεται η διασύνδεση, στη συνέχεια στους διάφορους hosts για να προσφέρονται υπηρεσίες και πάνω από το IPv6, και τέλος στους υπολογιστές που ζητάνε τις υπηρεσίες. Εκτός βέβαια από τη ενεργοποίηση της στοίβας του IPv6 παράλληλα με αυτή του IPv4 θα πρέπει να αναβαθμιστούν και οι διάφορες εφαρμογές ώστε να χρησιμοποιούν και τη στοίβα του IPv6.



Εικόνα 7 Ο μηχανισμός Dual Stack
(Πηγή: http://www.h3c.com)

Στην Εικόνα 7 φαίνεται ο μηχανισμός μετάβασης Dual Stack μεταξύ των πρωτοκόλλων IPv4 και IPv6. Όλοι οι κόμβοι και οι συσκευές δικτύου τρέχουν όμοια και στο IPv4 και στο IPv6. Η τιμή στο πεδίο για το Ethernet πληροφορεί τον κόμβο για το ποιό πρωτόκολλο ακολουθεί το πλαίσιο Ethernet. Στην κορυφή του επιπέδου δικτύου, τα πρωτόκολλα μεταφοράς UDP (User Datagram Protocol-Πρωτόκολλο αυτοδύναμων πακέτων χρήστη) ή το πρωτόκολλο μετάδοσης TCP (Transmission Control Protocol-Πρωτόκολλο ελέγχου μετάδοσης) παραμένουν αμετάβλητα και τρέχουν πανομοιότυπα πάνω από το IPv4 και το IPv6.

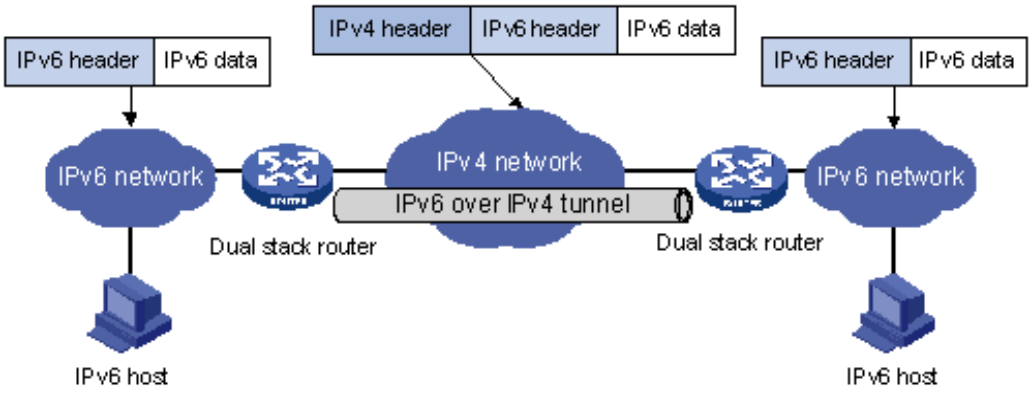
Ένα μειονέκτημα στον μηχανισμό Dual Stack είναι η αυξημένη κατανάλωση μνήμης στους δρομολογητές μιας και χρειάζονται να έχουν δύο πίνακες δρομολόγησης καθώς επίσης και μια μικρή αύξηση της κεντρικής μονάδας επεξεργασίας (Central Processing Unit-CPU) στους δρομολογητές ή στους πυρήνες των κόμβων. Όμως ένα από τα πλεονεκτήματα του είναι η απλότητα στην υλοποίηση τους. Το μόνο που προϋποθέτει είναι εγκατάσταση των δύο πρωτοκόλλων IP στα λειτουργικά συστήματα των μηχανημάτων του δικτύου και έτσι μπορούν να λάβουν αλλά και να προωθήσουν πακέτα και από τα δύο πρωτόκολλα. Στο σημείο αυτό το DNS (Σύστημα ονομάτων περιοχών) κάνει την επιλογή της στοίβας που θα χρησιμοποιηθεί, δηλαδή αν ο κόμβος με τον οποίο θα επικοινωνήσει έχει αποκλειστικά μόνο IPv6 διεύθυνση, θα χρησιμοποιηθεί η IPv6 στοίβα ενώ σε αντίθεση περίπτωση θα χρησιμοποιηθεί η IPv4 στοίβα. Στην

περίπτωση όμως που ο κόμβος έχει και IPv4 και IPv6 διευθύνσεις τότε πρέπει να χρησιμοποιηθεί το IPv6.

3.2 Ο Μηχανισμός Tunneling

Για όσο διάστημα διευρύνεται η χρήση του IPv6 είναι χρήσιμο και αναγκαίο η IPv4 υποδομή να παραμείνει λειτουργική και να χρησιμοποιηθεί επίσης στην μετάδοση φορτίου. Η πιο διαδεδομένη τεχνική, με την οποία γίνεται η εκμετάλλευση της υποδομής του IPv4 για την μεταφορά των IPv6 πακέτων είναι ο μηχανισμός Tunneling, η σημαντικότερη κατηγορία των μηχανισμών μετάβασης.

Το Tunneling είναι μια τεχνική που χρησιμοποιείται σε μεγάλο βαθμό σήμερα και στηρίζεται στην ενθυλάκωση ενός πρωτοκόλλου ενός δικτύου σε πακέτα άλλου πρωτοκόλλου για τη μετάδοση τους πάνω από άλλο δίκτυο. Η τεχνική αυτή χρησιμοποιείται και στο μεταβατικό στάδιο από το IPv4 σε IPv6. Συγκεκριμένα, οι IPv6 hosts και routers έχουν την δυνατότητα να ανταλλάσσουν IPv6 πακέτα, τα οποία ενθυλακώνουν μέσα σε IPv4 πακέτα, μεταδίδοντας τα έτσι πάνω από το υπάρχον δίκτυο. Με αυτόν τον τρόπο οι ενδιάμεσοι δρομολογητές, αν και δεν υποστηρίζουν το IPv6 πρωτόκολλο, προωθούν τα ενθυλακωμένα πακέτα σαν να πρόκειται για κανονικά IPv4 πακέτα. Για τη λειτουργία των μηχανισμών Tunneling πρέπει οι δύο κόμβοι στα άκρα του tunnel να είναι Dual Stack, να έχουν δηλαδή εγκαταστημένες και τις δύο στοίβες πρωτοκόλλων IPv4 και IPv6.



Εικόνα 8 Μηχανισμός Tunneling
(Πηγή: http://www.h3c.com)

Οι μηχανισμοί Tunneling κατηγοριοποιούνται ως προς τον μηχανισμό με τον οποίο ο κόμβος εξόδου, που πραγματοποιεί την ενθυλάκωση, καθορίζει τη διεύθυνση του κόμβου εξόδου. Οι κατηγορίες αυτές είναι το Configured tunneling (Διαμορφωμένο) και το Automatic tunneling (Αυτόματο).

Στο Configured tunneling η IPv4 διεύθυνση του άκρου του τούνελ καθορίζεται από τις διαμορφωμένες (configuration) πληροφορίες που έχουν οριστεί στον κόμβο στον οποίο γίνεται η ενθυλάκωση των πακέτων από τον διαχειριστή του. Για το

κάθε τούνελ που υλοποιεί ο συγκεκριμένος κόμβος πρέπει να υπάρχει αποθηκευμένη η διεύθυνση του άλλου άκρου. Όταν ένα πακέτο μεταδίδεται μέσω του τούνελ, η διεύθυνση του άλλου άκρου, που έχει ρυθμιστεί για το συγκεκριμένο τούνελ, τίθεται ως η διεύθυνση προορισμού στην επικεφαλίδα του IPv4 που ενθυλακώνει το IPv6 πακέτο.

Στο Automatic tunneling η IPv4 διεύθυνση του άκρου του τούνελ μπορεί να προκύψει από την IPv6 διεύθυνση προορισμού του πακέτου που πρόκειται να μεταδοθεί μέσω του τούνελ. Αυτή μπορεί να είναι είτε διεύθυνση 6to4 (βλέπε παρακάτω) είτε διεύθυνση IPv4-compatible (συμβατή) είτε μια διεύθυνση στην οποία το IPv4 εμπεριέχεται με κάποιο τρόπο στην IPv6 διεύθυνση. Στην περίπτωση αυτή, οι IPv4 και IPv6 κόμβοι επικοινωνούν πάνω από την IPv4 υποδομή δρομολόγησης.

Στην κατηγορία των Configured tunneling συγκαταλέγονται τα εξής είδη tunneling:

- Router-to-router tunneling: οι IPv4 ή οι IPv6 routers συνδέονται μεταξύ τους μέσω μιας IPv4 δομής και στέλνουν IPv6 πακέτα μεταξύ τους. Το τούνελ αντιστοιχεί σε ένα μεσαίο τμήμα της συνολικής διαδρομής του IPv6 πακέτου.
- Host-to-router tunneling: οι IPv4 ή οι IPv6 hosts στέλνουν IPv6 πακέτα προς ένα ενδιάμεσο IPv4 ή IPv6 router, στον οποίο έχουν πρόσβαση μέσω μιας IPv4 δομής. Σε αυτήν την περίπτωση το τούνελ αντιστοιχεί στη συνολική διαδρομή.

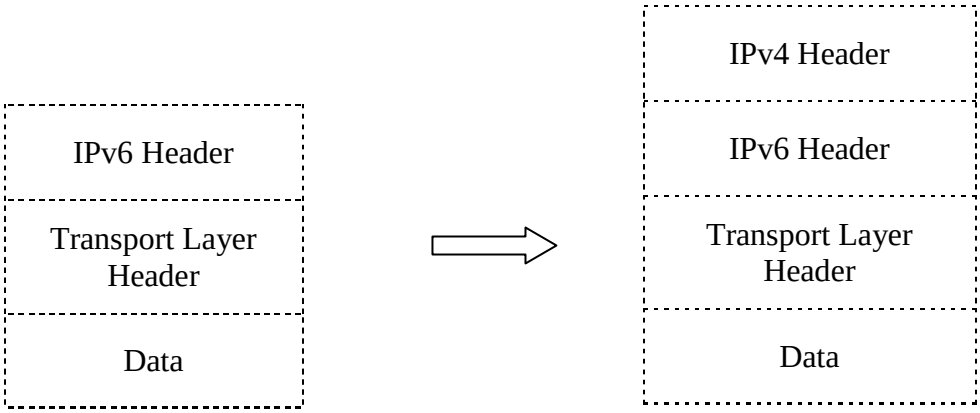
Στην κατηγορία των Automatic tunneling ανήκουν τα εξής είδη tunneling:

- Host-to-host tunneling: οι IPv4 ή οι IPv6 hosts είναι συνδεδεμένοι μεταξύ τους μέσω μιας IPv4 δομής και στέλνουν IPv6 πακέτα μεταξύ τους. Το τούνελ αντιστοιχεί στη συνολική διαδρομή.
- Router-to-host tunneling: το πακέτο μεταδίδεται μέσω του τούνελ μέχρι τον τελικό προορισμό. Σε αυτή την περίπτωση η διεύθυνση προορισμού του IPv6 πακέτου περιέχει τη IPv4 διεύθυνση προορισμού που θα χρησιμοποιηθεί στην επικεφαλίδα του IPv4.

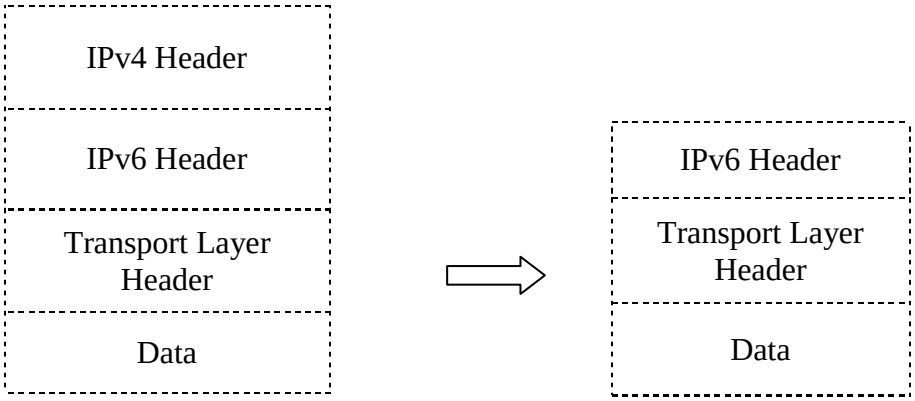
Οι δύο αυτές κατηγορίες tunnel έχουν κοινά χαρακτηριστικά λειτουργίας των μηχανισμών. Ο κόμβος εισόδου και των δύο κατηγοριών δημιουργεί την επικεφαλίδα του IPv4 με τιμή 41 στο πεδίο ΤΥΠΟΣ ΠΡΩΤΟΚΟΛΛΟΥ, κάτω από την οποία ενθυλακώνει το IPv6 πακέτο και δρομολογεί το πακέτο με την δρομολόγηση του IPv4, θέτοντας ως διεύθυνση προορισμού τη IPv4 διεύθυνση του κόμβου εξόδου, όπου θα γίνει η απενθυλάκωση. Στο άλλο άκρο του τούνελ ο κόμβος εξόδου παίρνει το ενθυλακωμένο πακέτο, το επανασυναρμολογεί αν προκύψει ο κατατεμαχισμός του, και αφού δει την τιμή 41 στην επικεφαλίδα του IPv4, την αφαιρεί. Αν η διεύθυνση προορισμού του IPv6 πακέτου είναι

διαφορετική από τη δική του, προωθεί το πακέτο στον προορισμό με την δρομολόγηση του IPv6.

Παρακάτω φαίνεται στην Εικόνα 9 η ενθυλάκωση ενός IPv6 πακέτου σε IPv4 πακέτο που πραγματοποιείται στον κόμβο εισόδου και στην Εικόνα 10 η απενθυλάκωση του πακέτου στο άλλο άκρο του τούνελ.



Εικόνα 9 Ενθυλάκωση IPv6 σε IPv4 πακέτο
(Πηγή: Φιλιππίδης, Δ.Φ. (2005)Μηχανισμοί Μετάβασης Από Το IPv4 Στο IPv6 Πρωτόκολλο Μελέτη Του 6to4 Μηχανισμού Σχεδίαση Και Υλοποίηση της 6to4 MIB. [pdf] Διαθέσιμο στο: http://artemis.cslab.ntua.gr/el_thesis/artemis.ntua.ece/DT2005-0085/DT2005-0085.pdf)



Εικόνα 10 Απενθυλάκωση IPv6 πακέτου
(Πηγή: Φιλιππίδης, Δ.Φ. (2005)Μηχανισμοί Μετάβασης Από Το IPv4 Στο IPv6 Πρωτόκολλο Μελέτη Του 6to4 Μηχανισμού Σχεδίαση Και Υλοποίηση της 6to4 MIB. [pdf] Διαθέσιμο στο: http://artemis.cslab.ntua.gr/el_thesis/artemis.ntua.ece/DT2005-0085/DT2005-0085.pdf)

3.2.1 Ο μηχανισμός automatic tunneling

Οι σημαντικότεροι μηχανισμοί automatic tunneling που έχουν χρησιμοποιηθεί και χρησιμοποιούνται μέχρι σήμερα είναι ο μηχανισμός Tunnel Broker, ο μηχανισμός 6to4, ο μηχανισμός 6over4, ο μηχανισμός ISATAP και ο μηχανισμός Teredo. Παρακάτω περιγράφονται συνοπτικά.

Tunnel Broker

Ο μηχανισμός μετάβασης Tunnel Broker δίνει τη δυνατότητα σε απομακρυσμένους χρήστες, που θέλουν να συνδεθούν στο IPv6 δίκτυο, να ζητήσουν τον ορισμό ενός tunnel μεταξύ του σταθμού τους και του δρομολογητή, προκειμένου να αποκτήσουν πρόσβαση στο εξωτερικό δίκτυο του IPv6, στο οποίο είναι συνδεδεμένος ο δρομολογητής.

Όταν ένας χρήστης επιθυμεί να συνδεθεί στο IPv6 δίκτυο, τότε το δηλώνει στον Tunnel Broker (συνήθως μέσω ενός web interface) και παρέχει τις απαραίτητες διαχειριστικές πληροφορίες. Ο Tunnel Broker, προκειμένου να εξυπηρετήσει το αίτημα του χρήστη, διαλέγει σε ποιον Tunnel Server θα αναθέσει την εξυπηρέτηση του αιτήματος, έπειτα καθορίζει διάφορες παραμέτρους για το τούνελ και καθιστά τη διαμόρφωση (configuration) για τον ορισμό του τούνελ.

Ο μηχανισμός Tunnel Broker παρουσιάζει αρκετά καλή κλιμάκωση και μπορεί να εξυπηρετήσει αρκετά μεγάλο αριθμό χρηστών μεμονωμένων ή αυτούς που ανήκουν σε κάποιο υποδίκτυο. Ο μηχανισμός Tunnel Broker είναι ο απλούστερος τρόπος για τους χρήστες να συνδεθούν στο IPv6 δίκτυο και σήμερα προσφέρεται δωρεάν στις περισσότερες περιπτώσεις. Παρόλο αυτά αδυνατεί να εξυπηρετήσει χρήστες, οι οποίοι χρησιμοποιούν ιδιωτικές IPv4 διευθύνσεις και βρίσκονται πίσω από κάποιο NAT μηχανισμό. Ακόμη υπάρχουν κάποια προβλήματα όσον αφορά την ανακατανομή των δυναμικών IPv4 διευθύνσεων καθώς και κάποια ζητήματα ασφάλειας. Επίσης, ένα άλλο πρόβλημα είναι ότι οι διαχειριστές δεν γνωρίζουν για την ύπαρξη των μηχανισμών.

6to4

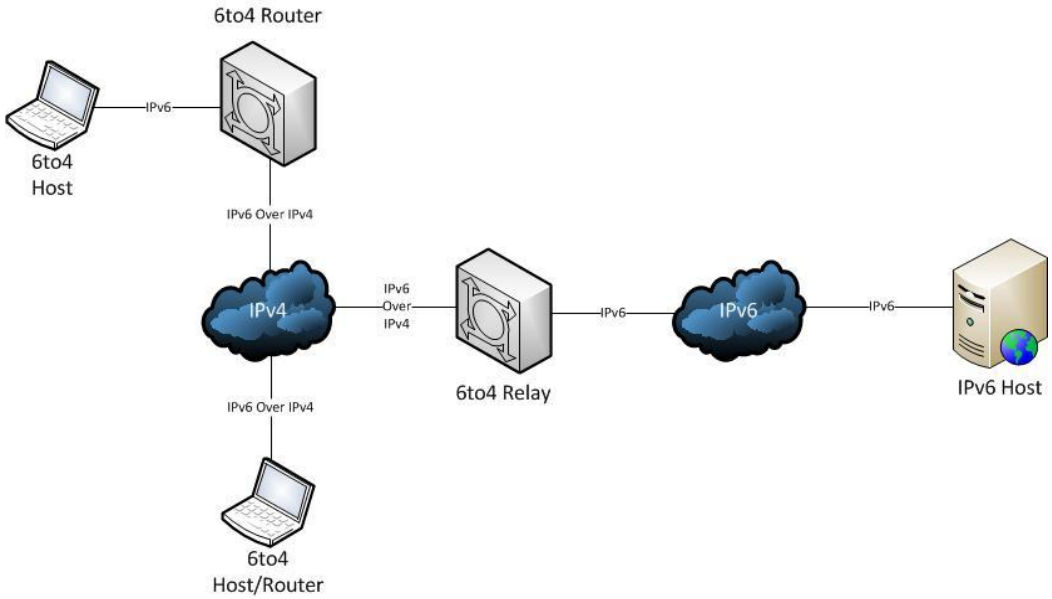
Ο μηχανισμός 6to4 χρησιμοποιείται για την επίτευξη διασύνδεσης IPv6 σταθμών, ακόμα και αν δεν παρέχεται IPv6 υποστήριξη στο δίκτυο στο οποίο και ανήκουν. Χρησιμοποιεί αυτόματο (automatic) tunneling, το οποίο δίνει ευελιξία στον τρόπο εφαρμογής του, αφού αυτό το χαρακτηριστικό του δίνει ελάχιστο διαχειριστικό κόστος. Περιγράφεται από το RFC3056.

Κάθε site που έχει τουλάχιστον μια IPv4 διεύθυνση, μπορεί να κάνει χρήση του μηχανισμού 6to4. Οι IPv6 διευθύνσεις που μπορεί να χρησιμοποιήσει είναι αυτές που παράγονται από το IPv6 πρόθεμα 2002:V4DDr::/48. Οι διευθύνσεις αυτές είναι κανονικές IPv6 διευθύνσεις, και όχι της μορφής των IPv4, και συνεπώς μπορούν να χρησιμοποιηθούν σε διαδικασίες autoconfiguration (αυτόματη διευθέτηση). Δηλαδή όλα τα sites που χρησιμοποιούν το μηχανισμό 6to4

δημιουργούν μια κλάση στο σύνολο των IPv6 διευθύνσεων, οι οποίες αρχίζουν με το πρόθεμα 2002::.

Ένας δρομολογητής με 6to4 που χρησιμοποιείται για να συνδέσει ένα εσωτερικό IPv6 δίκτυο με τον υπόλοιπο IPv6 ¨κόσμο¨ πάνω από την IPv4 υποδομή δικτύου ονομάζεται 6to4 δρομολογητής. Η τεχνική 6to4 χρησιμοποιεί την IPv4 υποδομή για να πετύχει τη διασύνδεση των απομακρυσμένων IPv6 κόμβων. Πιο συγκεκριμένα χρησιμοποιεί το IPv4 δίκτυο σαν ένα unicast σημείο προς σημείο επίπεδο διασύνδεσης και χρησιμοποιώντας τεχνικές ενθυλάκωσης υλοποιεί το IPv6 δίκτυο. Ο δεσμός μεταξύ της IPv4 διεύθυνσης και του IPv6 προθέματος δικτύου κάνουν εύκολη τη ρύθμιση του τούνελ. Δεν υπάρχει ανάγκη να καθοριστεί η IPv4 διεύθυνση προορισμού του τούνελ, αφού η διεύθυνση προορισμού εμπεριέχει ήδη την IPv4 διεύθυνση.

Η σωστή λειτουργία του μηχανισμού 6to4 εξαρτάται από τον τρόπο, με βάση τον οποίο οι σταθμοί επιλέγουν ποια διεύθυνση θα χρησιμοποιήσουν, από αυτές που επιστρέφονται από την υπηρεσία DNS. Δηλαδή, έστω ένας σταθμός που έχει 6to4 διεύθυνση και ρωτάει για την IPv6 διεύθυνση ενός άλλου σταθμού. Εάν η υπηρεσία DNS του επιτρέψει δύο IPv6 διευθύνσεις (μια κανονική και μια 6to4) είναι αναγκαίο ο σταθμός να χρησιμοποιήσει την 6to4 διεύθυνση στην προσπάθεια του να επικοινωνήσει με τον άλλο σταθμό.



Εικόνα 11 Περίπτωση εφαρμογής του μηχανισμού 6to
(Πηγή: http://thelazyadmin.com)

Στην παραπάνω Εικόνα 11 υπάρχει μια τυπική περίπτωση εφαρμογής του μηχανισμού 6to4. Ακόμη παρατηρούμε και άλλες συσκευές που παίζουν το δικό τους ρόλο σε ένα 6to4 δίκτυο. Μια από αυτές είναι το 6to4 relay, το οποίο είναι

ένας δρομολογητής που μπορεί να μεταδώσει την κίνηση μιας 6to4 διεύθυνσης μεταξύ 6to4 δρομολογητών και σταθμών πάνω από μια IPv4 υποδομή. Διευκολύνει την λειτουργία του DNS μιας και ο αναμεταδότης δρομολογητής είναι διασυνδεμένος και με το IPv6 δίκτυο και με το 6to4 δίκτυο.

6over4

Ο μηχανισμός 6over4 περιγράφεται από το RFC2529. Έχει αναπτυχθεί με κύριο σκοπό να επιτρέψει σε κάποιον απομονωμένο σταθμό IPv6, ο οποίος βρίσκεται πάνω σε φυσικό σύνδεσμο (link) χωρίς την παροχή IPv6 υποστήριξης, να γίνει ένα λειτουργικός IPv6 σταθμός με πρόσβαση στο IPv6 δίκτυο.

Ο μηχανισμός 6over4 κάνει χρήση του IPv4 multicast, το οποίο θεωρείται ως το επίπεδο διασύνδεσης (link layer) πάνω από το οποίο δομείται η IPv6 στοίβα. Προκειμένου να χρησιμοποιηθεί η 6over4 μέθοδος, πρέπει το διαχειριστικό τμήμα του IPv4 να υποστηρίζει το multicast. Επίσης, αν απαιτείται να υπάρχει σύνδεση με τα εξωτερικά sites (του IPv6), πρέπει απαραίτητα να υπάρχει και κάποιος δρομολογητής που να εφαρμόζει την ίδια μέθοδο στο σύνδεσμο που συνδέεται με το διαχειριστικό τμήμα του multicast.

Ο μηχανισμός 6over4 είναι εφαρμόσιμος στα όρια του ίδιου site και επειδή δεν χρησιμοποιεί IPv4-compatible (συμβατό) IPv6 διευθύνσεις ή configured (διαμορφωμένο) τούνελ παρέχει μεγάλη ανεξαρτησία, σχετικά με την τεχνολογία των συνδέσμων που χρησιμοποιούνται αλλά και την τοπολογία του IPv6 δικτύου που επιχειρεί να εφαρμοστεί. Ο μηχανισμός 6over4 αναφέρεται συχνά και ως virtual (εικονικό) Ethernet.

Ο τρόπος λειτουργίας της συγκεκριμένης μεθόδου είναι σχετικά απλός. Για κάθε IPv6 LAN (τοπικό δίκτυο) ορίζεται μία multicast session (σύνοδος), στην οποία ¨συμμετέχουν¨ τόσο οι σταθμοί που συμμετέχουν στο IPv6 υποδίκτυο, όσο και ο δρομολογητής που δρομολογεί την κίνηση του υποδικτύου προς τα έξω. Κάθε φορά που υπάρχει ένα IPv6 πακέτο προς μετάδοση, αυτό ενθυλακώνεται σε ένα IPv4 πακέτο και αποστέλλεται στην multicast διεύθυνση που αντιστοιχεί στην multicast session. Το πακέτο αυτό φτάνει σε όλους τους σταθμούς που συμμετέχουν στο IPv6 υποδίκτυο και στο δρομολογητή. Οι σταθμοί και οι δρομολογητές εξετάζουν το IPv6 πακέτο και αν απευθύνεται σε αυτούς, το χειρίζονται κατάλληλα. Αν το πακέτο απευθύνεται σε έναν προορισμό εκτός του υποδικτύου το προωθεί κατάλληλα ο δρομολογητής.

Ο συγκεκριμένος μηχανισμός δεν χρησιμοποιήθηκε σε μεγάλο βαθμό λόγω της απαίτησης του για IPv4 multicast, κάτι που οι περισσότεροι πάροχοι ISP (Internet service provider- υπηρεσία παροχής Internet) και διαχειριστές δεν το παρέχουν. Έτσι, η χρήση του μηχανισμού περιορίστηκε μόνο σε πανεπιστημιακά δίκτυα.

ISATAP

Ο μηχανισμός ISATAP (Intra-Site Automatic Tunnel Addressing Protocol-Πρωτόκολλο διευθυνσιοδότησης αυτόματου τούνελ εντός της ιστοσελίδας) είναι ένας μηχανισμός tunneling για περιπτώσεις χρήσης απομακρυσμένης πρόσβασης και είναι ορισμένο στο RFC4214. Μια συνηθισμένη περίπτωση απομακρυσμένης πρόσβασης είναι όταν το ISATAP χρησιμοποιείται εσωτερικά μέσα σε ένα δίκτυο για να συνδέσει σταθμούς διπλής στοίβας (dual stack) με το ευρύτερο IPv6 Διαδίκτυο. Μέσα σε ένα υποδίκτυο χρειάζεται συνήθως ένας ISATAP δρομολογητής, ο οποίος λειτουργεί ως ISATAP server με σύνδεση στο IPv6 Διαδίκτυο για όλους τους κόμβους στο ISATAP υποδίκτυο που εξυπηρετεί.

Ο μηχανισμός ISATAP αντιμετωπίζει το IPv4 δίκτυο ως ένα επίπεδο διασύνδεσης για το IPv6 και θεωρεί όλους τους κόμβους στο δίκτυο ως δυνητικούς IPv6 δρομολογητές. Είναι αυτόματος μηχανισμός με την έννοια ότι εφόσον έχει στηθεί ένας ISATAP δρομολογητής ή server χρειάζονται μόνο οι κόμβοι που χρησιμοποιούν το μηχανισμό να διαμορφωθούν ώστε να συνδέονται σε αυτόν.

Ένας κόμβος που χρησιμοποιεί ISATAP χρειάζεται ένα IPv6 πρόθεμα μήκους 64 bits για να κατασκευάσει τη διεύθυνσή του. Το πρόθεμα αυτό διαφημίζεται από τον δρομολογητή, ο οποίος πρέπει να εξασφαλίζει ότι το πρόθεμα αυτό δρομολογείται σε αυτόν.

Η βασική διαφορά του μηχανισμού ISATAP από το μηχανισμό 6to4 είναι ότι ο μηχανισμός ISATAP κάνει δυνατή την εσωτερική επικοινωνία στο υποδίκτυο (intra-site), ενώ ο μηχανισμός 6to4 καθιστά δυνατή την επικοινωνία μεταξύ των υποδικτύων (inter-site).

Teredo

Ο μηχανισμός Teredo έχει σχεδιαστεί ως μια ύστατη λύση σε περιπτώσεις όπου άλλοι τρόποι για την επίτευξη IPv6 διασύνδεσης δεν είναι διαθέσιμοι. Ουσιαστικά ο μηχανισμός Teredo απευθύνεται σε κόμβους των οποίων οι πάροχοι του δικτύου δεν είναι διαθέσιμοι να παρέχουν κανένα είδος υποστήριξης για το IPv6.

Ο μηχανισμός Teredo βασίζεται στην απόδοση διεύθυνσης και στην αυτόματη δημιουργία τούνελ για την παροχή IPv6 διασυνδεσιμότητας πάνω από IPv4 δίκτυα. Σκοπός του είναι να καλύψει το κενό που αφήνει ο μηχανισμός 6to4, όταν δεν υπάρχει η δυνατότητα για ένα 6to4 δρομολογητή στην άκρη του IPv6 υποδικτύου, αλλά αντίθετα είναι διαθέσιμη η υποστήριξη του μηχανισμού NAT (Network Address Translation) για διασύνδεση με το Διαδίκτυο.

Ο μηχανισμός Teredo δημιουργεί τούνελ μέσω των οποίων στέλνει την IPv6 κίνηση μεταξύ των συσκευών μέσα στα υποδίκτυα. Το πρόβλημα με τη δημιουργία τούνελ σε αυτή την περίπτωση είναι ότι τα IPv6 πακέτα που ενθυλακώνονται στα IPv4 πακέτα έχουν στο πεδίο ΤΥΠΟΣ ΠΡΩΤΟΚΟΛΛΟΥ την τιμή 41, και η μετάφραση του πρωτοκόλλου 41 δεν είναι ένα συνηθισμένο χαρακτηριστικό των

NAT, με αποτέλεσμα η IPv6 κίνηση να μην μπορεί να περάσει από αυτά. Ο μηχανισμός Teredo ενθυλακώνει τα IPv6 πακέτα ως IPv4 UDP (User Datagram Protocol- Πρωτόκολλο αυτοδύναμων πακέτων χρήστη) μηνύματα με IPv4 και επικεφαλίδες, καθώς τα UDP μηνύματα μπορούν να διαπεράσουν όλα τα NAT. Επομένως, αν ένα NAT υποστηρίζει την μετάφραση των UDP, τότε υποστηρίζεται και ο μηχανισμός Teredo.

Οι Teredo servers είναι κόμβοι που υποστηρίζουν το IPv6 και το IPv4, συνδέονται στο IPv4 δίκτυο και στο IPv6 δίκτυο και διαθέτουν ένα interface (διεπαφή) στο οποίο λαμβάνονται τα πακέτα από το Teredo tunnel. Ο ρόλος τους είναι να βοηθούν στην αρχική επικοινωνία μεταξύ των συσκευών που υποστηρίζουν το Teredo ή μεταξύ μιας Teredo συσκευής και κόμβων που υποστηρίζουν μόνο IPv6.

3.3 Ο Μηχανισμός Translation

Οι μηχανισμοί translation (μετάφρασης) επιτρέπουν την επικοινωνία μεταξύ των κόμβων που υποστηρίζουν μόνο IPv4 και κόμβων που υποστηρίζουν μόνο IPv6 και ουσιαστικά ¨μεταφράζουν¨ την κίνηση από το ένα πρωτόκολλο στο άλλο. Η ιδέα της μετάφρασης των διευθύνσεων των πακέτων σε άλλες δεν είναι καινούρια και μάλιστα αποτελούσε μια από τις κύριες τεχνικές εξοικονόμησης διευθύνσεων στο πρωτόκολλο IPv4. Αναμένεται ότι θα χρησιμοποιηθούν αρκετά στα τελευταία στάδια μετάβασης, και κυρίως για τις περιπτώσεις μηχανημάτων που δεν μπορούν να αναβαθμιστούν στο IPv6.

Συνήθως πρόκειται για ιδέες που είχαν αναπτυχθεί για άλλες δικτυακές εφαρμογές και απλά έχουν μετατραπεί έτσι ώστε να υποστηρίξουν τη διαδικασία μετάβασης στο IPv6. Γενικά οι τεχνικές μετάφρασης μπορούν να χωριστούν στις ακόλουθες κατηγορίες:

- Μετάφραση Επικεφαλίδων (Header Conversion), όπου γίνεται προσπάθεια να μεταφραστούν οι IPv4 επικεφαλίδες σε IPv6 επικεφαλίδες και αντίστροφα. Μοιάζει με το ήδη χρησιμοποιούμενο πρωτόκολλο NAT. Αν και αυτή η τεχνική είναι αρκετά γρήγορη, υπάρχουν κάποια προβλήματα στην εφαρμογή της, όπως ότι δεν μπορεί να κάνει μετάφραση των δικτυακών διευθύνσεων που εμφανίζονται σε επίπεδα εφαρμογής.
- Αναμετάδοση Μεταφοράς (Transport Relay), όπου ένας Εξυπηρετητής Αναμεταδότης (Relay Server) μπαίνει ανάμεσα στον αποστολέα και τον παραλήπτη και αναλαμβάνει να δέχεται τα πακέτα του επιπέδου μεταφοράς από τη στοίβα του ενός πρωτοκόλλου και να τα αναμεταδίδει στην άλλη στοίβα. Πρώτα ένα πακέτο φθάνει στον εξυπηρετητή και το προωθεί προς επεξεργασία στο επίπεδο μεταφοράς. Ο εξυπηρετητής ιδρύει μια σύνοδο με το σταθμό του αποστολέα και μια άλλη με το σταθμό του αποδέκτη, με διαφορετικό πρωτόκολλο η καθεμία. Μετά διαβάζει δεδομένα από τη μια και τα γράφει στην άλλη. Η μια σύνδεση είναι πάνω από τη IPv4 και η

άλλη πάνω από τη IPv6 και η αναμετάδοση λειτουργεί και προς την αντίστροφη κατεύθυνση.

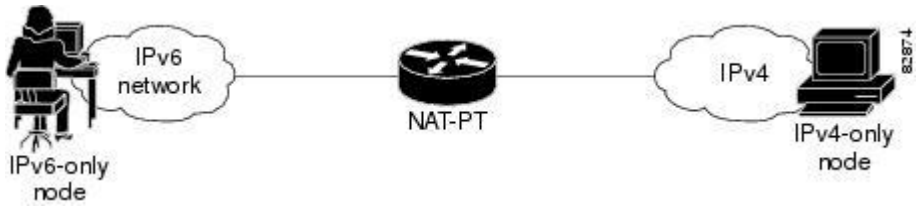
- Πύλη Επιπέδου Εφαρμογών (Application Level Gateway), η οποίο λειτουργεί ως μηχανή caching (κρυφή μνήμη) μεταξύ των εφαρμογών στο IPv4 και στο IPv6 δίκτυο. Προφανώς ο σταθμός που υλοποιεί την Πύλη Επιπέδου Εφαρμογών πρέπει να τρέχει και τα δύο πρωτόκολλα.
- Χαρτογράφηση Διευθύνσεων (Address Mapping), η οποία αναφέρεται στην ένα προς ένα αντιστοίχηση μεταξύ μιας IPv6 διεύθυνσης προορισμού και μιας δεδομένης IPv4 διεύθυνσης προορισμού και αντίστροφα. Το ίδιο γίνεται και για τις διευθύνσεις αποστολής.

Οι κυριότεροι μηχανισμοί αυτής της κατηγορίας είναι ο NAT-PT (Network Address Translation-Protocol Translation- Μετάφραση Διεύθυνσης Δικτύου-Πρωτόκολλο Μετάφρασης), ο οποίος χρησιμοποιεί SIIT (Stateless IP/ICMP Translation) αλγόριθμους για μετατροπή των IPv6 πακέτων σε IPv4 και αντίστροφα, και οι BIS (Bump In The Stack) και BIA (Bump In The API), οι οποίοι εκτελούν τις ίδιες διαδικασίες αλλά ο ένας στο επίπεδο μεταφοράς και ο άλλος στο επίπεδο εφαρμογής.

3.3.1 NAT-PT

Ο μηχανισμός NAT-PT(Network Address Translation-Protocol Translation-Μετάφραση Διεύθυνσης Δικτύου-Πρωτόκολλο Μετάφρασης) έχει οριστεί στο RFC2766 και είναι ένας δρομολογητής ή μεταφραστής από IPv4 σε IPv6 και αντίστροφα. Επιτρέπει σε IPv6 σταθμούς και εφαρμογές να επικοινωνούν με IPv4 σταθμούς και εφαρμογές αντίστοιχα. Ο σταθμός που κάνει τη μετάφραση συνήθως βρίσκεται στα όρια μεταξύ του IPv4 και του IPv6 δικτύου. Όπως φαίνεται και στη Εικόνα 12 ο μηχανισμός NAT-PT αποτελεί τα σύνορο μεταξύ του IPv6 και του IPv4 δικτύου.

Κάθε συσκευή που παίζει το ρόλο του στη μετάφραση διευθύνσεων, διατηρεί μια δεξαμενή (pool) με διευθύνσεις, οι οποίες χρησιμοποιούνται προκειμένου να αποδοθούν δυναμικά σε IPv6 σταθμούς, καθώς δημιουργείται μια σύνοδος (session) μεταξύ των δύο σταθμών που χρησιμοποιούν διαφορετικά πρωτόκολλα. Κάθε μηχανισμός NAT-PT έχει μια ομάδα από δρομολογήσιμες IPv4 διευθύνσεις παγκοσμίως που εκχωρούνται δυναμικά στους IPv6 κόμβους. Παράλληλα, όμως, με την μετάφραση των διευθύνσεων γίνεται και μετάφραση της IPv6 επικεφαλίδας σε IPv4 και αντίστροφα. Οι μηχανισμοί NAT-PT περιέχουν την Πύλη Επιπέδου Εφαρμογών (Application Level Gateway), όπως το IPv4 έχει το NAT ή το firewall.



Εικόνα 12 Ο μηχανισμός NAT-PT
(Πηγή: http://www.cisco.com)

Η εφαρμογή του NAT-PT είναι αρκετά απλή και δεν απαιτεί καμία επιπλέον ρύθμιση από την πλευρά του σταθμού και προσφέρεται σαν υπηρεσία στον χρήστη. Κατά τη διαδικασία της αρχιτεκτονικής του NAT-PT, ο IPv4 κόμβος κάνει ένα DNS ερώτημα για μια IPv4 διεύθυνση και ο μηχανισμός NAT-PT το μεταφράζει σε ένα γενικό ερώτημα για κάθε τύπο διευθύνσεων της ζητούμενης διεύθυνσης. Όταν το DNS ερώτημα λάβει την απάντηση από την IPv6 διεύθυνση, τότε το ερώτημα υποκλέπτεται από το μηχανισμό NAT-PT. Η DNS απάντηση ξαναγράφεται στην IPv4 διεύθυνση από την ομάδα διευθύνσεων του NAT-PT. Ορισμένα από τα μειονεκτήματα του συγκεκριμένου μηχανισμού παρουσιάζουν μεγάλες ομοιότητες με αυτά που συναντάμε και σε άλλες εφαρμογές μετάφρασης επικεφαλίδας. Το βασικό μειονέκτημα του είναι ότι δεν μπορούν να εφαρμοστούν τεχνικές ασφάλειας από άκρο σε άκρο, αφού η διεύθυνση στην οποία θα μεταφραστεί η αρχική διεύθυνση προορισμού δεν είναι από την αρχή γνωστή. Ένα ακόμη μειονέκτημα αποτελεί και το γεγονός ότι η εφαρμογή του απαιτεί τη χρήση ενός χώρου IPv4 διευθύνσεων, που μπορεί να είναι και αρκετά μεγάλο ανάλογα με το φόρτο της χρήσης. Εξαιτίας των μειονεκτημάτων του μηχανισμού και ειδικότερα των μελλοντικών περιορισμών πάνω στην ανάπτυξη των IPv6 δικτύων που δημιουργεί, το NAT-PT σταματάει να συστήνεται ως γενικός μηχανισμός μετάβασης για την επικοινωνία των IPv4 δικτύων και των IPv6 δικτύων.

3.3.1.1 NAPT-PT

Το NAPT-PT (Network Address Port Translation-Protocol Translation-Μετάφραση Διεύθυνσης Θύρας Δικτύου-Πρωτόκολλο Μετάφρασης) είναι ένας μηχανισμός του NAT-PT. Και ο μηχανισμός NAT-PT και ο NAPT-PT είναι απαξιωμένοι μηχανισμοί μετάβασης. Περιγράφεται και αυτό από το RFC2766 και κάνει μετάφραση και των θυρών και των διευθύνσεων. Το NAPT-PT πραγματοποιεί τη μετάφραση από το IPv6 σε IPv4 για τους αριθμούς θύρας του TCP/UDP που βασίζονται στη δυναμική μετάφραση των IP διευθύνσεων.

Το NAPT-PT μπορεί να αντιστοιχίσει διαφορετικές IPv6 διευθύνσεις σε μια IPv4 διεύθυνση. Διαφορετικοί IPv6 hosts διακρίνονται από διαφορετικούς αριθμούς θύρας, έτσι ώστε οι IPv6 hosts μπορούν να συμμερίζονται με μια IPv4 διεύθυνση για να ολοκληρώσει τη μετάφραση των διευθύνσεων. Με αυτό το μηχανισμό αποφεύγονται οι δύο hosts στη μια πλευρά του μηχανισμού από τη χρήση της ίδιας εκτεθειμένης θύρας από την άλλη πλευρά του μηχανισμού, η οποία θα μπορούσε να προκαλέσει την αστάθεια της εφαρμογής ή/και κενά ασφάλειας.

3.3.2 Stateless IP/ICMP Translation (SIIT)

Ο μηχανισμός Stateless IP/ICMP Translation (SIIT) περιγράφεται από το RFC2765. Μεταφράζει τη μορφή της επικεφαλίδας του IPv4 σε IPv6 και αντίστροφα. Ο μηχανισμός SIIT μπορεί να χρησιμοποιηθεί για ένα θέμα που επιτρέπει τους IPv6 hosts να επικοινωνούν μόνο με IPv4 hosts. Δεν μπορεί να εκχωρήσει διευθύνσεις και να δρομολογήσει λεπτομέρειες. Μπορεί να θεωρηθεί μια ειδική περίπτωση του NAT.

3.3.3 Bump In The Stack (BIS)

Ο μηχανισμός Bump In The Stack (BIS) παρεμβαίνει στα IP πακέτα ενός σταθμού μεταξύ της IP στοίβας και της δικτυακής κάρτας, και μεταφράζει από IPv4 σε IPv6 και αντίστροφα, ανάλογα αν είναι εισερχόμενα πακέτα ή εξερχόμενα. Περιγράφεται από το RFC2767.

Πρέπει και στα δύο άκρα μιας σύνδεσης να έχουν εγκατασταθεί συγκεκριμένες μονάδες, προσαρμοσμένες στο λειτουργικό σύστημα που χρησιμοποιείται, οι οποίες θα εκτελούν τη μετάφραση μεταξύ του IPv4 και του IPv6. Αποτελείται από τρεις βασικές μονάδες:

- Μεταφραστής (Translator): Μεταφράζει τα πακέτα από IPv4 σε IPv6 και αντίστροφα.
- Αναλυτής Ονομάτων (Extension Name Resolver): Εξυπηρετεί τα DNS αιτήματα των εφαρμογών.
- Χαρτογράφος Διευθύνσεων (Address Mapper): Διαχειρίζεται τον IPv4 χώρο διευθύνσεων του συστήματος που χρησιμοποιεί το μηχανισμό Bump In The Stack.

3.3.4 Bump In The API (BIA)

Ο μηχανισμός Bump In The API (BIA) λειτουργεί παρόμοια με το μηχανισμό Bump In The Stack, αλλά κάνει τη μετάφραση των εξερχόμενων πακέτων προτού αυτά δημιουργηθούν, επεμβαίνοντας στο API (Application Programming Interface-Διασύνδεση εφαρμογής προγράμματος). Περιγράφεται από το RFC3338.

Και οι δύο μηχανισμοί έχουν το πλεονέκτημα ότι δεν απαιτούν καμία μετατροπή των υπαρχουσών εφαρμογών, και άρα είναι κατάλληλοι για περιπτώσεις όπου δεν υπάρχει ο κώδικας παλιών IPv4 εφαρμογών ώστε να τροποποιηθούν κατάλληλα για το IPv6. Η βασική τους διαφορά είναι ότι ο μηχανισμός Bump In The Stack είναι κατάλληλος για συστήματα χωρίς καθόλου IPv6 στοίβα, ενώ ο μηχανισμός Bump In The API είναι κατάλληλος για συστήματα που διαθέτουν IPv6 στοίβα. Και οι δύο μηχανισμοί έχουν σημαντικούς περιορισμούς, υποστηρίζουν μόνο unicast και όχι multicast επικοινωνία και δεν μπορούν να μεταφράσουν επιλογές του IPv4 σε αντίστοιχες επιλογές του IPv6 και αντίστροφα. Ακόμα, όπως συμβαίνει και με το NAT-PT, χρειάζεται να γίνει μετάφραση των ενσωματωμένων

διευθύνσεων με τη χρήση της κατάλληλης Πύλης Επιπέδου Εφαρμογών (Application Level Gateway).

Επομένως, οι μηχανισμοί Bump In The Stack και Bump In The API είναι σχεδιασμένοι κυρίως για την αρχική φάση της μετάβασης από το IPv4 στο IPv6 και για εφαρμογές του IPv4, οι οποίες για διάφορους λόγους δεν είναι δυνατόν να μετατραπούν ώστε να δουλεύουν με το IPv6.

3.4 Ο Μηχανισμός SOCKS

Ο μηχανισμός SOCKS είναι ένας μηχανισμός πύλης επιπέδου εφαρμογής (application level gateway), ο οποίος υλοποιείται από ένα μηχάνημα που ονομάζεται SOCKS Server και λειτουργεί ως μηχανισμός αναμετάδοσης στο επίπεδο συνόδου TCP ή UDP μεταξύ δύο σταθμών, οι οποίοι χρησιμοποιούν διαφορετικό πρωτόκολλο, ο ένας IPv4 και ο άλλος IPv6.

Για να επιτευχθεί η επικοινωνία μεταξύ των σταθμών, ο ένας πρέπει να είναι πίσω από τον SOCKS Server και ο άλλος να είναι σε δίκτυο εξωτερικά από τον SOCKS Server. Ο σταθμός που βρίσκεται πίσω από τον SOCKS Server εγκαθιστά μια δικτυακή βιβλιοθήκη, η οποία λειτουργεί ως ενδιάμεσο επίπεδο μεταξύ των εφαρμογών και του επιπέδου μεταφοράς (UDP, TCP). Έτσι κάθε φορά που μια εφαρμογή χρησιμοποιεί κάποιες κλήσεις σε socket, αυτές οι κλήσεις προς την εφαρμογή μεταφράζονται στην αντίστοιχη κλήση που υπάρχει στη βιβλιοθήκη, που χρησιμοποιεί ο μηχανισμός και υλοποιεί την σύνδεση με τον απέναντι σταθμό με τη χρήση του SOCKS Server.

Όταν ένας εσωτερικός σταθμός θέλει να δημιουργήσει μια σύνδεση μια κάποιον εξωτερικό σταθμό IPv6 στέλνει ένα αίτημα στον SOCKS Server με όρισμα το Πλήρως Καθορισμένο Όνομα Διαχειριστικού Τμήματος (Fully Qualified Domain Name- FQDN) του IPv6 σταθμού. Ο SOCKS Server βρίσκει την αντιστοίχηση του ονόματος στην IPv6 διεύθυνση και στέλνει μια ψεύτικη IPv4 διεύθυνση στον εσωτερικό σταθμό, η οποία παίζει το ρόλο του αντιπροσώπου του IPv6 σταθμού στον IPv4 σταθμό. Εκείνη τη στιγμή δημιουργούνται δύο συνδέσεις: μια IPv4 TCP μεταξύ του εσωτερικού σταθμού και του SOCKS Server και μια TCP ή UDP IPv6 μεταξύ του SOCKS Server και του εξωτερικού IPv6 σταθμού.

Οι εφαρμογές δεν χρειάζονται καμία μετατροπή προκειμένου να συνεργαστούν με τη συγκεκριμένη τεχνική, αφού όλη η δουλειά γίνεται από το ενδιάμεσο επίπεδο δικτυακών κλήσεων (socket calls) που εγκαθίσταται στον εσωτερικό σταθμό. Το βασικό μειονέκτημα του συγκεκριμένου μηχανισμού είναι πως πάντα οι συνδέσεις πρέπει να αρχικοποιούνται από τους σταθμούς που βρίσκονται πίσω από τον SOCKS Server. Έτσι ο SOCKS θεωρείται ένας μηχανισμός one way (μιας κατεύθυνσης).

3.5 Ο Μηχανισμός Dual Stack Transition Mechanism (DSTM)

Ο μηχανισμός Dual Stack Transition Mechanism (DSTM) έχει αναπτυχθεί για να επιτρέψει την επικοινωνία μεταξύ των IPv6 σταθμών και των IPv4 δικτύων που υπάρχουν σήμερα. Είναι ένας εναλλακτικός τρόπος στις τεχνικές μετάφρασης επικεφαλίδας.

Ο μηχανισμός DSTM βασίζεται στη χρήση ενός DHCPv6 server, ο οποίος αποδίδει προσωρινά παγκόσμιες IPv4 διευθύνσεις στους IPv6 σταθμούς που θέλουν να επικοινωνήσουν με κάποιον IPv4 σταθμό. Τα IPv4 πακέτα ενθυλακώνονται σε IPv6 πακέτα και μεταφέρονται μέσα στο IPv6 δίκτυο μέχρι το συνοριακό δρομολογητή που το διασυνδέει με το IPv4 δίκτυο. Η λειτουργία του μηχανισμού γίνεται με την αρχικοποίηση της επικοινωνίας που μπορεί να γίνει ή από την πλευρά του IPv6 σταθμού ή από την πλευρά του IPv4 σταθμού. Αυτό αποτελεί και σημαντικό πλεονέκτημα του μηχανισμού αυτού σε σχέση με άλλες τεχνικές, οι οποίες επιτρέπουν την επικοινωνία των IPv6 σταθμών με το IPv4 δίκτυο και απαιτούν την αρχικοποίηση της επικοινωνίας μόνο από το IPv6 σταθμό (όπως το SOCKS).

Όταν η επικοινωνία αρχικοποιείται από το IPv6 σταθμό, αυτός ρωτάει την υπηρεσία DNS για τη διεύθυνση του IPv4 σταθμού και από την απάντηση αντιλαμβάνεται ότι πρόκειται για IPv4 σταθμό. Τότε ζητάει από τον DHCPv6 server μια προσωρινή IPv4 διεύθυνση, προκειμένου να τη χρησιμοποιήσει στην επικοινωνία του με το IPv4 σταθμό. Όταν η επικοινωνία αρχικοποιείται από το IPv4 σταθμό, αυτός ρωτάει την υπηρεσία DNS για τη διεύθυνση του IPv6 σταθμού, τότε ο DNS αναγνωρίζει ότι πρόκειται για IPv6 σταθμό, φροντίζει να του αποδοθεί μια IPv4 διεύθυνση, ενημερώνει το IPv6 σταθμό για την προσωρινή IPv4 διεύθυνση και τελικά απαντάει στο σταθμό που αρχικοποίησε την επικοινωνία για τη διεύθυνση αυτή. Η κύρια δυσκολία της εφαρμογής του έχει σχέση με τη μη διαθεσιμότητα του DHCPv6 server, παρόλο που η διαδικασία προτυποποίησης είναι σχετικά πρόσφατη.

3.6 Ο Μηχανισμός Dual-Stack Lite (DS-Lite)

Ο μηχανισμός Dual-Stack Lite (DS-Lite) επιτρέπει σε ένα φορέα παροχής υπηρεσιών να μοιραστεί ο υπάρχον χώρος IPv4 διευθύνσεων και υποστηρίζει τους χρήστες του IPv4 και του IPv6 που χρησιμοποιούν μια IPv6 υποδομή. Αυτό επιτρέπει τη διατήρηση του χώρου των IPv4 διευθύνσεων με την ανάκτηση των διευθύνσεων από το δίκτυο πρόσβασης καθώς μεταβιβάζεται στο IPv6, και μοιράζονται τις υπάρχουσες IPv4 διευθύνσεις μεταξύ της βάσης των χρηστών. Περιγράφεται από το RFC6333.

Σε αντίθεση με άλλες στρατηγικές, ο μηχανισμός Dual-Stack Lite συνδυάζει τον μηχανισμό Tunneling και τις NAT τεχνολογίες, και αποσυνδέει το δίκτυο

πρόσβασης του φορέα παροχής υπηρεσιών από το διαδίκτυο. Αυτά τα χαρακτηριστικά μπορούν να απλοποιήσουν τη μετάβαση στο IPv6, επιτρέποντας τη σταδιακή ανάπτυξη του IPv6, ενώ συνεχίζει να υποστηρίζει τους χρήστες που κατέχουν το IPv4.

Η αρχιτεκτονική του Dual-Stack Lite αποτελείται από το παρακάτω στοιχεία:

- Η Dual-Stack Lite πύλη περιέχει το στοιχείο Basic Bridging Broadband (B4).
- Το Address Family Transition router (AFTR).
- Το 4in6 tunneling συνδέει το στοιχείο B4 με το AFTR.

Ο μηχανισμός Dual-Stack Lite έχει αναπτυχθεί σε όλη την υποδομή του IPv6 και κάνει tunneling στα IPv4 πακέτα με τη χρήση του μηχανισμού tunneling προς το AFTR. Το AFTR επιθεωρεί το IPv6 πακέτο, δείχνει τη IPv4 διεύθυνση προέλευσης και προορισμού, και στη συνέχεια μεταφράζει τη IPv4 διεύθυνση προέλευσης.

Ένα από τα πλεονεκτήματα του Dual-Stack Lite είναι ότι επιτρέπει τη σταδιακή μετάβαση στο IPv6. Παρέχει πρόσβαση στο περιεχόμενο του IPv6 για τους χρήστες, καθώς και υπηρεσίες διαδικτύου για το IPv4. Ο μηχανισμός αυτός μπορεί να εφαρμοστεί σε όλο το περιβάλλον του IPv6 και μπορεί να ανακτήσει το χώρο των IPv4 διευθύνσεων. Οι μηχανισμοί tunneling δημιουργούνται μέσα στο AFTR μετά την παραλαβή ενός έγκυρου IPv6 πακέτου, που έχει οριστεί για επεξεργασία με το μηχανισμό Dual-Stack Lite. Δεν απαιτείται όμως διαμόρφωση του τούνελ.

3.7 Ο Μηχανισμός 6rd

Ο μηχανισμός 6rd (IPv6 Rapid Deployment-Ταχεία Ανάπτυξη του IPv6) διευκολύνει την ταχεία ανάπτυξη του IPv6 στις υποδομές του IPv4 των παροχών υπηρεσιών Διαδικτύου (Internet service providers- ISPs). Περιγράφεται από το RFC5569 και το RFC5969. Ο μηχανισμός αυτός είναι μια παραλλαγή του 6to4, με τη διαφορά ότι λειτουργεί εξ ολοκλήρου εντός του ISP δικτύου του παρόχου, αποφεύγοντας τα σημαντικά προβλήματα δρομολόγησης του 6to4. Χρησιμοποιεί το δικό του IPv6 πρόθεμα αντί του 2002::/16 του μηχανισμού 6to4.

Ο μηχανισμός 6rd χρειάζεται όμως και το IPv4 ανά πελάτη. Επίσης απαιτείται ελαφρώς ο relay router (δρομολογητής αναμετάδοσης) και ο CPE (customer-provided equipment-εξοπλισμός που παρέχεται στον πελάτη)(π.χ. τηλέφωνα, δρομολογητές, αντάπτορες). Η κίνηση προς άλλα 6rd sites γίνεται με ένα 6in4 τούνελ προς μια απομακρυσμένη τοποθεσία, ενώ η κίνηση προς το IPv6 γίνεται με ένα 6in4 τούνελ προς το relay router. Ο relay router ανακοινώνει το πρόθεμα στο IPv6. Ο πάροχος περιορίζει τους χρήστες στους relay routers που επιθυμεί και λύνει έτσι κάποια σχετικά προβλήματα αξιοπιστίας ή ασφάλειας του 6to4.

Ο μηχανισμός 6rd χρησιμοποιεί 32 bits από το χώρο των IPv6 διευθύνσεων για να χαρτογραφήσει ολόκληρο το χώρο των IPv4 διευθύνσεων και να καταναλώνει περισσότερο χώρο διευθύνσεων από το τυπικό με το IPv6 να υποστηρίζεται από όλους τους δρομολογητές του ISP. Αυτό μπορεί να ελαττωθεί αν παραλείψουμε κάποια τμήματα του χώρου των IPv4 διευθύνσεων, και σε ορισμένες περιπτώσεις αναπτύσσοντας πολλαπλές τομείς του 6rd.

3.8 Οι Μηχανισμοί 4in6 και 6in4

Ο μηχανισμός 4in6 επιτρέπει τη δημιουργία σήραγγας του IPv4 δικτύου πάνω στο κορμό του IPv6 δικτύου. Είναι ένας μηχανισμός διαλειτουργίας του Διαδικτύου που επιτρέπει στο πρωτόκολλο IPv4 να χρησιμοποιηθεί σε ένα δίκτυο IPv6. Ο μηχανισμός 4in6 χρησιμοποιεί tunneling για να ενθυλακώσουν στην κυκλοφορία του IPv4 τα configured (διαμορφωμένο) tunnels του IPv6, όπως ορίζεται και στο RFC2473. Το 4in6, όπως και το 6in4, είναι συνήθως μη αυτόματο, αλλά μπορεί να αυτοματοποιηθεί χρησιμοποιώντας πρωτόκολλα όπως το TSP (Tunnel Setup Protocol) που επιτρέπει την εύκολη σύνδεση με ένα Tunnel Broker.

Ο μηχανισμός 4in6 χρησιμοποιεί το IPsec για να ενθυλακώσει τα πακέτα που ανταλλάσσονται μεταξύ του IPv4 δικτύου μέσω ενός κορμού του IPv6. Με την ενθυλάκωση τα πακέτα δρομολόγησης ανταλλάσσονται κατά μήκος του χώρου του IPv6 δικτύου.

Ο μηχανισμός 6in4 χρησιμοποιεί τούνελ για να ενσωματώσουν την κυκλοφορία του IPv6 πάνω από τους διαμορφωμένους IPv4 δεσμούς, όπως ορίζεται στο RFC4213. Η κυκλοφορία του 6in4 στέλνεται μέσω του IPv4 Διαδικτύου μέσα σε IPv4 πακέτα, των οποίων οι επικεφαλίδες έχουν την τιμή 41 στο πεδίο ΤΥΠΟΣ ΠΡΩΤΟΚΟΛΛΟΥ. Στο 6in4, η επικεφαλίδα του IPv4 πακέτου ακολουθείται αμέσως από το IPv6 πακέτο που μεταφέρεται. Η ενθυλάκωση είναι απλώς το μέγεθος της IPv4 επικεφαλίδας των 20 bytes.

Ο μηχανισμός 6in4 δεν έχει χαρακτηριστικά ασφάλειας και έτσι μπορεί κανείς εύκολα να πάρει κάποιο IPv6 πακέτο πλαστογραφώντας την πηγή μιας IPv4 διεύθυνσης από το ένα άκρο του τούνελ και στέλνοντάς το στο άλλο άκρο του τούνελ. Το πρόβλημα αυτό μπορεί να λυθεί εν μέρει με το IPsec .

3.9 Οι Μηχανισμοί NAT64,DNS64 και 464XLAT

Ο μηχανισμός του NAT64 επιτρέπει στα IPv6 hosts να επικοινωνούν με τους IPv4 servers. Ο NAT64 server είναι το τελικό σημείο για μια τουλάχιστον IPv4 διεύθυνση και ένα τμήμα του IPv6 δικτύου των 32 bit. Ο χρήστης του IPv6 ενσωματώνει τη IPv4 διεύθυνση θέλοντας να επικοινωνήσει με τη χρήση αυτών των bits και στέλνει τα πακέτα της προς τη διεύθυνση που προκύπτει. Στη συνέχεια ο NAT64 server δημιουργεί μια αντιστοίχηση NAT μεταξύ της IPv6 διεύθυνσης

και της IPv4 διεύθυνση, που τους επιτρέπει να επικοινωνούν μεταξύ τους. Περιγράφεται από το RFC6146.

Ο μηχανισμός NAT64 εκτελεί τη stateful μετάφραση, η οποία επιτρέπει την επικοινωνία μεταξύ των IPv6 πελατών με τους IPv4 servers με τη χρήση unicast UDP, TCP ή ICMP. Μια ή περισσότερες δημόσιες διευθύνσεις IPv4, που έχουν ανατεθεί στο μηχανισμό NAT64, μοιράζονται μεταξύ των διαφόρων IPv6 χρηστών. Όταν το stateful NAT64 χρησιμοποιείται σε συνδυασμό με το DNS64, δεν απαιτούνται συνήθως αλλαγές από το IPv6 πελάτη ή τους IPv4 servers. Μια stateful μετάφραση είναι κατάλληλη για εγκατάσταση στην πλευρά του χρήστη ή του φορέα παροχής υπηρεσιών, επιτρέποντας στους IPv6 hosts να φτάσουν στους απομακρυσμένους κόμβους του IPv4.

Η λειτουργία του NAT64 μπορεί να θεωρηθεί απλή, σαν ένα router με τουλάχιστον δύο διεπαφές (interfaces). Μια από αυτές είναι συνδεδεμένη σε ένα δίκτυο IPv4 και η άλλη είναι συνδεδεμένη με το δίκτυο IPv6. Τα πακέτα από το δίκτυο IPv6 δρομολογούνται στο δίκτυο IPv4 μέσω αυτού του δρομολογητή. Αυτός ο δρομολογητής εκτελεί όλες τις απαραίτητες μεταφράσεις που απαιτούνται για τη μεταφορά πακέτων από το δίκτυο IPv6 στο IPv4 και αντίστροφα.

Ο μηχανισμός DNS64 περιγράφει ένα DNS server που βρίσκει εγγραφές A (A records) και συνθέτει τις εγγραφές AAAA (AAAA records) από το αρχείο A. Το πρώτο μέρος από τη IPv6 διεύθυνση δείχνει ένα IPv6/ IPv4 μεταφραστή και το δεύτερο μέρος ενσωματώνει τη IPv4 διεύθυνση από την εγγραφή A. Ο μεταφραστής είναι ο NAT64 server. Ο μηχανισμός DNS64 περιγράφεται από το RFC6147.

Ο μηχανισμός DNS64 λειτουργεί για τις περιπτώσεις όπου το DNS χρησιμοποιείται για να βρει την απομακρυσμένη διεύθυνση του host. Ακόμη, αφού ο DNS64 server πρέπει να επιστρέψει τις εγγραφές που δεν προσδιορίζονται από τον ιδιοκτήτη του domain, τότε η επικύρωση του DNSSEC (Domain Name System Security Extensions-Επεκτάσεις ασφάλειας του συστήματος ονομάτων περιοχών) θα αποτύχει σε περίπτωση που ο DNS server δεν είναι ο domain server του ιδιοκτήτη.

Ο μηχανισμός 464XLAT επιτρέπει στους χρήστες του IPv6 δικτύου να έχουν πρόσβαση στις υπηρεσίες του Διαδικτύου του IPv4. Περιγράφεται από το RFC6877. Ο χρήστης χρησιμοποιεί ένα μεταφραστή SIIT για να μετατρέψει τα πακέτα IPv4 σε IPv6 πακέτα, τα στέλνει σε ένα μεταφραστή NAT64, τα οποία μεταφράζει πάλι σε IPv4 και τα στέλνει σε ένα IPv4 server.

Ο μηχανισμός 464XLAT παρέχει περιορισμένη IPv4 συνδεσιμότητα σε ένα IPv6 δίκτυο, συνδυάζοντας το πρωτόκολλο μετάφρασης stateful (RFC6146) και το πρωτόκολλο μετάφρασης stateless (RFC6145). Ο μηχανισμός είναι εύκολος στην εγκατάσταση και σήμερα είναι διαθέσιμο. Είναι αποτελεσματικός στην παροχή

βασικών υπηρεσιών του IPv4 στους καταναλωτές πάνω από το IPv6 δίκτυο πρόσβασης και καθιστά αποτελεσματική τη χρήση των λιγοστών πόρων του IPv4. Δεν είναι όμως υποκατάστατο για το IPv4 ή τις υπηρεσίες του Dual-Stack Lite.

3.10 Οι Μηχανισμοί NAT444 και NAT464

Το Large Scale NAT (LSN-μεγάλης κλίμακας NAT) προσθέτει ένα άλλο στρώμα μετάφρασης, έτσι όπως ακριβώς οι ιδιωτικές διευθύνσεις IPv4, που χρησιμοποιούνται στο εσωτερικό του NAT, μπορούν επίσης να χρησιμοποιηθούν για την εκχώρηση διευθύνσεων στο εξωτερικό του NAT. Το LSN βρίσκεται σε ένα δίκτυο παροχής υπηρεσιών και όχι σε ένα δίκτυο πελατών. Είναι σχεδόν πάντα μια υπηρεσία σε ένα router και όχι μια αυτόματη συσκευή.

Οι μηχανισμοί NAT444 και NAT464 αποτελούν σενάρια χρήσης του LSN και θέτουν τη δημιουργία του Dual-Stack δικτύου για μια εξαντλημένη ομάδα IPv4 διευθύνσεων. Η εστίαση αυτή γίνεται κυρίως για τους παρόχους ευρυζωνικών υπηρεσιών, που πρέπει να γίνεται ώστε να συνεχίσει να εκχωρεί διευθύνσεις σε μεγάλο αριθμό νέων πελατών, όταν δεν υπάρχουν νέες IPv4 διευθύνσεις να χρησιμοποιηθούν.

Ο μηχανισμός NAT444 δεν είναι μια μακροπρόθεσμη λύση για την εξάντληση της IPv4 διεύθυνσης. Θα πρέπει να χρησιμοποιείται μόνο αν είναι απολύτως αναγκαίο, λόγω των μακροπρόθεσμων προοπτικών του κόστους διατήρησης ενός δικτύου NAT444. Οι συνδέσεις κάποιου χρήστη σε δημόσιους server θα περάσουν μέσα από τρεις διαφορετικές domain IPv4 διευθύνσεις: το ιδιωτικό δίκτυο του χρήστη, το ιδιωτικό δίκτυο του μεταφορέα και το δημόσιο Διαδίκτυο.

Ο NAT444 μεταφράζει από μια IPv4 διεύθυνση σε άλλη IPv4 διεύθυνση σε τρίτη IPv4 διεύθυνση. Η προσέγγιση αυτή είναι ενδιαφέρουσα γιατί ο υπάρχον CPE NAT μπορεί να χρησιμοποιηθεί χωρίς τροποποιήσεις. Οι πάροχοι υπηρεσίας δεν πρέπει να επιβάλλουν ειδικές απαιτήσεις εξοπλισμού για τους χρήστες ή να απαιτούν από τους χρήστες να αλλάξουν τον υπάρχον εξοπλισμό.

Ένα θέμα σχετικά με το NAT444 είναι η δυνατότητα των επικαλύψεων των διευθύνσεων μεταξύ του δικτύου του χρήστη και των ιδιωτικών διευθύνσεων που χρησιμοποιούνται από το φορέα παροχής υπηρεσιών. Ένα άλλο θέμα είναι όταν ένας πελάτης θέλει να στείλει κάποιο πακέτο σε άλλο χρήστη από το ίδιο LSN.

Με το μηχανισμό NAT464 τα IPv4 πακέτα που προέρχονται από το δίκτυο των χρηστών μεταφράζονται σε IPv6 πακέτα για την αναμετάδοση μεταξύ των CPE NAT και του LSN, και στη συνέχεια μεταφράζεται πάλι σε δημόσια IPv4 διεύθυνση από το LSN. Όπως στο Dual-Stack Lite, έτσι και στο NAT464, ο πάροχος δεν έχει IPv4 για να δώσει στους πελάτες. Είναι πιο περίπλοκο από το Dual-Stack Lite και λιγότερο επεκτάσιμο και αποδοτικό. Είναι καλύτερο από το NAT444, γιατί ο πάροχος είναι ένα βήμα πιο κοντά στη IPv6 υποδομή. Το CPE

κάνει μια μετάφραση NAT από την ιδιωτική IPv6 του πελάτη σε μια IPv6 που έχει αποδόσει το δίκτυο, αντί για 4in6 τούνελ.

Το πλεονέκτημα στο μηχανισμό NAT464 είναι ότι οι δεσμοί μεταξύ του παρόχου και του πελάτη είναι IPv6, και όχι dual stack, έτσι η εύρεση αρκετών IPv4 διευθύνσεων για τους πελάτες υποχωρεί. Επειδή υποστηρίζει το IPv4-over-IPv6 αντί να υποστηρίζει παράλληλα και το IPv4 και το IPv6, μας φέρνει πιο κοντά σε αυτό το οποίο τελικά θέλουμε, ένα ¨καθαρό¨ IPv6 δίκτυο.

Δεν υπάρχουν συγκρούσεις μεταξύ της IPv6 διεύθυνσης στο εξωτερικό του CPE NAT και τις ιδιωτικές IPv4 διευθύνσεις στο εσωτερικό του CPE NAT. Και αν υποθέσουμε ότι το CPE NAT μεταφράζει τα εισερχόμενα πακέτα σε μια IPv4 διεύθυνση στο εσωτερικό του τοπικού δικτύου, θα πρέπει να υπάρχουν θέματα φιλτραρίσματος που πραγματοποιούν την επικοινωνία μεταξύ δύο πελατών πίσω από τον ίδιο LSN.

Το NAT464 απλοποιεί τα πράγματα στην ενδιάμεση ζώνη μεταξύ του LSN και του CPE NAT, αλλά η σχέση μεταξύ τους είναι πιο προβληματική. Το πρόβλημα είναι ότι αυτές οι δύο συσκευές είναι NAT64 και πρέπει να μεταφραστούν μεταξύ και των δύο εκδόσεων του πρωτοκόλλου. Λίγα CPE NAT υποστηρίζουν το NAT64, έτσι οι πάροχοι που υιοθετούν αυτή τη λύση αντιμετωπίζουν τους απαιτητικούς πελάτες που ζητούν να αλλάξουν τον εξοπλισμό τους.

Το μειονέκτημα του μηχανισμού NAT464 είναι ότι τόσο το CPE NAT όσο και το LSN πρέπει να κάνουν τη μετάφραση μεταξύ του IPv4 και του IPv6, η οποία είναι σύνθετη και παρουσιάζει την απόδοση, την κλιμάκωση και τα προβλήματα πλεονασμού.

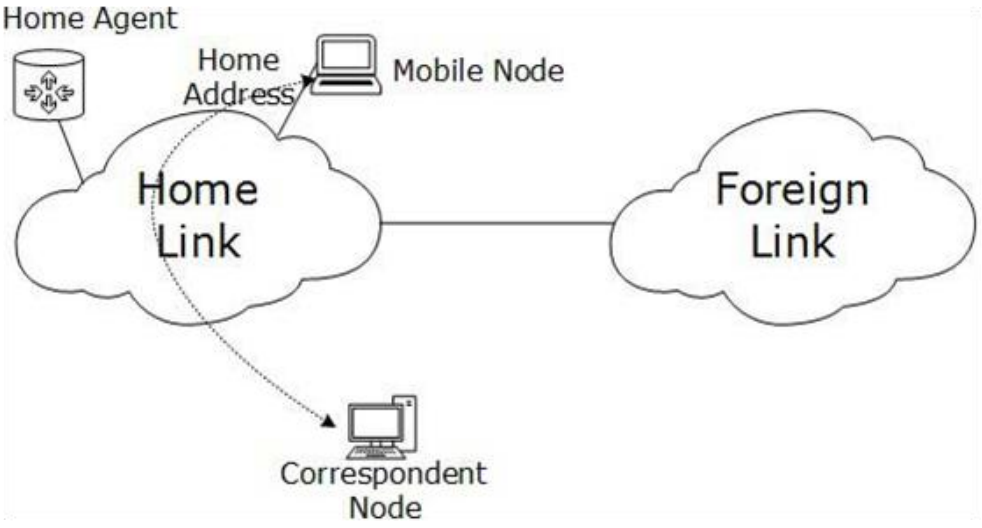
3.11 Οι Μηχανισμοί IPv6 Mobility και IPv6 Routing

Κατά το μηχανισμό IPv6 Mobility (RFC3775) όταν ένας κεντρικός υπολογιστής είναι συνδεδεμένος με ένα δίκτυο, αποκτά μια IP διεύθυνση και όλη η επικοινωνία γίνεται με αυτή τη διεύθυνση σε αυτό το δίκτυο. Μόλις ο host αλλάζει τη θέση του, δηλαδή κινείται σε κάποια διαφορετική περιοχή ή δίκτυο, αλλάζει και η IP διεύθυνση. Όλη η επικοινωνία που συμβαίνει στον host με την παλιά IP διεύθυνση κλείνει, και παρουσιάζονται προβλήματα ειδικά σε εφαρμογές.

Το IPv6 Mobility είναι ο μηχανισμός που δίνει στον κόμβο τη δυνατότητα να περιφέρεται μεταξύ των δικτύων χωρίς να κλείνουν οι τρέχουσες συνδέσεις και διατηρώντας τη IP διεύθυνση. Οι φορείς που συνδέονται με αυτό το μηχανισμό είναι οι παρακάτω.

- Mobile Node (Κινητός κόμβος): Η συσκευή που χρησιμοποιεί IPv6 Mobility.

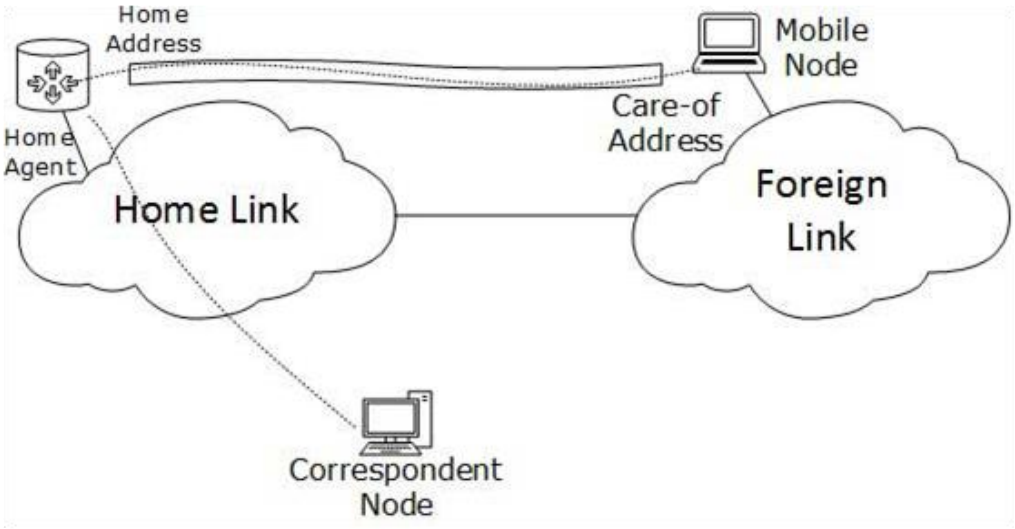
- Home Link (Αρχικός σύνδεσμος): Η σύνδεση αυτή έχει ρυθμιστεί με το αρχικό πρόθεμα υποδικτύου στο τοπικό δίκτυο, όπου ο κόμβος αποκτά τη Home Address.
- Home Address (Αρχική διεύθυνση): Είναι η διεύθυνση που αποκτά ο Mobile Node από το Home Link. Αυτή είναι η μόνιμη διεύθυνση του Mobile Node. Αν ο Mobile Node παραμείνει στο Home Link, η επικοινωνία γίνεται ως συνήθως.
- Home Agent (Αρχικός παράγοντας): Είναι ένα router που λειτουργεί ως καταχωρητής για τα Mobile Node. Είναι συνδεδεμένος στο Home Link και διατηρεί τις πληροφορίες σχετικά με το Mobile Node, τη Home Address και τις τρέχουσες IP διευθύνσεις τους.
- Foreign Link (Εξωτερικός σύνδεσμος): Οποιοδήποτε άλλο τοπικό δίκτυο που συνδέεται ο κόμβος.
- Care-of Address (Διεύθυνση φύλαξης): Όταν ένα Mobile Node βρεθεί σε Foreign Link, παίρνει μια καινούρια IP από το υποδίκτυο του Foreign Link. Ο Home Agent έχει την πληροφορία για τη Home Address και για τη Care-of Address. Ένα Mobile Node μπορεί να έχει πολλαπλές Care-of Address, αλλά μόνο μια Care-of Address είναι δεσμευμένο με τη Home Address.
- Correspondent Node (Κόμβος ανταποκριτής): Μια IPv6 συσκευή που επικοινωνεί με ένα Mobile Node.



Εικόνα 13 Το Mobile Node συνδεδεμένο στο Home Link.
(Πηγή: http://www.tutorialspoint.com)

Όπως φαίνεται και στην Εικόνα 13, όταν ο Mobile Node είναι συνδεδεμένος με το Home Link, όλες οι επικοινωνίες συμβαίνουν στη Home Address. Όταν σε ένα Foreign Link ο Mobile Node αποκτά μια διεύθυνση από το τοπικό δίκτυο, αυτή η διεύθυνση ονομάζεται Care-of Address. Ο Mobile Node στέλνει μια αίτηση δέσμευσης στο Home Agent μαζί με τη νέα Care-of Address. Ο Home Agent

δεσμεύεται με τη Home Address του Mobile Node, εγκαθιδρύοντας ένα τούνελ μεταξύ τους, όπως φαίνεται στην Εικόνα 14. Όταν ένας Correspondent Node επικοινωνεί με το Mobile Node, ο Home Agent προωθεί το πακέτο στη Care-of Address πάνω από το τούνελ.



Εικόνα 14 Το Mobile Node συνδεδεμένο στο Foreign Link.
(Πηγή: http://www.tutorialspoint.com)

Όμως η βελτιστοποίηση της διαδρομής γίνεται όταν ένα Correspondent Node ξεκινήσει την επικοινωνία με την αποστολή πακέτων στη Home Address και στη συνέχεια αυτά διοχετεύονται στο τούνελ από το Home Agent. Όταν ο Mobile Node πάρει το πακέτο από το Correspondent Node, δεν προωθεί τις απαντήσεις στο Home Agent. Στέλνει το πακέτο απευθείας στο Correspondent Node χρησιμοποιώντας τη Home Address. Η λειτουργία αυτή είναι προαιρετική και μη προεπιλεγμένη (default).

Ο μηχανισμός IPv6 Routing είναι η διαδικασία επιλογής της κατάλληλης διαδρομής για να φτάσει ένα πακέτο στον προορισμό του. Ο μηχανισμός αυτός παραμένει ο ίδιος, όμως όλα τα πρωτόκολλα δρομολόγησης έχουν ανασχεδιαστεί κατάλληλα. Τα πρωτόκολλα δρομολόγησης κατηγοριοποιούνται βάσει αλγορίθμου σε δύο κατηγορίες:

1) Distance Vector Routing Protocol (Απόσταση διανύσματος του πρωτοκόλλου δρομολόγησης): Ένας δρομολογητής διαφημίζει τις διαδρομές του και μαθαίνει νέα δρομολόγια από τους γείτονές του. Το κόστος υπολογίζεται ως αριθμός hops μεταξύ της πηγής και του προορισμού. Στηρίζεται στην επιλογή διαδρομής των γειτόνων. Τα πρωτόκολλα RIP και BGP είναι Distance Vector Routing Protocol.
2) Link-State Routing Protocol (Κατάσταση- σύνδεσμος του πρωτοκόλλου δρομολόγησης): Αναγνωρίζει την κατάσταση μιας σύνδεσης και το διαφημίζει στους γείτονές του. Η πληροφορία για νέους συνδέσμους μαθαίνεται από τους γειτονικούς δρομολογητές. Αφού η πληροφορία για

τους συνδέσμους σταθεροποιηθεί τρέχει ο αλγόριθμος για την εύρεση καλύτερων μονοπατιών σε όλους τους διαθέσιμους συνδέσμους. Το πρωτόκολλο OSPF (Open Shortest Path First- άνοιγμα συντομότερης διαδρομής) είναι Link-State Routing Protocol.

Τα πρωτόκολλα δρομολόγησης μπορούν να χωριστούν σε δύο κατηγορίες με βάση την περιοχή λειτουργίας:

1) Interior Routing Protocol (Εσωτερικό πρωτόκολλο δρομολόγησης): Χρησιμοποιείται σε ένα αυτόνομο σύστημα ή οργάνωση για τη διανομή δρομολογίων μεταξύ όλων των δρομολογητών. Για παράδειγμα, τα RIP και OSPF.
2) Exterior Routing Protocol (Εξωτερικό πρωτόκολλο δρομολόγησης): Χρησιμοποιείται μεταξύ δύο διαφορετικών αυτόνομων συστημάτων ή οργανώσεις για τη διανομή πληροφοριών δρομολόγησης. Για παράδειγμα, το BGP.

Τα πρωτόκολλα δρομολόγησης είναι τα εξής:

- RIPng (Routing Information Protocol next generation- πρωτόκολλο δρομολόγησης πληροφοριών επόμενης γενιάς): Είναι ένα Interior Routing Protocol και είναι πρωτόκολλο Distance Vector. Έχει αναβαθμιστεί για να υποστηρίζει το IPv6.
- OSPFv3 (Open Shortest Path First version 3- άνοιγμα συντομότερης διαδρομής έκδοση 3): Είναι ένα Interior Routing Protocol, το οποίο έχει τροποποιηθεί για την υποστήριξη του IPv6. Είναι ένα Link-State πρωτόκολλο.
- BGPv4 (Border Gateway Protocol version 4- πρωτόκολλο συνόρου πύλης έκδοση 4): Είναι το μόνο διαθέσιμο Exterior Routing Protocol. Το BGP είναι ένα Distance Vector Routing Protocol. Το BGPv4 έχει τη δυνατότητα να μεταφέρει πληροφορίες για άλλα πρωτόκολλα εκτός του IPv4.

3.12 Οι Μηχανισμοί IVI και Transport Relay Translation (TRT)

Τα IVI, Transport Relay Translation (TRT-Μεταφορά αναμετάδοσης μετάφρασης) και Tunnel Broker (βλέπε κεφάλαιο 3.2) είναι μηχανισμοί μετάβασης στο IPv6 σε ενημερωτικό στάδιο. Ο μηχανισμός Transport Relay Translation (TRT) ορίζεται στο RFC3142. Είναι σχεδιασμένο για χρήση μόνο σε IPv6 δίκτυα που συνδέονται με εξωτερικά συστήματα IPv4. Το TRT έχει εσωτερικό interface IPv6 και εξωτερικό interface IPv4.

Η μετάβαση μεταξύ του IPv6 και του IPv4 πραγματοποιείται σε επίπεδο μεταφοράς στο σύστημα TRT. Για να χειρίζεται το TRT τις IPv4 συνδέσεις, στηρίζεται στη χρήση ενός DNS μεσολαβητή και το εσωτερικό IPv6 host αναζητά τη IP διεύθυνση προορισμού. Ακόμη, ένα πακέτο με πρόθεμα /64 δρομολογείται μέσω του TRT. Το TRT παίρνει τα πακέτα, τελειώνει τη IPv6 σύνδεση και ανοίγει μια νέα IPv4 σύνδεση στη διεύθυνση, που περιέχεται στα τελευταία 32 bits της αρχικής IPv6 διεύθυνσης. Παρόμοια διαδικασία χρησιμοποιείται για τις επικοινωνίες UDP.

Τα πλεονεκτήματα του μηχανισμού Transport Relay Translation είναι ότι μπορεί να λειτουργήσει με μια παγκόσμια IPv4 διεύθυνση. Δεν γίνονται τροποποιήσεις σε λειτουργίες του IPv4 ή του IPv6. Δεν γίνεται κατακερματισμός ή υπάρχουν προβλήματα με το MTU μονοπάτι. Ο μηχανισμός TRT είναι διαφανής με τους hosts ή τις εφαρμογές και είναι προσαρμόσιμος.

Όμως, όπως και το NAT, αντιμετωπίζει προβλήματα με το ωφέλιμο φορτίο στις ενσωματωμένες IP διευθύνσεις. Δεν υπάρχει πιο εύκολος τρόπος για να επιτρέπει τις συνδέσεις από τους εξωτερικούς IPv4 hosts σε εσωτερικούς IPv6 hosts. Το TRT είναι μονής κατεύθυνσης (από το IPv6 στο IPv4) και η χαρτογράφηση από τη διεύθυνση IPv4 στη IPv6 είναι δύσκολη. Απαιτείται ειδικός κωδικός για την αναμετάδοση ¨μη φιλικών¨ πρωτοκόλλων NAT. Το TRT είναι ένα stateful σύστημα και μια σύνδεση στο στρώμα μεταφοράς πρέπει να περάσει από το ίδιο TRT.

Ο μηχανισμός IVI αναφέρεται στο μηχανισμό μετάφρασης stateless IPv4/IPv6 και ορίζεται από το RFC6219. Ο μηχανισμός είναι συμμετρικός και η επικοινωνία του IPv6 και του IPv4 υποστηρίζεται. Ο μηχανισμός IVI σημαίνει η συνύπαρξη του IPv6 με το IPv4 και η μετάβαση του IPv6.

Επιτρέπει στους hosts σε διαφορετικές διευθύνσεις (IPv4 και IPv6) να επικοινωνούν μεταξύ τους και διατηρεί τη διαφάνεια της διεύθυνσης από άκρο σε άκρο. Είναι παραδοτέο σε παγκόσμιο επίπεδο και έχει αποτελεσματική χρήση των παγκόσμιων IPv4 διευθύνσεων. Είναι ανεξάρτητος μηχανισμός και αναπτύσσεται σταδιακά. Υποστηρίζει την επικοινωνία της αρχικής IPv6 και της αρχικής IPv4 για κάθε IPv6 host (όχι κάθε IPv6 διεύθυνση) και ανταποκρίνεται σε διαφορετικές απαιτήσεις των servers και των πελατών.

Ο μηχανισμός IVI μπορεί να έχει 4 σενάρια ανάπτυξης:

- $1^{ο}$ σενάριο: ένα IPv6 δίκτυο στο IPv4 Διαδίκτυο.
- $2^{ο}$ σενάριο: το IPv4 Διαδίκτυο σε ένα IPv6 δίκτυο.
- $3^{ο}$ σενάριο: ένα IPv6 δίκτυο σε ένα IPv4 δίκτυο.
- $4^{ο}$ σενάριο: ένα IPv4 δίκτυο σε ένα IPv6 δίκτυο.

3.13 Οι Μηχανισμοί 4rd, AYIYA, dIVI και MAP

Τα 4rd, AYIYA, dIVI και MAP είναι μηχανισμοί μετάβασης στο IPv6 σε πρόχειρο στάδιο. Ο μηχανισμός 4rd (IPv4 Residual Deployment- Υπολειμματική Ανάπτυξη του IPv4) επιτρέπει την παροχή των IPv4 υπηρεσιών σε όλο το IPv6 δίκτυο ενός ISP. Είναι παρόμοιας τεχνολογίας tunneling με το μηχανισμό 6rd. Σε αντίθεση λοιπόν με το 6rd, το 4rd έχει στόχο τα προχωρημένα στάδια της μεταβατικής περιόδου από IPv4 σε IPv6,όταν δηλαδή στην πορεία του δικτύου υπάρχουν IPv6 πακέτα και όχι IPv4 πακέτα. Σε αυτά τα δίκτυα το 4rd διατηρεί μια υπολειμματική IPv4 υπηρεσία για τους πελάτες που το χρειάζονται.

Ο μηχανισμός 4rd ανήκει στην ομάδα των μηχανισμών μετάβασης που βασίζονται στο μηχανισμό IP tunneling. Αυτή η προσέγγιση διατηρεί το δίκτυο στη διαφάνεια από άκρο σε άκρο σε IPv4 πακέτα, σε αντίθεση με εκείνα που βασίζονται σε μηχανισμούς μετάφρασης του IPv4 σε IPv6. Όπως και το 6rd, το 4rd χρησιμοποιεί αυτόματες και stateless αντιστοιχίσεις μεταξύ της IPv6 διεύθυνσης και της IPv4 διεύθυνσης. Χρησιμοποιεί δρομολόγια τούνελ μεταξύ των κόμβων του πελάτη.

Ο μηχανισμός 4rd περιλαμβάνει ένα μηχανισμό για να μοιραστούν στατικά οι IPv4 διευθύνσεις μεταξύ πολλών πελατών. Έτσι, σε κάθε 4rd κόμβος ενός πελάτη έχει εκχωρηθεί ένα σύνολο από θύρες, στις οποίες μπορεί να χρησιμοποιήσει ελεύθερα τα TCP, UDP κλπ. Η ανάθεση είναι τέτοια ώστε κανένας πελάτης να μην έχει από τις πρώτες 4.096 θύρες (που έχουν μεγαλύτερη αξία από τις άλλες), ώστε η διαδικασία να είναι αλγοριθμική.

Ο μηχανισμός AYIYA (Anything In Anything- Οτιδήποτε σε οτιδήποτε) είναι ένα πρωτόκολλο δικτύωσης υπολογιστών για τη διαχείριση του πρωτοκόλλου IP tunneling που χρησιμοποιείται ανάμεσα των ξεχωριστών δικτύων πρωτοκόλλου Internet. Χρησιμοποιείται συχνά για τη διέλευση του IPv6 πάνω από μια σύνδεση του IPv4 δικτύου, όταν το NAT μετασχηματίζει ένα ιδιωτικό δίκτυο με μια μόνο IPv6 διεύθυνση, που μπορεί να αλλάζει συχνά λόγω της παροχής του DHCP από το ISP.

Ο μηχανισμός AYIYA έχει τα εξής χαρακτηριστικά:

- Tunneling των πρωτοκόλλων δικτύωσης μέσα σε ένα άλλο IP πρωτόκολλο.
- Διαφανής χειρισμός του NAT.
- Η ασφάλεια των δικτύων παρέχεται εμποδίζοντας τα πακέτα στο τούνελ να είναι επαναλαμβανόμενα ή ψεύτικα.
- Ένα από τα δύο άκρα του τούνελ θα πρέπει να είναι σε θέση να αλλάξει για να παρέχει χαρακτηριστικά κινητικότητας.

Ο μηχανισμός AYIYA μπορεί να χρησιμοποιηθεί για να τροφοδοτήσει κινητά hosts μέσω tunneling της κίνησης από τη Home Address στο Home Agent πάνω από ένα δίκτυο. Κάθε απομακρυσμένο host που επικοινωνεί με το κινητό host δεν

χρειάζεται την υποστήριξη του AYIYA. Όταν ο απομακρυσμένος host υποστηρίζει το AYIYA, θα μπορούσε άμεσα να δημιουργήσει ένα τούνελ με τον κινητό host να ιδρύει το τούνελ. Ο απομακρυσμένος host μπορεί να προσδιορίσει αν ένας host υποστηρίζει το AYIYA υποβάλλοντας ένα ερώτημα στις εγγραφές του DNS και χρησιμοποιεί ένα δημόσιο/ιδιωτικό κλειδί για τον έλεγχο ταυτότητας των πακέτων. Χρησιμοποιώντας το μηχανισμό AYIYA για την παροχή του IPv6 για ένα host παρέχει ήδη κινητικότητα για το σημείο τερματισμού, καθώς μπορεί να χρησιμοποιήσει τη IPv6 διεύθυνση, ανεξάρτητα από τη γεωγραφική τοποθεσία.

Ο μηχανισμός dIVI αναφέρεται σε μια τεχνική μετάφρασης dual stateless IPv4/IPv6. Το dIVI είναι μια επέκταση της 1:1 (ένα προς ένα) stateless μετάφρασης του IPv4/IPv6 (μηχανισμός IVI) με τα χαρακτηριστικά της IPv4 διεύθυνσης και της dual μετάφρασης. Το dIVI-PD, όμως, είναι η περαιτέρω επέκταση του dIVI, το οποίο χρησιμοποιείται στο Wireline (Ενσύρματο) και στο Wireless (Ασύρματο) περιβάλλον πρόσβασης, όπου προτιμάται η αντιπροσωπία του προθέματος (/64 ή μικρότερο).

Ο μηχανισμός dIVI έχει ως στόχο να ωφελήσει τους φορείς του δικτύου (ISP) να μοιράζονται τις δημόσιες IPv4 διευθύνσεις μεταξύ ενός συνόλου πελατών. Παράλληλα, αξιοποιεί το IPv6 στο δίκτυο με έναν τρόπο που κάνει την κυκλοφορία του IPv4 πελάτη να μοιάζει με φυσική κυκλοφορία του IPv6 στο δίκτυο, με αποτέλεσμα να απλοποιηθούν οι λειτουργίες. Σε αντίθεση με το Dual-Stack Lite κλπ, το dIVI δεν απαιτεί καμία stateful NAT και DNS64 στο δίκτυο, έτσι επωφελείται από το χειριστή του δικτύου να μη συναλλάσσεται με οποιαδήποτε καταγραφή του NAT κλπ. Το dIVI διατηρεί τη διαφάνεια της στην από άκρο σε άκρο διεύθυνση και την αρχική αμφίδρομης επικοινωνίας.

Ο μηχανισμός MAP (Mapping of Address and Port- Χαρτογράφηση της διεύθυνσης και της θύρας) είναι ένας μηχανισμός μετάβασης στο IPv6, ο οποίος συνδυάζει τη A+P (Address plus Port- Διεύθυνση συν Θύρα) μετάφραση διεύθυνση και θύρας με το tunneling των πακέτων του IPv4 πρωτοκόλλου πάνω από ένα φορέα ISP του εσωτερικού IPv6 δικτύου.

Ο μηχανισμός MAP χρησιμοποιεί τα επιπλέον διαθέσιμα bits στη IPv6 διεύθυνση για να περιέχουν τα επιπλέον bits της θύρας του A+P, τα οποία δεν μπορούν να κωδικοποιηθούν στη IPv4 διεύθυνση. Έτσι, καταργείται εντελώς η ανάγκη για τη ¨δρομολόγηση της θύρας¨ μέσα στο φορέα του δικτύου, αξιοποιώντας την εγκατάσταση του IPv6 του φορέα. Ουσιαστικά, το MAP είναι μια σχεδόν stateless εναλλακτική λύση για το LSN NAT και το Dual-Stack Lite, που ωθεί τη λειτουργία της μετάφρασης της IP διεύθυνσης/θύρας του IPv4 εξολοκλήρου στο υπάρχον CPE της εφαρμογής IPv4 NAT. Αποφεύγει έτσι το NAT444 και τα stateful προβλήματα του LSN NAT στο χειριστή του δικτύου και παρέχει ένα μηχανισμό μετάβασης για την ανάπτυξη των αρχικών IPv6 με μια μικρή προστιθέμενη πολυπλοκότητα.

Υπάρχουν δύο τρόποι λειτουργίας του συνολικού πλαισίου του MAP. Ο ένας είναι ο MAP-T, ο οποίος χρησιμοποιεί τη μετάφραση του πρωτοκόλλου για τη μεταφορά της IPv4 κυκλοφορίας. Ο άλλος τρόπος είναι ο MAP-E, ο οποίος χρησιμοποιεί την ενθυλάκωση. Το MAP-T έχει ως αποτέλεσμα τη stateless λειτουργία του NAT64 στο CPE router και στα άκρα του router, ενώ το MAP-E έχει ως αποτέλεσμα τη stateless ενθυλάκωση των πακέτων του IPv4-over-IPv6 στο CPE router και στα άκρα του router. Φυσικά, και οι δύο τρόπο αφήνουν τη stateful NAT44 στο CPE router.

3.14 Ο Μηχανισμός Tunnel Setup Protocol (TSP)

Το Tunnel Setup Protocol (TSP- Πρωτόκολλο ρύθμισης του τούνελ) είναι ένας μηχανισμός μετάβασης στο IPv6 σε πειραματικό στάδιο. Το TSP είναι ένα πρωτόκολλο ελέγχου δικτύωσης που χρησιμοποιείται για να διαπραγματευτεί τις παραμέτρους ρύθμισης του IP τούνελ μεταξύ του host τούνελ του πελάτη και του tunnel broker server. Ο μηχανισμός ορίζεται στο RFC5572.

Το TSP επιτρέπει τη δημιουργία τούνελ των διαφόρων εσωτερικών πρωτοκόλλων μέσα σε διάφορα εξωτερικά πακέτα πρωτοκόλλων. Χρησιμοποιείται από τον πελάτη του τούνελ για να διαπραγματευτεί το τούνελ με το broker. Ένας κινητός κόμβος με την εφαρμογή TSP μπορεί να συνδεθεί με το IPv4 δίκτυο και το IPv6 δίκτυο είτε πρόκειται για το IPv4 είτε για το IPv6. Ένα tunnel broker μπορεί να τερματίσει τα τούνελ στα κινητά τούνελ servers.

Ο μηχανισμός TSP περιλαμβάνει τη διέλευση του NAT (όπως το Teredo), αλλά αν έχει ο χρήστης μια δημόσια IPv4 διεύθυνση, τότε η διέλευση του NAT δεν χρησιμοποιείται. Το TSP βασίζεται κατά βάθος στο μηχανισμό 6in4. Έχει προστεθεί και ένας επιπλέον μηχανισμός για να επιτρέπει την αυτόματη δημιουργία τούνελ, μαζί με την πιστοποίηση.

Ο μηχανισμός TSP υποστηρίζει συνοπτικά τις παρακάτω λειτουργίες:

- Έλεγχος ταυτότητας του χρήστη στο tunnel broker.
- Υποστηρίζει τρεις μηχανισμούς τούνελ:
    - Το IPv6 over IPv4 τούνελ. Απαιτεί δημόσιες IPv4 διευθύνσεις σε κάθε άκρο.
    - Το IPv4 in IPv6 τούνελ.
    - Το IPv6 over UDP/IPv4 τούνελ με ενσωματωμένη διέλευση του NAT.
- Εκχώρηση της IP διεύθυνσης και για τα δύο άκρα του τούνελ.
- Διαπραγμάτευση των πρωτοκόλλων δρομολόγησης.
- Εκχώρηση του προθέματος της IPv6 διεύθυνσης για τους δρομολογητές.
- Καταχώρηση του DNS για τα τελικά σημεία του τούνελ.

- Διαπραγμάτευση για τον ενεργό μηχανισμό τούνελ.
- Προσδιορισμός της ανάγκης για τη διέλευση του NAT.

Υπάρχουν τέσσερις χωριστές συνιστώσες στο TSP:

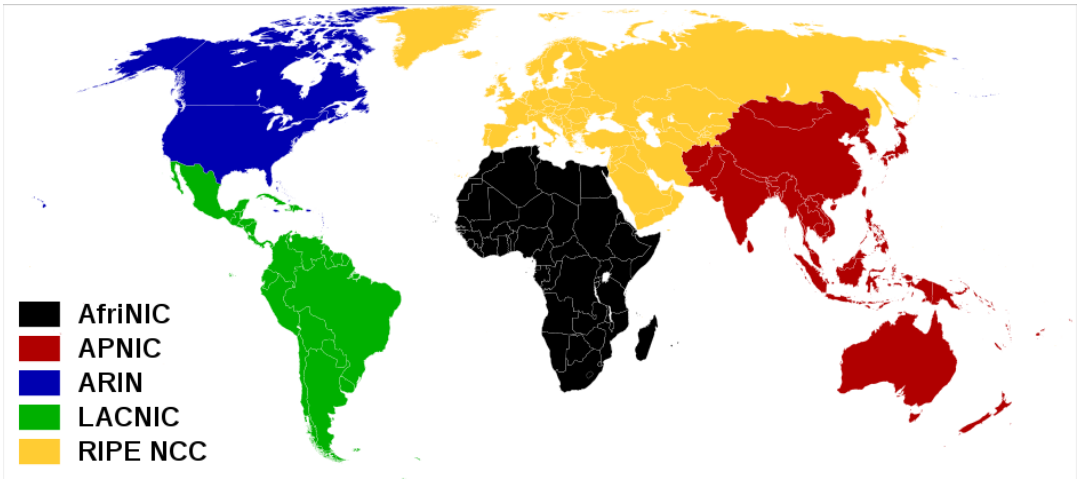
- Ο πελάτης του TSP.
- Ο πελάτης του τελικού σημείου του τούνελ.
- Ο server του TSP.
- Ο server του τελικού σημείου του τούνελ.

Κεφάλαιο 4: ΜΕΤΡΗΣΗ ΤΗΣ ΤΡΕΧΟΥΣΑΣ ΚΑΤΑΣΤΑΣΗΣ ΤΟΥ IPv6 ΠΡΩΤΟΚΟΛΛΟΥ

Όπως έχουμε ήδη αναφερθεί, το Internet Protocol version 6 (IPv6) είναι η επόμενη γενιά του πρωτοκόλλου του Internet, το οποίο αναπτύχθηκε και εξαπλώθηκε εξαιτίας της εξάντλησης του αποθέματος των μη διαθέσιμων IPv4 διευθύνσεων, που έχει προβλεφθεί από τα τέλη της δεκαετίας του 1980. Ο χώρος των IP διευθύνσεων διαχειρίζεται από το IANA (Internet Assigned Numbers Authority-Αρχή των εκχωρημένων αριθμών του Internet) και από το RIR (Regional Internet Registry-Περιφερειακά μητρώα του Internet) σε παγκόσμιο επίπεδο.

Το RIR είναι ένας οργανισμός που διαχειρίζεται την κατανομή και την καταγραφή των πηγών του Διαδικτύου μέσα σε μια συγκεκριμένη γεωγραφική περιοχή. Οι πηγές του Διαδικτύου περιλαμβάνουν IP διευθύνσεις και αριθμούς των αυτόνομων συστημάτων (AS). Το σύστημα του RIR εξελίχτηκε με την πάροδο του χρόνου και τελικά ¨χώρισε¨ τον κόσμο σε πέντε RIR:

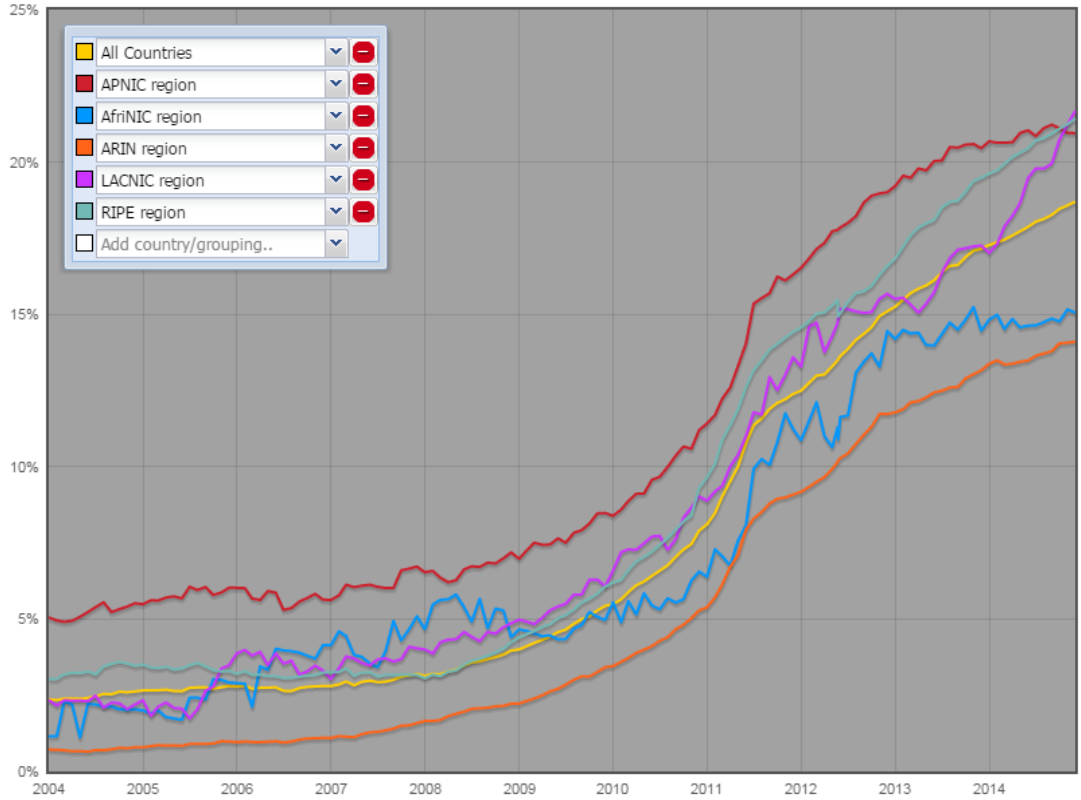
- African Network Information Centre (AfriNIC), για την Αφρική.
- American Registry for Internet Numbers (ARIN), για τις Ηνωμένες Πολιτείες, τον Καναδά, αρκετά τμήματα της Καραϊβικής και την Ανταρκτική.
- Asia-Pacific Network Information Centre (APNIC), για την Ασία, την Αυστραλία, τη Νέα Ζηλανδία και τις γειτονικές χώρες.
- Latin America and Caribbean Network Information Centre (LACNIC), για τη Λατινική Αμερική και τμήματα της περιοχής της Καραϊβικής.
- Reseaux IP Europeens Network Coordination Centre (RIPE NCC), για την Ευρώπη, τη Ρωσία, τη Μέση Ανατολή και την Κεντρική Ασία.



Εικόνα 15 Ο χάρτης του συστήματος RIR
(Πηγή: http://en.wikipedia.org)

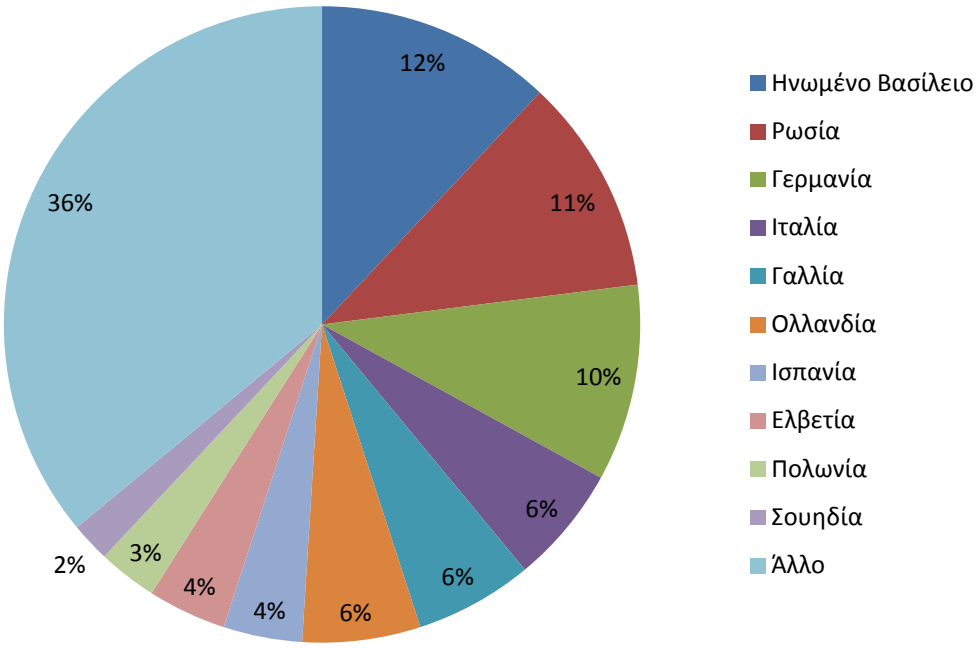
Τα πέντε RIR είναι υπεύθυνα στα προσδιορισθέντα εδάφη τους για την ανάθεση στους τελικούς χρήστες και τις τοπικές γραμματείες του Διαδικτύου, όπως το ISP. Το IPv4 παρέχει περίπου 4,3 δισεκατομμύρια διευθύνσεις και ένα υποσύνολο από αυτές έχουν διανεμηθεί από το IANA στο RIR σε τεμάχια περίπου 16,8 εκατομμύρια διευθύνσεις το καθένα. Το IANA εκπροσωπεί τους πόρους του Διαδικτύου για τα RIR, τα οποία ακολουθούν τις περιφερειακές πολιτικές τους για να αναθέσουν τους πόρους στους πελάτες τους, οι οποίοι περιλαμβάνουν τους ISP και τις οργανώσεις των τελικών χρηστών.

Το IANA είναι υπεύθυνο για τον παγκόσμιο συντονισμό του συστήματος διευθυνσιοδότησης του Πρωτοκόλλου Internet, καθώς και τους αριθμούς του αυτόνομου συστήματος που χρησιμοποιείται για τη δρομολόγηση της κυκλοφορίας του Διαδίκτυο. Ο ρόλος του IANA είναι η κατανομή των IP διευθύνσεων από τη δεξαμενή των μη διατεθέντων διευθύνσεων στα RIR ανάλογα με τις ανάγκες τους. Όταν ένα RIR απαιτεί περισσότερες IP διευθύνσεις για την κατανομή ή την ανάθεση μέσα στην περιοχή, το IANA κάνει μια πρόσθετη κατανομή στο RIR. Το IANA δεν κάνει απευθείας κατανομές στους ISP ή στους τελικούς χρήστες, εκτός από ειδικές περιπτώσεις, όπως είναι οι κατανομές των διευθύνσεων ή άλλες συγκεκριμένες ανάγκες του πρωτοκόλλου.



Διάγραμμα 1 Δεδομένα των αυτόνομων συστημάτων του IPv6
(Πηγή:
http://v6asns.ripe.net/v/6?s=_ALL;s=_RIR_APNIC;s=_RIR_AfriNIC;s=_RIR_ARIN;s=_RIR_LACNIC;s=_RIR_RIPE_NCC)

Το Διάγραμμα 1 δείχνει τα ποσοστά των δικτύων (αυτόματων συστημάτων) που ανακοινώνει ένα IPv6 πρόθεμα για κάθε RIR. Η τελευταία μέτρηση έγινε στις 1 Δεκεμβρίου του 2014, στην οποία βλέπουμε ότι το ποσοστό για όλες τις χώρες είχε φτάσει το 18,70%, το ποσοστό για τη περιοχή APNIC είχε φτάσει το 20,95%, για το AfriNIC είχε φτάσει το 15,06%,για το ARIN είχε φτάσει το 14,10%, για το LACNIC είχε φτάσει το 21,68% και για το RIPE είχε φτάσει το 21,43%. Παρατηρούμε ότι και τα έξη μεγέθη έχουν ανοδική πορεία, αλλά η περιοχή APNIC κατέχει τα μεγαλύτερα ποσοστά. Η περιοχή AfriNIC έχει μια μη ομαλή ανοδική πορεία, καθώς οι τιμές της αυξάνονται και μειώνονται συνεχώς, και το μεγαλύτερο ποσοστό της είναι 15,24% το Νοέμβριο του 2013. Η περιοχή ARIN κατέχει τα μικρότερα ποσοστά από όλα τα μεγέθη. Οι περιοχές ARIN, RIPE, LACNIC και όλες οι χώρες έχουν μια σχετικά ομαλή τάση και με τα τρία τελευταία μεγέθη (RIPE, LACNIC και όλες οι χώρες) να έχουν σχεδόν τις ίδιες μετρήσεις.



Γράφημα 1 Οι δέκα κορυφαίες χώρες-μέλη του RIRE NCC
(Πηγή: https://labs.ripe.net/statistics/membership-by-country)

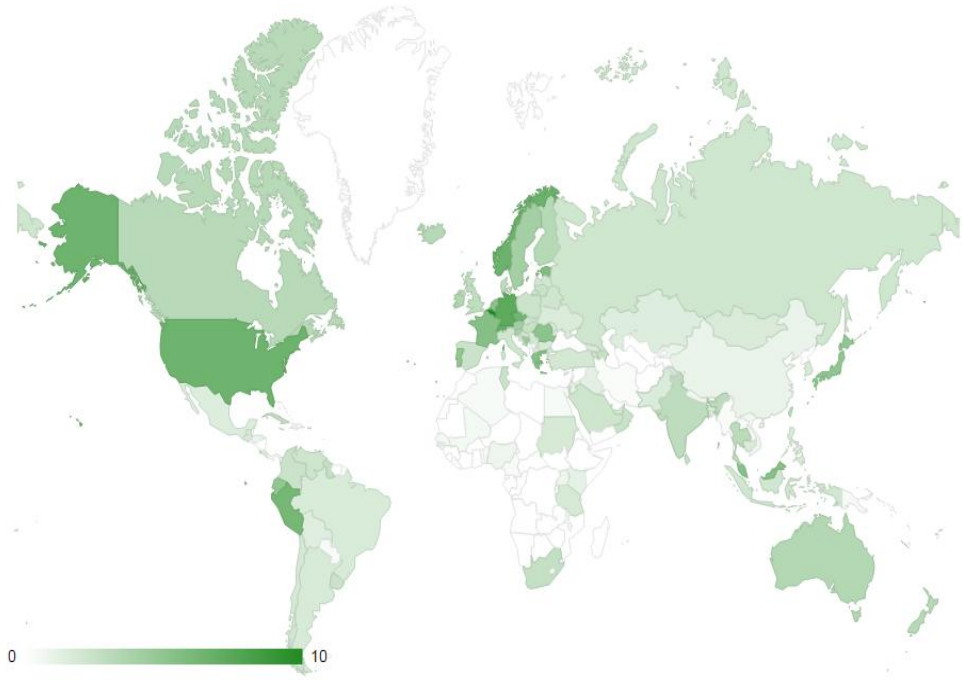
Το Γράφημα 1 μας δείχνει την κατανομή των RIRE NCC μελών ανά χώρα. Η υπηρεσία της περιοχής RIRE NCC καλύπτει συνολικά 76 χώρες. Παρατηρούμε ότι το μεγαλύτερο ποσοστό το κατέχει το Ηνωμένο Βασίλειο με 12% και ακολουθεί η Ρωσία με 11% και η Γερμανία με 10%.

4.1 Η Μεταβατική Κατάσταση του IPv6

Η μετάβαση του IPv6 είναι ένα σύστημα με πολλαπλά στάδια. Η θέσπιση του IPv6 απαιτεί να περάσει από στάδια σε παγκόσμιο, περιφερειακό, πανελλαδικό και τοπικό επίπεδο. Η μετάβαση του κύκλου ζωής του IPv6 μπορεί πάρει χρόνια πριν από οποιοδήποτε σημαντική IPv6 κίνηση που μπορεί να μετρηθεί. Καθένα από αυτά τα στάδια πρέπει να μετρηθούν.

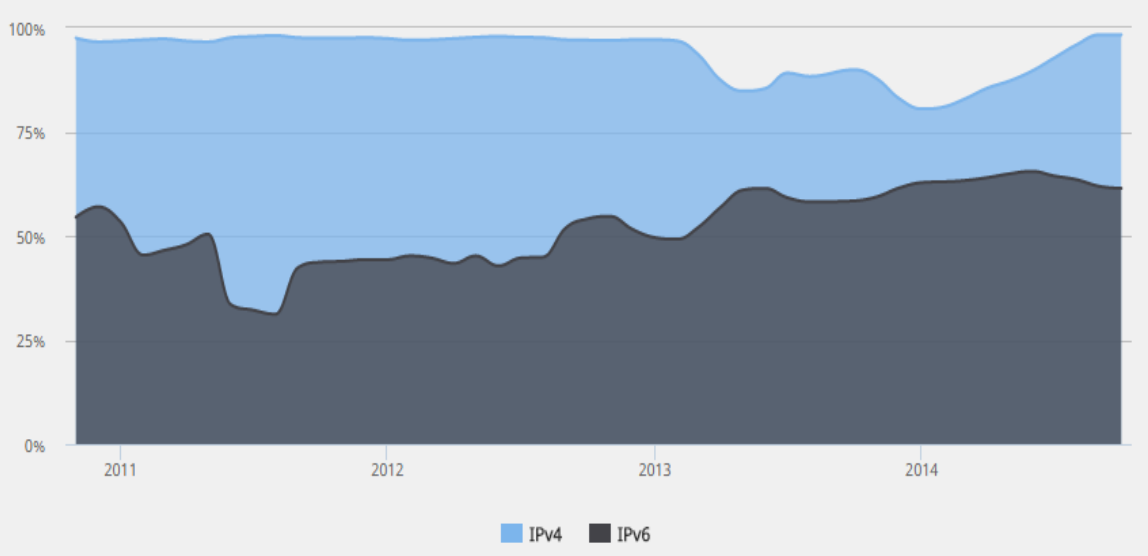
Υπάρχουν δημόσια διαθέσιμα δεδομένα που μπορούν να συγκεντρωθούν και να παρακολουθούνται επί ένα χρονικό διάστημα. Κάποια δεδομένα πρέπει να συλλέγονται ανιχνεύοντας το Διαδίκτυο και ελέγχοντας τις ιστοσελίδες. Ο πυρήνας του Διαδικτύου είναι παγκόσμιος. ωστόσο, οι μεγάλες οικονομίες έχουν τοπικό σύστημα διέλευσης, οι οποίες διασυνδέονται με όλους τους παρόχους υπηρεσιών, την κυβέρνηση, την εκπαίδευση, τους τοπικούς παρόχους και τις επιχειρήσεις. Τόσο η παγκόσμια διέλευση όσο και η εθνική διέλευση πρέπει να μετρηθούν. Παρόλο που το Διαδίκτυο είναι παγκόσμιο σύστημα, οι χρήστες και οι στατιστικές

περιεχομένου έχουν τοπικό χαρακτήρα και πρέπει να εξεταστούν και να αξιολογηθούν σε τοπικό επίπεδο.



Εικόνα 16 Παγκόσμιος χάρτης με τις μετρήσεις του IPv6
(Πηγή: http://6lab.cisco.com/stats/index.php?option=all)

Στην Εικόνα 16 βλέπουμε τον παγκόσμιο χάρτη με τις στατιστικές μετρήσεις του προθέματος του IPv6, της διέλευσης του αυτόνομου συστήματος (AS), της περιεκτικότητας του Διαδικτύου και των χρηστών σε κάθε χώρα. Για παράδειγμα, τα ποσοστά των Ηνωμένων Πολιτειών της Αμερικής είναι 37,8% για το πρόθεμα του IPv6, 61,47% για τη διέλευση του αυτόνομου συστήματος, 46,85% για την περιεκτικότητα του Διαδικτύου και 10,9% για τους χρήστες. Δηλαδή, η συνολική ανάπτυξη του IPv6 είναι 32,32% και ο σχετικός δείκτης είναι 6,6/10. Τα ποσοστά της Γερμανίας είναι 52,18% για το πρόθεμα του IPv6, 82,48% για τη διέλευση του αυτόνομου συστήματος, 46,1% για την περιεκτικότητα του Διαδικτύου και 11,8% για τους χρήστες. Η συνολική ανάπτυξη του IPv6 είναι 38,11% και ο σχετικός δείκτης είναι 7,3/10. Για το Βέλγιο τα ποσοστά είναι 40,23%, 77,62%, 48,59% και 27,2% αντίστοιχα. Η συνολική ανάπτυξη του IPv6 είναι 46,67% και ο σχετικός δείκτης είναι 10/10. Τέλος, για την Ελλάδα τα ποσοστά είναι 39,66%, 61,94%, 51% και 5,87% αντίστοιχα. Η συνολική ανάπτυξη του IPv6 είναι 28,46% και ο σχετικός δείκτης είναι 5,4/10.



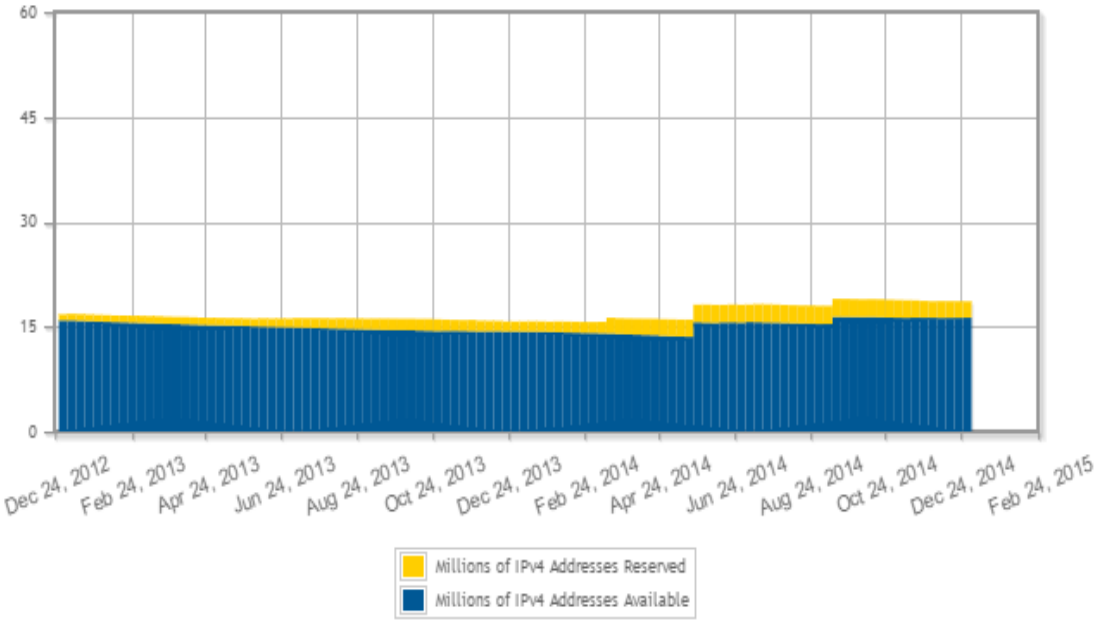
Διάγραμμα 2 Γενική υποστήριξη του IPv6 και του IPv4
(Πηγή: http://ipv6-test.com/stats/)

Στο Διάγραμμα 2 απεικονίζεται η εξέλιξη της υποστήριξης του IPv6 και του IPv4 πρωτοκόλλου, και μπορούμε να αναμένουμε ότι το 100% σχεδόν των host υποστηρίζουν το IPv4 με μια αργή ανάπτυξη για το IPv6. Η τελευταία μέτρηση αυτού του διαγράμματος έγινε στις 30 Σεπτεμβρίου του 2014, η οποία αποτελείται από τις συντεταγμένες 98,3% για το IPv4 και 61,4% για το IPv6. Στις 31 Δεκεμβρίου του 2013 σημειώθηκε η μικρότερη διαφορά ανάμεσα στην υποστήριξη των δύο πρωτοκόλλων, καθώς το IPv4 έφτανε στο 80,5% και το IPv6 στο 62,8%. Αντίθετα, στις 31 Ιουλίου του 2011 σημειώνεται η μεγαλύτερη διαφορά, αφού το IPv4 έφτανε στο 98,1% και το IPv6 στο 31,2%. Επίσης παρατηρούμε ότι ενώ το IPv6 έχει μια σχετική ανοδική πορεία, το IPv4 έχει μια σχετική σταθερή τάση μέχρι το 2013, μετά έχει μια μικρή κατηφορική πορεία μέχρι το Δεκέμβριο του 2013 και το 2014 αποκτά μια έντονη ανοδική τάση.

Χώρα	Αριθμός εξεταζόμενων	IPv4	IPv4%	IPv6	IPv6%
Η.Π.Α	120,815	119,454	98,9%	95,413	79%
Γερμανία	24,258	23,476	96,8%	14,104	58,1%
Καναδάς	9,151	9,049	98,9%	6,363	69,5%
Βέλγιο	2,240	2,135	95,3%	1,373	61,3%
Ελλάδα	2,317	2,291	98,9%	1,475	63,7%

Πίνακας 3 Η υποστήριξη του IPv6 σε πέντε ενδεικτικές χώρες (Οκτώβριος 2014)
(Πηγή: http://ipv6-test.com/stats/)

Στον παραπάνω πίνακα έχουμε ένα παράδειγμα πέντε ενδεικτικών χωρών, οι οποίες εξετάσθηκαν για την υποστήριξη των πρωτοκόλλων IPv4 και IPv6. Βλέπουμε ότι και στις πέντε χώρες η υποστήριξη του IPv4 φτάνει σχεδόν το 100% και η υποστήριξη του IPv6 είναι μεγαλύτερο του 50%.

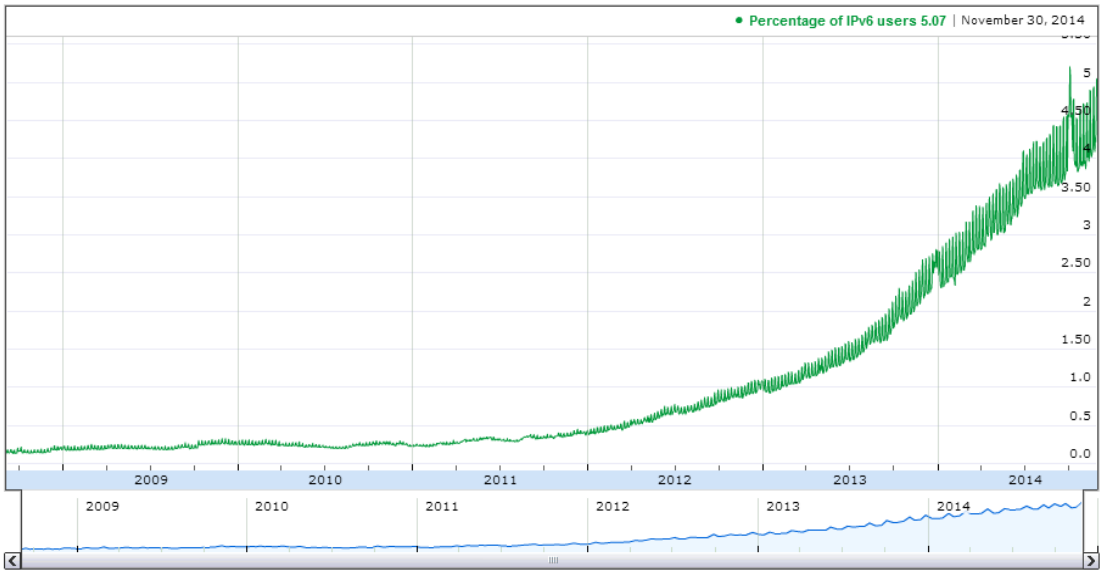


Διάγραμμα 3 Διαθέσιμες και δεσμευμένες IPv4 διευθύνσεις που διαχειρίζεται το RIPE NCC (Πηγή: https://www.ripe.net/internet-coordination/ipv4-exhaustion/ipv4-available-pool-graph)

Το Διάγραμμα 3 μας δείχνει τον αριθμό των διαθέσιμων (η στήλη με μπλε χρώμα) και δεσμευμένων (η στήλη με κίτρινο χρώμα) IPv4 διευθύνσεων που διαχειρίζεται το RIPE NCC για τα τελευταία 2 χρόνια. Η τελευταία μέτρηση έγινε στις 29 Δεκεμβρίου του 2014, στην οποία βλέπουμε ότι οι διαθέσιμες IPv4 διευθύνσεις είχαν φτάσει τα 16,27 εκατομμύρια και οι δεσμευμένες IPv4 διευθύνσεις τα 2,33 εκατομμύρια. Παρατηρούμε ότι η πορεία των δεσμευμένων IPv4 διευθύνσεων είναι πάντα ανοδική, ενώ η πορεία των διαθέσιμων IPv4 διευθύνσεων είναι καθοδική μέχρι τις 19 Μαΐου του 2014 και έπειτα έχει μια σχετικά ανοδική πορεία. Η μικρότερη μέτρηση των διαθέσιμων IPv4 διευθύνσεων ήταν στις 19 Μαΐου του 2014 με τιμή 13,54 εκατομμύρια και η μεγαλύτερη μέτρηση τους ήταν στις 15 Σεπτεμβρίου του 2014 με τιμή 16,39 εκατομμύρια. Η μικρότερη μέτρηση των δεσμευμένων IPv4 διευθύνσεων ήταν στις 31 Δεκεμβρίου του 2012 με τιμή 0,87 εκατομμύρια και η μεγαλύτερη μέτρηση ήταν στις 21 Ιουλίου και στις 1 Σεπτεμβρίου του 2014 με τιμή 2,60 εκατομμύρια.

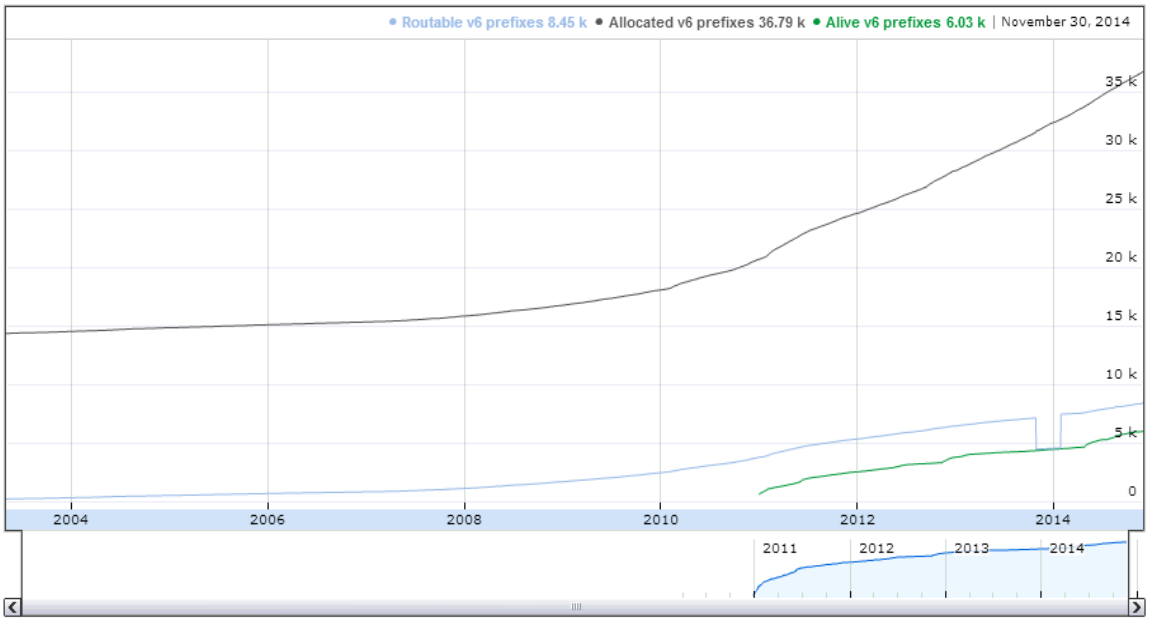
Υπάρχουν πολύ λίγα δεδομένα σχετικά με το IPv6 σε σχέση με τους πελάτες. Οι υπάρχουσες μετρήσεις είναι κυρίως μικρής κλίμακας ή/και έμμεσα σχετίζονται με τη IPv6 διαθεσιμότητα των πελατών (π.χ. το ποσοστό της IPv6 κυκλοφορίας). Μια από τις καλύτερες μετρήσεις θα μπορούσε είναι το 0,086% το 2008. Υπάρχει όμως και μια γενική ανησυχία ότι ενεργοποιώντας το IPv6 μπορεί να προκαλέσει πολλά

προβλήματα, όπως μια μη βέλτιστη δρομολόγηση. (Πηγή: Gunderson, S.H. (2008) Global IPv6 Statistics-Measuring the current state of IPv6 for ordinary users. [pdf] Διαθέσιμο στο: https://www.ietf.org/proceedings/73/slides/v6ops-4.pdf).



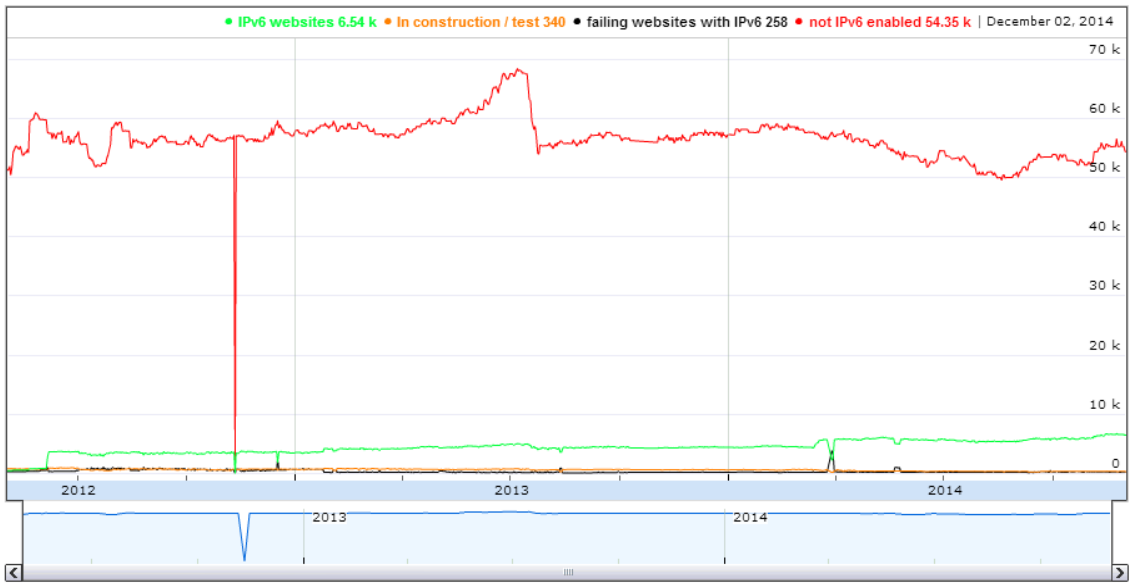
Διάγραμμα 4 Δεδομένα των IPv6 χρηστών
(Πηγή:http://6lab.cisco.com/stats/cible.php?country=world&option=prefixes)

Στο Διάγραμμα 4 παρατηρούμε τα ποσοστά των IPv6 χρηστών με την πάροδο του χρόνου. Η τελευταία μέτρηση έγινε στις 30 Νοεμβρίου του 2014, στην οποία βλέπουμε ότι το ποσοστό των χρηστών έχει φτάσει στο 5,06%. Γενικά παρατηρούμε μια σχετική ανοδική τάση με την πάροδο του χρόνου, ειδικά στις 4 Οκτωβρίου του 2014 φτάνει τη μεγαλύτερη τιμή του 5,21%, ενώ μέχρι και τις 11 Φεβρουαρίου του 2012 διατηρεί μια σχετική σταθερή πορεία μικρότερη από το 0,5%.



Διάγραμμα 5 Δεδομένα των IPv6 προθεμάτων
(Πηγή: http://6lab.cisco.com/stats/cible.php?country=world&option=users)

Στο Διάγραμμα 5 βλέπουμε τα στοιχεία των IPv6 προθεμάτων με την πάροδο του χρόνου, δηλαδή τα δρομολογήσιμα, τα κατανεμημένα και τα ενεργά IPv6 προθέματα. Η τελευταία μέτρηση έγινε στις 30 Νοεμβρίου του 2014, στην οποία βλέπουμε ότι τα κατανεμημένα IPv6 προθέματα φτάνουν τις 36.790, τα δρομολογήσιμα φτάνουν τις 8.450 και τα ενεργά τις 6.030. Στις 5 Ιανουαρίου του 2011 παρατηρούμε την πρώτη μέτρηση του ενεργού IPv6 προθέματος με 721, ενώ τα δρομολογήσιμα φτάνουν τις 3.820 και τα κατανεμημένα τις 20.780.

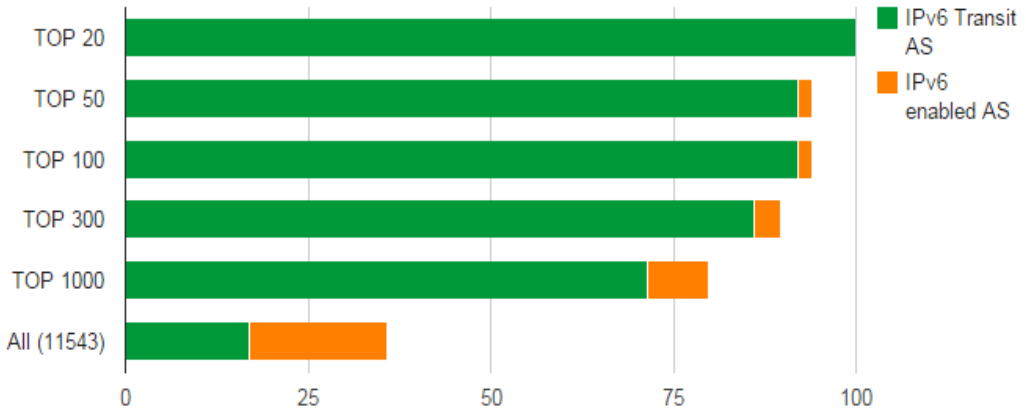


Διάγραμμα 6 Δεδομένα των IPv6 ιστοσελίδων
(Πηγή: http://6lab.cisco.com/stats/cible.php?country=world&option=all)

Στο Διάγραμμα 6 παρατηρούμε κάποια στοιχεία για τις IPv6 ιστοσελίδες με την πάροδο του χρόνου, συγκεκριμένα τις ενεργές ιστοσελίδες, τις μη ενεργοποιημένες, τις υπό κατασκευή και τις ιστοσελίδες που ¨πέφτουν¨ με το IPv6. Η τελευταία μέτρηση έγινε στις 2 Δεκεμβρίου του 2014, στην οποία παρατηρούμε ότι οι ενεργές IPv6 ιστοσελίδες φτάνουν τις 6.540, οι μη ενεργοποιημένες ιστοσελίδες τις 54.350, οι υπό κατασκευή φτάνουν τις 340 και εκείνες που ¨πέφτουν¨ με το IPv6 τις 258. Μια μεγάλη πτώση παρατηρούμε στις 11 Νοεμβρίου του 2012, όπου οι μη ενεργοποιημένες IPv6 ιστοσελίδες είχαν φτάσει τις 468, οι ενεργές IPv6 ιστοσελίδες είχαν φτάσει μόνο τη 1 και εκείνες που ¨πέφτουν¨ μόλις τις 31. Ενώ οι υπό κατασκευή ιστοσελίδες είχαν την μεγαλύτερη πτώση τους στις 30 Μαρτίου του 2014 με τιμή μόλις 201.

Διάγραμμα 7 Διέλευση αυτόνομου συστήματος του IPv6 και του IPv4
(Πηγή: http://6lab.cisco.com/stats/cible.php?country=world&option=network)

Στο Διάγραμμα 7 έχουμε τη διέλευση του αυτόνομου συστήματος των IPv6 και IPv4 με την πάροδο του χρόνου. Η τελευταία μέτρηση έγινε στις 4 Δεκεμβρίου του 2014, στην οποία παρατηρούμε ότι η διέλευση του αυτόνομου συστήματος για το IPv6 φτάνει τις 1.950 και για το IPv4 φτάνει τις 7.740. Γενικά, η τάση και των μεγεθών είναι σχετικά ανοδική αλλά παρατηρούμε τέσσερις απότομες πτώσεις τους. Η πρώτη έγινε στις 3 Μαρτίου του 2013, όπου μόνο η διέλευση για το IPv4 έπεσε στο 0, ενώ η διέλευση για το IPv6 είχε φτάσει στις 1.500 και διατηρούσε σταθερή ανοδική τάση. Η δεύτερη έγινε στις 30 Απριλίου του 2013, η τρίτη στις 5 Απριλίου του 2014 και η τέταρτη στις 7 Απριλίου του 2014, όπου και στις τρεις περιπτώσεις και τα δύο μεγέθη είχαν ¨πέσει¨ στο 0.

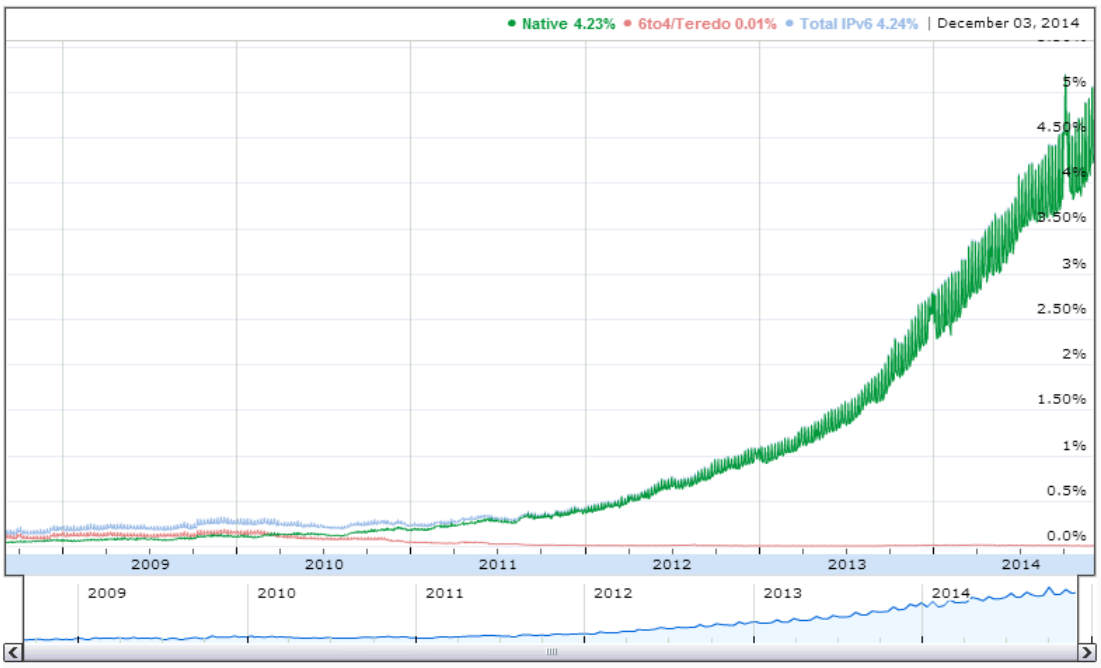


Διάγραμμα 8 Επισκόπηση διέλευσης αυτόνομου συστήματος
(Πηγή: http://6lab.cisco.com/stats/cible.php?country=world&option=network)

Στο Διάγραμμα 8 έχουμε την επισκόπηση της διέλευσης του αυτόνομου συστήματος, συγκεκριμένα η στήλη με το πράσινο χρώμα αποτελεί τη διέλευση του αυτόνομου συστήματος από το IPv6, ενώ η στήλη με το κίτρινο χρώμα αποτελεί το ενεργοποιημένο IPv6 για το αυτόνομου σύστημα. Οι 20 κορυφαίες μετρήσεις αποτελούνται μονάχα από τη διέλευση του αυτόνομου συστήματος από το IPv6, ενώ στις 50 και στις 100 κορυφαίες μετρήσεις αποτελούν μόνο το 92% και το 2% αποτελείται από το ενεργοποιημένο IPv6 για το αυτόνομο σύστημα. Στις1000 κορυφαίες μετρήσεις το 71,3% αποτελείται από τη διέλευση του αυτόνομου συστήματος από το IPv6 και το 8,4% από το ενεργοποιημένο IPv6 για το αυτόνομο σύστημα.

4.2 Η Μεταβατική Κατάσταση μέσω των Τούνελ 6to4 και Teredo

Όπως προαναφερθήκαμε, η μετάβαση του IPv6 πρωτοκόλλου μπορεί να χρειαστεί πολλά χρόνια για να ολοκληρωθεί. Παρατηρούμε ότι με το πέρασμα των χρόνων η χρήση του IPv6 αυξάνεται. Μπορούμε να συμπεράνουμε πως ο χρήστης αποκτά πρόσβαση στο IPv6 με βάση τη IPv6 διεύθυνση. Δυστυχώς, δεν γίνεται με εύκολο τρόπο να διακρίνει κανείς τη native (φυσική) μέθοδο από τα τούνελ με βάση μόνο τις διευθύνσεις. Η Google συνεχώς μετράει τη διαθεσιμότητα της IPv6 συνδεσιμότητας μεταξύ των χρηστών της.



Διάγραμμα 9 Πρόσβαση στη Google με IPv6
(Πηγή: http://www.google.com/intl/en/ipv6/statistics.html)

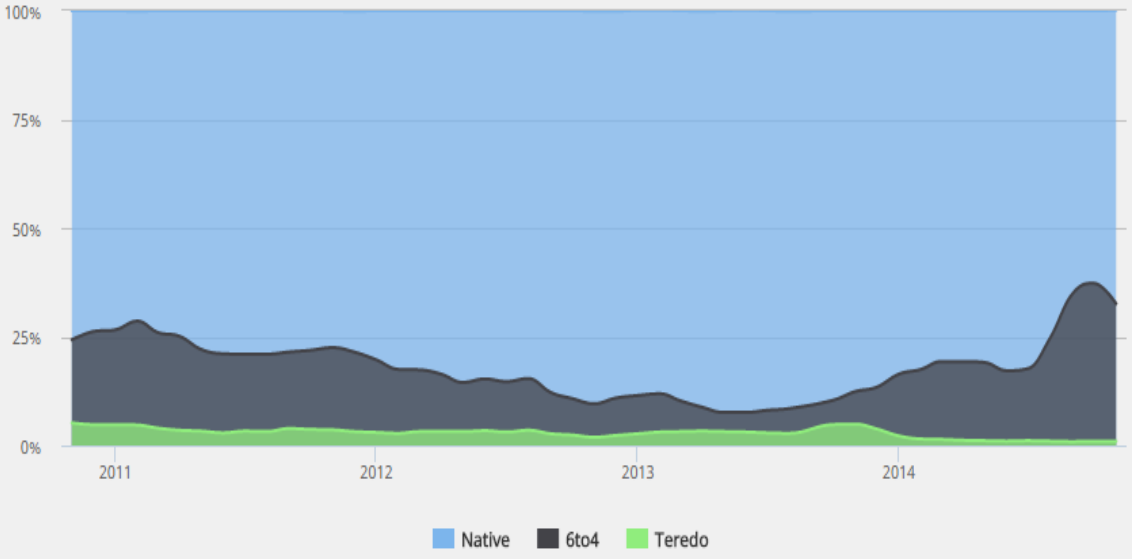
Το παραπάνω Διάγραμμα 9 δείχνει το ποσοστό των χρηστών που έχουν πρόσβαση στη Google με IPv6. Συγκεκριμένα δείχνει το ποσοστό των χρηστών που χρησιμοποιούν τη native μέθοδο, τα τούνελ 6to4/Teredo και τη συνολική IPv6. Η τελευταία μέτρηση έγινε στις 3 Δεκεμβρίου του 2014, στην οποία παρατηρούμε ότι η χρήση της native μεθόδου είχε φτάσει στο 4,23%, η χρήση των 6to4/Teredo είχε φτάσει στο 0,01% και η χρήση της συνολικής IPv6 είχε φτάσει στο 4,24%. Παρατηρούμε ότι οι τιμές της native μεθόδου και της συνολικής IPv6 σχεδόν συμπίπτουν και οι τάσεις τους αυξήθηκαν απότομα από το 2011 και έπειτα και παραμένουν ανοδικές μέχρι και την τελευταία μέτρηση, ενώ η τάση των τούνελ 6to4/Teredo παραμένει σταθερή με το πέρασμα των χρόνων. Στις 4 Οκτωβρίου του 2014 παρατηρούμε τη μεγαλύτερη τιμή της native μεθόδου και της συνολικής IPv6, καθώς φτάνουν το μέγιστο ποσοστό του 5,19% και του 5,21% αντίστοιχα, ενώ το ποσοστό των τούνελ 6to4/Teredo παραμένει σταθερό στο 0,01%.

Είναι σημαντικό να σημειωθεί ότι τα στατιστικά της κίνησης του IPv6 για τη Google έδειξαν ότι η παγκόσμια κυκλοφορία του IPv6 έχει περάσει επιτέλους το 5%. Ειδικά, αν κοιτάξουμε για τα στατιστικά στοιχεία ανά χώρα, μπορούμε να δούμε την αύξηση της ανάπτυξης της κυκλοφορίας του IPv6 σε κάποιες χώρες, όπως στο Βέλγιο (29,22%), στη Γερμανία (12,42%), στις ΗΠΑ (10,99%), στην Ελβετία (10,31%), στην Ελλάδα (6,06%) και σε άλλες χώρες. (Πηγή: http://www.google.com/intl/en/ipv6/statistics.html#tab=per-country-ipv6-adoption). Μπορεί να μη φαίνεται το 5% μεγάλο ποσοστό, αλλά αυτό είναι ένα μεγάλο βήμα για την πορεία του IPv6, καθώς περισσότερα από δισεκατομμύρια ανθρώπους και συσκευές είναι σε θέση να συνδεθούν με το Διαδίκτυο.

Μέθοδος	Παγκόσμια χρήση
6to4	67,9%
Native/other	29,1%
ISATAP	1,6%
Teredo	1,4%

Πίνακας 4 Παγκόσμια χρήση των IPv6 τούνελ
(Πηγή: Gunderson, S.H. (2008) Global IPv6 Statistics-Measuring the current state of IPv6 for ordinary users. [pdf] Διαθέσιμο στο: https://www.ietf.org/proceedings/73/slides/v6ops-4.pdf)

Στον Πίνακα 4 βλέπουμε τη παγκόσμια χρήση για κάποιες μεθόδους του IPv6 το 2008. Παρατηρούμε ότι η μέθοδος 6to4 έχει τη περισσότερη χρήση με ποσοστό 67,9%. Ακολουθεί η native μέθοδος με 29,1% και στο τέλος το ISATAP και το Teredo με 1,6% και 1,4% αντίστοιχα. Παρόλο αυτά σε κάποιες χώρες ξεχώρισαν το 2008 αυτές οι μέθοδοι , όπως στις Η.Π.Α. και στον Καναδά η μέθοδος 6to4 αποτέλεσε το 95%, στη Γαλλία η native μέθοδος το 95% και στην Κίνα η native μέθοδος το 71% και η μέθοδος ISATAP το 25%. (Πηγή: Gunderson, S.H. (2008) Global IPv6 Statistics-Measuring the current state of IPv6 for ordinary users. [pdf] Διαθέσιμο στο: https://www.ietf.org/proceedings/73/slides/v6ops-4.pdf).



Διάγραμμα 10 Οι τύποι της IPv6 διεύθυνσης
(Πηγή: http://ipv6-test.com/stats/)

Στο Διάγραμμα 10 παρατηρούμε την εξέλιξη των τύπων διευθύνσεων με την πάροδο του χρόνου, καθώς και τη μέτρηση της χρήσης των τούνελ 6to4 και Teredo. Θα πρέπει να σημειωθεί ότι η μέθοδος 6rd λειτουργεί ως native διεύθυνση, έτσι δεν μπορεί να ανιχνευθεί εδώ ως τούνελ. Η τελευταία μέτρηση έγινε στις 31 Οκτωβρίου του 2014, στην οποία παρατηρούμε ότι η υποστήριξη της native μεθόδου είχε φτάσει στο 67,5%, η χρήση του τούνελ 6to4 είχε φτάσει στο 31,6% και η χρήση του τούνελ Teredo στο 1%. Παρατηρούμε οτι η υποστήριξη του

τούνελ Teredo έχει μια καθοδική τάση, ειδικά από το Νοέμβριο του 2013 και μετά η τάση του κατεβαίνει απότομα. Παραδόξως η καλύτερη μέτρηση του τούνελ Teredo είναι το 5,2% στις 31 Οκτωβρίου του 2010, η οποία αποτελεί την πρώτη μέτρηση του παραπάνω διαγράμματος. Η καλύτερη μέτρηση του τούνελ 6to4 είναι και η μικρότερη μέτρηση για τη native μέθοδο με τα ποσοστά 36,3% και 62,7% αντίστοιχα στις 30 Σεπτεμβρίου του 2014. Στις 31 Μαΐου του 2013 έχουμε την καλύτερη μέτρηση για τη native μέθοδο με ποσοστό 92,5%, ενώ το τούνελ 6to4 είχε φτάσει στο 4,5% και το τούνελ Teredo είχε φτάσει στο 3,1%.

Έτος	Native	Teredo	6to4	ISATAP
2008	21.75%	35.57%	21.89%	2.50%
2009	23.78%	46.68%	18.07%	1.48%
2010	25.53%	48.37%	19.80%	0.60%
2011	27.06%	53.92%	16.78%	0.30%
2012	24.07%	60.48%	14.14%	0.19%
2013	37.86%	48.50%	12.16%	0.08%

Πίνακας 5 Ανάλυση των τύπων της IPv6 σύνδεσης σε έξι χρόνια
(Πηγή: http://www.sixscape.com/joomla/sixscape/index.php/ipv6-training-certification/ipv6-forum-official-certification/ipv6-forum-network-engineer-silver/network-engineer-silver-transition-mechanisms/tunnels/teredo-a-little-worm-that-bores-holes-in-your-firewall)

Τα στατιστικά στοιχεία του Πίνακα 5 περιλαμβάνουν χιλιάδες συνδέσεις από ένα site από το 2008 έως το 2013. Κατά την περίοδο των έξι χρόνων, η χρήση του Teredo έχει μείνει γύρω στο 50%, με μια κορυφή στο 60% το 2012. Οι native συνδέσεις ήταν γύρω στο 20%-25%, αλλά ξαφνικά ανέβηκε κοντά στο 40% το 2013 (το native περιλαμβάνει και το τούνελ 6in4). Η χρήση του 6to4 έχει μειωθεί από 21,89% σε μόλις 12,16%. Το ISATAP ξεκίνησε με το μικρό ποσοστό 2,50% και έχει σχεδόν εξαφανιστεί με το ποσοστό 0,08%.

Το Teredo είναι ένα αυτοματοποιημένος μηχανισμός τούνελ που βασίζεται στο 6in4 για την απόκτηση πρόσβασης στο IPv6 Internet από έναν κόμβο σε ένα IPv4 δίκτυο. Το Teredo είναι εγκατεστημένο σε όλα τα αντίγραφα των Windows Vista. Αν ένας κόμβος με Windows είναι μέλος ενός τομέα δικτύου της Microsoft, τότε το Teredo είναι απενεργοποιημένο. Αν ο κόμβος δεν είναι μέλος ενός τομέα δικτύου της Microsoft, τότε το Teredo είναι ενεργοποιημένο. Το τούνελ 6to4 στα Windows θα λειτουργήσει μόνο αν ο κόμβος έχει μια δημόσια IPv4 διεύθυνση. Το ISATAP απαιτεί κάποια διαμόρφωση από το DNS για να λειτουργήσει. Αλλά αν

ένας κόμβος είναι μέλος ενός τομέα δικτύου της Microsoft μπορεί να χρησιμοποιηθεί το IPv6 μέσω Teredo.

Υπάρχει ένα πρόγραμμα ανοικτού πηγαίου κώδικα που υλοποιεί το τούνελ Teredo για το Linux, το BSD και το Mac OS-X και ονομάζεται Miredo. Μπορεί να ενεργήσει ως ένας πελάτης, ένας αναμεταδότης (relay) ή/και ένα server. Υπάρχουν διαθέσιμα στο δημόσιο Teredo relay routers (παρόμοια με τα 6to4 relay routers), τα οποία επιτρέπουν σε κάθε κόμβο, που υποστηρίζει το τούνελ Teredo, να έχει πρόσβαση στο IPv6 Internet. Επίσης η Microsoft τρέχει δημόσιους Teredo servers.

Το Teredo δίνει ένα κόμβο αυτόματης πρόσβασης για το IPv6, αλλά για πλήρη λειτουργικότητα στα Windows πρέπει να αλλάξει κανείς κάποια από τα πράγματα που κάνουν τα Windows. Αν ένα site είναι μηχανισμού dual stack, τότε θα πρέπει να έχει κανείς το IPv4. Αυτό είναι χρήσιμο μόνο για την πρόσβαση σε IPv6 sites. Είναι όμως καλύτερο να απενεργοποιήσει κανείς μόνος του τους τρεις αυτομάτους μηχανισμούς τούνελ για τα Windows Vista και να κάνει το υποδίκτυό του native dual stack.

Λειτουργικό Σύστημα	Εισχώρηση του IPv6	Αναλογία Native/other	Αναλογία 6to4	Αναλογία Teredo/ISATAP
Mac OS	2.44%	9%	91%	0%
Linux	0.93%	86%	13%	1%
Windows Vista	0.32%	55%	43%	2%
Windows Server 2003	0.07%	-	-	-
Windows XP	0.03%	50%	30%	20%
Windows 2000	<0.01%	-	-	-

Πίνακας 6 Κατανομή ανά λειτουργικό σύστημα
(Πηγή: Gunderson, S.H. (2008) Global IPv6 Statistics-Measuring the current state of IPv6 for ordinary users. [pdf] Διαθέσιμο στο: https://www.ietf.org/proceedings/73/slides/v6ops-4.pdf)

Ο παραπάνω Πίνακας 6 μας δείχνει την εισχώρηση του IPv6 και τους τύπους συνδεσιμότητας για κάθε λειτουργικό σύστημα. Παρατηρούμε ότι το Mac OS κατέχει το μεγαλύτερο ποσοστό (91%) για τη 6to4 μέθοδο, η εισχώρηση του IPv6 φτάνει στο 2,44%, η αναλογία της native μέθοδο φτάνει στο 9%, ενώ η αναλογία του Teredo/ISATAP στο 0%. Το Linux κατέχει μόλις το 13% για τη 6to4 μέθοδο, η εισχώρηση του IPv6 είναι στο 0,93%, για τη native μέθοδο κατέχει το μεγαλύτερο ποσοστό στο 86%, ενώ για το Teredo/ISATAP μόλις το 1%. Τα Windows Vista κατέχει το 43% για τη 6to4 μέθοδο, η εισχώρηση του IPv6 φτάνει στο 0,32%, για τη native μέθοδο στο 55%, ενώ για το Teredo/ISATAP στο 2%. Το Windows Server 2003 έχουμε μόνο την εισχώρηση του IPv6 με ποσοστό μόλις 0,07%. Τα Windows XP κατέχει το 0,03% για την εισχώρηση του IPv6, για τη

6to4 μέθοδο κατέχει το 30%, για τη native μέθοδο το 50%, ενώ για το Teredo/ISATAP το 20%. Τέλος, τα Windows 2000 κατέχει μόνο την εισχώρηση του IPv6 με ποσοστό λιγότερο από 0,01%. Επίσης, έχουμε ότι το 52% του συνόλου των IPv6 επισκέψεων γίνονται από το λειτουργικό σύστημα Mac με τη 6to4 μέθοδο, και το 92% των χρηστών του Teredo συνδέονται από τα Windows (συμπεριλαμβανόμενου και τα Windows Vista). (Πηγή: Gunderson, S.H. (2008) Global IPv6 Statistics-Measuring the current state of IPv6 for ordinary users. [pdf] Διαθέσιμο στο: https://www.ietf.org/proceedings/73/slides/v6ops-4.pdf).

Γενικά, παρατηρούμε ότι η επικράτηση του IPv6 εξακολουθεί να είναι χαμηλή, λόγω των μεγάλων διακυμάνσεων των επιμέρους χωρών και μπορεί να επηρεάζεται σε μεγάλο βαθμό από ενιαίες επεκτάσεις (π.χ. επιχειρήσεων). Η προεπιλεγμένη πολιτική έχει μεγάλη σημασία. Τα Windows Vista παρέχουν 10 φορές περισσότερο την επικράτηση του IPv6 από ότι τα Windows XP και το Mac OS παρέχει 8 φορές περισσότερο την επικράτηση του IPv6 από ότι τα Windows Vista. Η 6to4 μέθοδος είναι μακράν ο πιο κοινός μηχανισμός μετάβασης, τουλάχιστον όταν δεν μετράμε ότι τα Windows Vista δεν προτιμώνται από τη μέθοδο Teredo.

Κεφάλαιο 5: ΣΥΜΠΕΡΑΣΜΑ

Όταν άρχισε να δημιουργείται το Internet με τη μορφή που γνωρίζουμε σήμερα, το πρωτόκολλο IPv4 διέθετε περίπου 4 δισεκατομμύρια διευθύνσεις. Το νούμερο αυτό φάνταζε υπερβολικά μεγάλο πριν 30 και περισσότερο χρόνια, ωστόσο η ραγδαία ανάπτυξη του Internet έδειξε ότι το τέλος του IPv4 δε θα αργούσε να έρθει. Η μεγάλη αύξηση των χρηστών του Διαδικτύου συνέβαλε στην εξάντληση των αποθεμάτων των διευθύνσεων. Αυτό, φυσικά, δεν σημαίνει ότι το Διαδίκτυο θα πάψει να υπάρχει σε λίγα χρόνια.

Το νέο πρωτόκολλο δίνει λύση σε πολλά από τα προβλήματα του προκάτοχού του, εκμεταλλεύεται σε μεγάλο βαθμό τις νέες εφαρμογές και γενικά προσφέρει μια άλλη δυναμική στο Internet και στις δικτυακές επικοινωνίες γενικότερα. Ωστόσο, η μετάβαση στο IPv6 είναι εξαιρετικά δύσκολη και σίγουρα δεν μπορεί να συντελεστεί σε μικρό χρονικό διάστημα, αν αναλογίσει κανείς τον αριθμό των χρηστών, το μέγεθος του Internet, το μικρό ποσοστό της ενημέρωσης και το μικρό βαθμό κατανόησης για το νέο πρωτόκολλο.

Το IPv6 πρωτόκολλο βρίσκεται ακόμα σε μεταβατικό στάδιο, ωστόσο η ανάγκη εγκαθίδρυσής του γίνεται επιτακτική. Μερικοί από τους πιο σημαντικούς λόγους για τη μετάβαση αυτή είναι η αναβάθμιση υπηρεσιών, η υποστήριξη κινητών χρηστών, η έλλειψη απόδοσης διευθύνσεων από το IPv6 πρωτόκολλο και η ασφάλεια που παρέχει.

Ένα από τα συμπεράσματα που μπορούν να ειπωθούν είναι ότι το IPv6 πρωτόκολλο κρατάει τα περισσότερα από τα θετικά χαρακτηριστικά του IPv4, ορισμένα αυτούσια και άλλα μερικώς τροποποιημένα και αφαιρεί όλα εκείνα που αποτελούν εμπόδιο στην απόδοση και την ασφάλεια. Δεν σχεδιάστηκε εξολοκλήρου από την αρχή αλλά βασίστηκε στο IPv4 και στην εμπειρία που είχε αποκτήσει από αυτό. Εντούτοις τα νέα χαρακτηριστικά του IPv6 θα απαιτήσουν νέες λύσεις που θα βοηθήσουν στην προστασία της επόμενης γενιάς δικτύων.

Κατά το διάστημα της μετάβασης από IPv4 σε IPv6, το οποίο εκτιμάται ότι θα είναι μεγάλο, οι εταιρίες ISP (υπηρεσία παροχής Internet) θα πρέπει να παρέχουν στους πελάτες τους παράλληλα διασύνδεση μέσω διευθύνσεων IPv4 και IPv6 (dual stack). Αν και τα δύο πρωτόκολλα μπορούν να λειτουργούν παράλληλα, η συνύπαρξη είναι προβληματική σε πολλές περιπτώσεις, καθώς η μετάφραση μιας διεύθυνσης από το ένα πρωτόκολλο στο άλλο συνεπάγεται χρονική καθυστέρηση.

Όπως προαναφερθήκαμε, το IPv6 πρωτόκολλο έχει σχεδιαστεί για να ξεπεράσει τους περιορισμούς του IPv4. Ο σκοπός του IPv6 είναι να επεκταθεί η IP διεύθυνση και ταυτόχρονα να καταστήσει το πρωτόκολλο απλούστερο στη χρήση και πιο αποτελεσματικό στη λειτουργία του. Προφανώς, η πρόθεση των πελατών είναι να «εγκατασταθούν» σε ένα πρωτόκολλο πολλαπλών υπηρεσιών. Το IPv6 βασίστηκε πάνω στο IPv4 σε όλη τη διαδικασία σχεδιασμού, το οποίο είχε μεγάλη επιτυχία,

και τα περισσότερα από τα χαρακτηριστικά του έχουν διατηρηθεί. Επιπλέον, το IPv6 έχει σχεδιαστεί για να συμπληρώνει και άλλα σχετικά πρωτόκολλα που έχουν αναπτυχθεί ή βρίσκονται υπό ανάπτυξη όπως για παράδειγμα πρωτόκολλα που ασχολούνται με την υποστήριξη της φωνής, βίντεο, δεδομένων, ή άλλων διαδικασιών μέσω διαδικτύου.

ΒΙΒΛΙΟΓΡΑΦΙΑ

- Comer, D.E. (2007), *Δίκτυα και Διαδίκτυα Υπολογιστών και Εφαρμογές τους στο Internet*, Αθήνα: Κλειδάριθμος.
- Κουριέρης, Ι. (2011), *IPv6 Ασφάλεια*. [pdf] Διαθέσιμο στο: http://digilib.lib.unipi.gr/dspace/bitstream/unipi/4169/1/Kourieris.pdf
- Φιλιππίδης, Δ.Θ. (2005), *Μηχανισμοί Μετάβασης από το IPv4 στο IPv6 Πρωτόκολλο- Μελάτη του 6to4 Μηχανισμού- Σχεδίαση και Υλοποίηση της 6to4 MIB*. [pdf] Διαθέσιμο στο: http://artemis.cslab.ntua.gr/el_thesis/artemis.ntua.ece/DT2005-0085/DT2005-0085.pdf
- EBusiness Forum, *Το Αλφαβητάρι της Τεχνολογίας*. [pdf] Διαθέσιμο στο: http://www.ebusinessforum.gr/old/content/downloads/EbusinessForum_-_IPv6.pdf
- Μαυρουδή, Μ. (2002), *IPv6, MBONE, MOBILE IPv6, ICMPv6, IGMPv6, IPv6 Over ATM, IP Multicasting Over ATM*. [pdf] Διαθέσιμο στο: http://conta.uom.gr/conta/ekpaideysh/metaptyxiaka/technologies_diktywn/ergasies/2002/Mauroudi_IPv6.pdf
- Davies, J. (2012), *Understanding IPv6-Third Edition*. [pdf] Διαθέσιμο στο: http://dl.e-book-free.com/2013/07/understanding_ipv6_3rd_edition.pdf
- A10 Networks, *Deployment Guide for DS-Lite*. [pdf] Διαθέσιμο στο: http://www.a10networks.com/resources/files/A10-DG-DS-Lite.pdf
- Byrne, C. (2014), *464XLAT: Breaking Free of IPv4*. [pdf] Διαθέσιμο στο: https://conference.apnic.net/data/37/464xlat-apricot-2014_1393236641.pdf
- Στάμος, Κ. (2014) *Το Πρωτόκολλο IPv6*. [ppt] Διαθέσιμο στο: https://docs.google.com/file/d/0B1NVmMSWLH93aDVyeFRZVUtIYTQ/edit?pli=1
- Μπούρας, Χ. *Εισαγωγή στην IPv6 Τεχνολογία*. [pdf] Διαθέσιμο στο: http://www.ebusinessforum.gr/old/content/downloads/Introduction_IPv6.pdf
- Fernandez, D. (2002) *Transition Mechanisms BIA, TRT & SOCKS*. [pdf] Διαθέσιμο στο: http://www.ipv6-es.com/02/docs/david_fernandez_3.pdf
- Li, X. (2012) *Details of APRICOT-IVI trial SSID*. [pdf] Διαθέσιμο στο: http://www.apricot.net/apricot2012/__data/assets/pdf_file/0003/45588/Details-of-APRICOT-IVI-trial-SSID-xingli-20120229-v6.pdf
- Li, X. (2008) *IPv4/IPv6 Smooth Migration (IVI)*. [pdf] Διαθέσιμο στο: http://archive.apnic.net/meetings/26/program/ipv6/li-coexistence.pdf
- Gunderson, S.H. (2008) *Global IPv6 Statistics-Measuring the current state of IPv6 for ordinary users*. [pdf] Διαθέσιμο στο: https://www.ietf.org/proceedings/73/slides/v6ops-4.pdf
- Fiocco, A. Kaczmarek, H. (2010) *IPv6 Deployment Statistics*. [pdf] Διαθέσιμο στο:

http://6lab.cisco.com/stats/data/IPv6%20Adoption%20Statistics%20user%20guide.pdf
- Καυκάς, Γ. Μαυρομμάτης, Θ. Σελιμάς, Α. (2011) *Πρωτόκολλο IPv6-Παρουσίαση-Μελλοντικές Εξελίξεις.* [pdf] Διαθέσιμο στο: http://www.lib.teipat.gr/ptyxiakes/sdo/sdo_esps/2011-2014/12452pe.pdf

Ιστοσελίδες

- http://en.wikipedia.org
- http://www.islab.demokritos.gr/gr/html/ptixiakes/ATM_IPv6_&_SecurityConsiderations/kefalaio2.htm
- http://www.h3c.com/portal/Products___Solutions/Technology/IPv4___IPv6_Services/Technology_Introduction/200702/201180_57_0.htm
- http://www.tutorialspoint.com/ipv6/ipv6_routing.htm
- http://www.tutorialspoint.com/ipv6/ipv6_mobility.htm
- http://www.sixscape.com/joomla/sixscape/index.php/ipv6-training-certification/ipv6-forum-official-certification/ipv6-forum-network-engineer-silver/network-engineer-silver-transition-mechanisms/tunnels/4in6-tunnel
- http://www.networkworld.com/article/2231905/cisco-subnet/large-scale-nat-architectures.html
- http://www.networkworld.com/article/2232181/cisco-subnet/understanding-dual-stack-lite.html
- http://www.sixscape.com/joomla/sixscape/index.php/ipv6-training-certification/ipv6-forum-official-certification/ipv6-forum-network-engineer-silver/network-engineer-silver-transition-mechanisms/tunnels/tsp-tunnel-setup-protocol
- http://technet.microsoft.com/en-us/library/cc758763(v=ws.10).aspx
- http://www.networkworld.com/article/2208835/lan-wan/ipv6-tunnel-basics.html?null
- http://www.datalabs.edu.gr/Forum/default.aspx?g=posts&m=495
- http://www.webopedia.com/DidYouKnow/Internet/ipv6_ipv4_difference.html
- http://technet.microsoft.com/en-us/library/cc759208(v=ws.10).aspx
- http://www.ipv6actnow.org/info/statistics/
- http://www.google.com/intl/en/ipv6/statistics.html
- http://ipv6-test.com/stats/
- https://labs.ripe.net/statistics
- http://www.sixscape.com/joomla/sixscape/index.php/ipv6-training-certification/ipv6-forum-official-certification/ipv6-forum-network-engineer-silver/network-engineer-silver-transition-mechanisms/tunnels/teredo-a-little-worm-that-bores-holes-in-your-firewall

- https://www.vyncke.org/ipv6status/
- http://6lab.cisco.com/index.php
- http://www.internetsociety.org/deploy360/blog/2014/12/googles-ipv6-traffic-hits-5-globally-28-in-belgium-12-in-usa-and-germany/

ΟΡΟΛΟΓΙΑ

A+P – Address plus Port: Είναι η τεχνική για την κοινή χρήση των IPv4 διευθύνσεων μεταξύ πολλών χρηστών χωρίς τη χρήση του stateful NAT στο δίκτυο μεταφοράς. Το A+P χρησιμοποιεί το πρωτόκολλο TCP ή UDP και τις IP διευθύνσεις για να διευρύνει το φάσμα των διαθέσιμων host διευθύνσεων

A record (Address Record): Χρησιμοποιείται για να βρεθεί η διεύθυνση ενός υπολογιστή που είναι συνδεδεμένος με το Διαδίκτυο.

AAAA record: Χρησιμοποιείται στο DNS (Domain Name System) για να αντιστοιχίζονται το ονόματα των host σε IPv6 διευθύνσεις.

AFTR – Address Family Transition Router: Είναι το πιο πρόσφατο προϊόν στην εταιρία ISC (Internet Systems Consortium) του ανοικτού κώδικα των προϊόντων υποδομής του Διαδικτύου. Προορίζεται για να διευκολύνει τη μετάβαση από το IPv4 στο IPv6.

ARP – Address Resolution Protocol: Είναι το πρωτόκολλο που χρησιμοποιεί ένας υπολογιστής για να αντιστοιχίζει μια IP διεύθυνση σε μια διεύθυνση υλικού.

B4 – Basic Bridging Broadband: Είναι μια λειτουργία που εφαρμόζεται σε ένα κόμβο dual stack, είτε μια άμεσα συνδεδεμένη συσκευή είτε ένα CPE (Customer-provided equipment), που δημιουργεί ένα τούνελ σε ένα AFTR (Address Family Transition Router).

BGP – Border Gateway Protocol: Είναι το κύριο πρωτόκολλο εξωτερικών πυλών (Exterior Gateway Protocol) που χρησιμοποιείται στο Διαδίκτυο. Παρέχει δρομολόγηση μεταξύ των αυτόνομων συστημάτων (AS).

CPU – Central Processing Unit: Είναι ένα ηλεκτρικό κύκλωμα μέσα σε έναν υπολογιστή που εκτελεί εντολές ενός προγράμματος υπολογιστή από την εκτέλεση βασικών αριθμητικών, λογικών, ελέγχου και εισόδου/εξόδου (I/O) λειτουργιών που ορίζονται από τις οδηγίες. Αναφέρεται σε έναν επεξεργαστή και τη μονάδα ελέγχου, διακρίνοντας τα βασικά στοιχεία ενός υπολογιστή από τα εξωτερικά στοιχεία, όπως η κύρια μνήμη και τα περιφερειακά στοιχεία.

CIDR – Classless Inter-Domain Routing: Είναι η μέθοδος διευθυνσιοδότησης IP και δρομολόγησης, η οποία αντικατέστησε τη διευθυνσιοδότηση με κλάσεις.

CPE – Customer-provided Equipment: Είναι κάθε τερματικό και σχετικός εξοπλισμός που βρίσκεται στις εγκαταστάσεις του συνδρομητή. Γενικά αναφέρεται σε συσκευές, όπως τηλέφωνα, routers, διακόπτες, αντάπτορες οικιακού δικτύου και πύλες πρόσβασης στο Διαδίκτυο που επιτρέπουν στους καταναλωτές να έχουν πρόσβαση σε υπηρεσίες επικοινωνιών παροχής υπηρεσιών και τα διανέμουν στην οικία τους με το LAN (Local Area Network).

DHCP – Dynamic Host Configuration Protocol: Είναι το πρωτόκολλο που χρησιμοποιούν οι υπολογιστές για να παίρνουν πληροφορίες διευθέτησης.

DNS – Domain Name System: Είναι το αυτοματοποιημένο σύστημα που χρησιμοποιείται για τη μετάφραση ονομάτων υπολογιστών σε ισοδύναμες IP διευθύνσεις.

DNSSEC – Domain Name System Security Extensions: Είναι μια ακολουθία των προδιαγραφών του Internet Engineering Task Force (IETF) για τη διασφάλιση ορισμένων ειδών πληροφοριών από το DNS (Domain Name System), όπως χρησιμοποιείται στα δίκτυα του IP (Internet Protocol).

Firewall: Το firewall χρησιμοποιείται για να δηλώσει ότι κάποια συσκευή ή πρόγραμμα έχει ρυθμιστεί για να επιτρέπει ή να απορρίπτει πακέτα δεδομένων που περνούν από ένα δίκτυο υπολογιστών σε ένα άλλο.

FQDN – Fully Qualified Domain Name: Είναι ένα domain name που προσδιορίζει την ακριβή θέση του στην ιεραρχία του DNS (Domain Name System).

Host: Ένας host είναι ένας υπολογιστής ή μια άλλη συσκευή που συνδέεται σε ένα δίκτυο υπολογιστών. Μπορεί να προσφέρει πηγές πληροφόρησης, υπηρεσίες και εφαρμογές για τους χρήστες ή τους άλλους κόμβους στο δίκτυο.

ICMP – Internet Control Message Protocol: Είναι το πρωτόκολλο που χρησιμοποιεί το IP για να αναφέρει τα σφάλματα και τις εξαιρέσεις.

IETF – Internet Engineering Task Force: Είναι η ομάδα δράσης μελέτης τεχνολογιών του Internet, που ελέγχει τα πρότυπα των πρωτοκόλλων TCP/IP.

Interface: Ένα interface είναι ένα κοινό σύνορο στο οποίο δύο ξεχωριστά συστατικά ενός υπολογιστή ανταλλάσσουν πληροφορίες. Η ανταλλαγή αυτή μπορεί να γίνει μεταξύ του λογισμικού, του υλικό (hardware) του υπολογιστή, των περιφερειακών συσκευών, των ανθρώπων και συνδυασμοί αυτών.

Internet Layer: Είναι μια ομάδα διαδικτύωσης μεθόδων, πρωτοκόλλων και προδιαγραφών στο πρωτόκολλο του Διαδικτύου, τα οποία χρησιμοποιούνται για τη μεταφορά των datagrams (πακέτα) από τους αρχικούς host δια μέσου των ορίων του δικτύου στο host του προορισμού, που καθορίζεται από μια διεύθυνση δικτύου (IP address).

IP – Internet Protocol: Είναι το πρωτόκολλο που ορίζει τη μορφή των πακέτων που χρησιμοποιούνται σε ένα διαδίκτυο TCP/IP καθώς και το μηχανισμό για τη δρομολόγηση ενός πακέτου προς τον προορισμό του.

IPsec – IP security: Είναι το πρωτόκολλο που επιτρέπει σε έναν αποστολέα να επιλέγει πιστοποίηση ταυτότητας ή εμπιστευτικότητα για κάθε αυτοδύναμο πακέτο.

ISP – Internet Service Provider: Είναι ένας εμπορικός οργανισμός που παρέχει στους συνδρομητές του πρόσβασης στο Διαδίκτυο.

Link Layer: Είναι το χαμηλότερο στρώμα του πρωτοκόλλου του Διαδικτύου, γνωστό και ως TCP/IP. Είναι μια ομάδα των μεθόδων και των πρωτοκόλλων επικοινωνίας που λειτουργούν μόνο στο σύνδεσμο ότι ένας host είναι φυσικά συνδεδεμένος με αυτό.

LAN – Local Area Network: Είναι ένα δίκτυο που χρησιμοποιεί τεχνολογία σχεδιασμένη για να καλύπτει μια μικρή γεωγραφική περιοχή.

MTU – Maximum Transmission Unit: Είναι η μεγαλύτερη ποσότητα δεδομένων που μπορεί να σταλεί μέσω ενός δεδομένου δικτύου σε ένα μόνο πακέτο.

NAT – Network Address Translation: Είναι μια τεχνολογία που παρέχει συνδεσιμότητα σε πολλούς υπολογιστές, οι οποίοι βρίσκονται σε μια τοποθεσία μέσω μιας και μόνο έγκυρης IP διεύθυνσης.

NAT44: Είναι ένας τύπος NAT που αντιστοιχίζει τις ιδιωτικές IPv4 διευθύνσεις με τις δημόσιες IPv4 διευθύνσεις.

NDP – Neighbor Discovery Protocol: Ανήκει στο πρωτόκολλο του Διαδικτύου που χρησιμοποιείται με το IPv6. Λειτουργεί στο Link Layer και είναι υπεύθυνο για την αυτόματη διευθέτηση των κόμβων, για τη ανακάλυψη άλλων κόμβων στο link, για τν καθορισμό των διευθύνσεων του Link Layer των άλλων κόμβων, για τον εντοπισμό διεύθυνσης, για την εύρεση διαθέσιμων routers και servers του Domain Name System (DNS), για την ανακάλυψη του προθέματος της διεύθυνσης και για τη διατήρηση της προσβασιμότητας των πληροφοριών σχετικά με τις διαδρομές για άλλους ενεργούς γειτονικούς κόμβους.

OSPF – Open Shortest Path First: Είναι ένα πρωτόκολλο που χρησιμοποιείται για τη διάδοση πληροφοριών δρομολόγησης μέσα σε ένα μεμονωμένο αυτόνομο σύστημα.

Q.o.S. – Quality of Service: Είναι ένας όρος που αναφέρεται σε οποιοδήποτε μηχανισμό που παρέχει στατικές εγγυήσεις για τις παρεχόμενες υπηρεσίες.

RFC – Request For Comments: Είναι τα έγγραφα μέσω των οποίων δημοσιοποιούνται πρότυπα για τα πρωτόκολλα TCP/IP.

RFC791: Προδιαγραφές του πρωτοκόλλου Διαδικτύου (Internet Protocol).

RFC1825: Αρχιτεκτονική ασφάλειας για το πρωτόκολλο Διαδικτύου.

RFC2473: Γενικό Tunneling πακέτων στις προδιαγραφές του IPv6.

RFC2529: Μετάδοση των IPv6-over-IPv4 Domains χωρίς ρητό (explicit) τούνελ.

RFC2765: Αλγόριθμος του Stateless IP/ICMP Translation (SIIT).

RFC2766: Το Network Address Translation-Protocol Translation (NAT-PT).

RFC2767: Οι Dual Stack hosts που χρησιμοποιούν την τεχνική Bump-In-the-Stack (BIS).

RFC3056: Σύνδεση των IPv6 Domains μέσω των IPv4 Clouds.

RFC3142: Ένα IPv6-to-IPv4 Transport Relay Translator.

RFC3338: Οι Dual Stack hosts που χρησιμοποιούν το Bump-In-the-API (BIA).

RFC3775: Υποστήριξη του Mobility στο IPv6.

RFC4213: Μηχανισμοί Μετάβασης για τους IPv6 Hosts και Routers.

RFC4214: Το Intra-Site Automatic Tunnel Addressing Protocol (ISATAP).

RFC4443: Το Internet Control Message Protocol (ICMPv6) για το Internet Protocol version 6 (IPv6).

RFC5569: Το IPv6 Rapid Deployment (6rd) στις υποδομές του IPv4.

RFC5572: Το IPv6 Tunnel Broker με το Tunnel Setup Protocol (TSP).

RFC5969: IPv6 Rapid Deployment (6rd) στις υποδομές του IPv4-Προδιαγραφές πρωτοκόλλου.

RFC6145: Αλγόριθμος του Stateless IP/ICMP Translation. Αυτό το έγγραφο είναι η νέα έκδοση του RFC2765.

RFC6146: Stateful NAT64: Διεύθυνση Δικτύου και Πρωτόκολλο Μετάφρασης από τους πελάτες του IPv6 στους IPv4 Servers.

RFC6147: DNS64: Επεκτάσεις του DNS για NAT (Network Address Translation) από τους πελάτες του IPv6 στους IPv4 Servers.

RFC6219: Ο σχεδιασμός της ανάπτυξης και του μηχανισμού IVI για την συνύπαρξη και μετάβαση των IPv4/IPv6 από το China Education and Research Network (CERNET- Δίκτυο εκπαίδευσης και έρευνας της Κίνας).

RFC6333: Οι ευρυζωνικές αναπτύξεις του Dual-Stack Lite μετά την εξάντληση του IPv4.

RFC6877: 464XLAT: Συνδυασμός της Stateful και της Stateless Μετάφρασης.

RIP – Routing Information Protocol: Είναι το πρωτόκολλο που χρησιμοποιεί τη μέθοδο των διανυσμάτων απόστασης για να διαδίδει πληροφορίες δρομολόγησης μέσα σε ένα αυτόνομο σύστημα.

Router: Είναι μια συσκευή δικτύωσης, συνήθως εξειδικευμένο υλικό, που προωθεί πακέτα δεδομένων μεταξύ δικτύων υπολογιστών.

Server: Είναι ένα λογισμικό ικανό να δέχεται εντολές από τον πελάτη και να δίνει απαντήσεις αναλόγως. Διευκολύνει τους πελάτες να μοιράζονται δεδομένα, πληροφορίες ή άλλους πόρους λογισμικού και υλικού. Το server μπορεί να λειτουργήσει σε οποιοδήποτε υπολογιστή.

Socket: Είναι ένα τελικό σημείο μιας ροής ενδοεπικοινωνίας μέσου ενός δικτύου υπολογιστών.

TCP – Transmission Control Protocol: Είναι το πρωτόκολλο της οικογένειας TCP/IP, το οποίο παρέχει στα προγράμματα-εφαρμογές πρόσβαση σε μια συνδεσμική υπηρεσία επικοινωνίας. Παρέχει αξιόπιστη επίδοση με έλεγχο ροής και αντιμετωπίζει τις μεταβαλλόμενες συνθήκες στο Διαδίκτυο προσαρμόζοντας τη μέθοδο επαναμετάδοσης που χρησιμοποιεί.

TCP/IP: Είναι η οικογένεια πρωτοκόλλων που χρησιμοποιείται στο Διαδίκτυο. Δύο από τα σημαντικότερα πρωτόκολλα είναι το TCP και τοIP.

Transport Layer: Παρέχει την από άκρο σε άκρο ή τη host-to-host υπηρεσία επικοινωνίας για εφαρμογές μέσα σε μια πολυεπίπεδη αρχιτεκτονική των στοιχείων του δικτύου και των προτωκόλλων.

TSP – Tunnel Setup Protocol: Είναι ένα πρωτόκολλο ελέγχου δικτύου που χρησιμοποιείται για να διαπραγματευτεί τις παραμέτρους ρύθμισης των IP τούνελ μεταξύ ενός τούνελ host του πελάτη και ενός τούνελ server. Μια σημαντική χρήση του είναι σε μηχανισμούς μετάβασης του IPv6.

UDP – User Datagram Protocol: Είναι το πρωτόκολλο της οικογένειας TCP/IP, το οποίο παρέχει στα προγράμματα-εφαρμογές πρόσβαση σε μια ασυνδεσμική υπηρεσία επικοινωνίας.

WAN – Wide Area Network: Είναι ένα δίκτυο που χρησιμοποιεί τεχνολογία σχεδιασμένη για την κάλυψη μιας μεγάλης γεωγραφικής περιοχής.