ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΔΥΤΙΚΗΣ ΕΛΛΑΔΑΣ

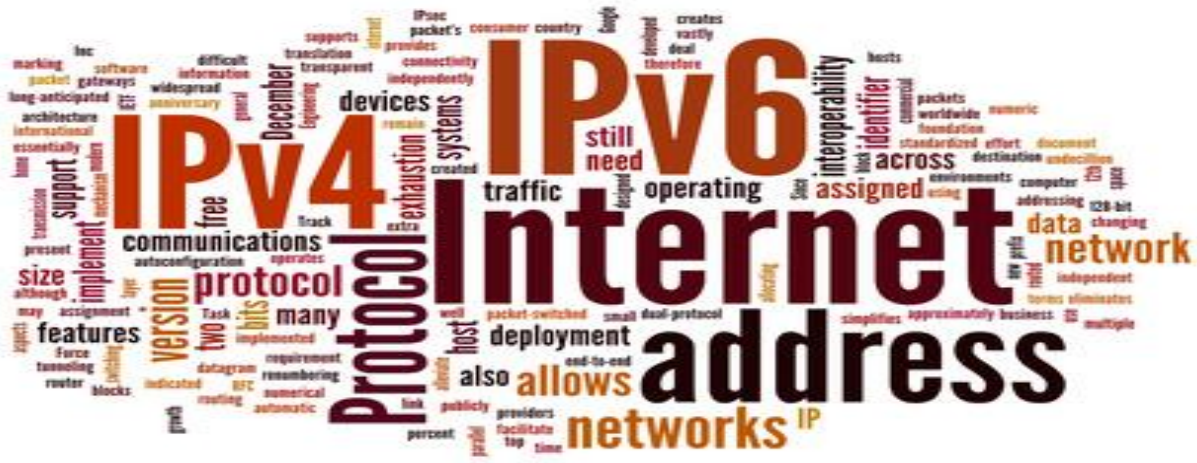
ΣΧΟΛΗ: ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΟΙΚΟΝΟΜΙΑΣ

ΤΜΗΜΑ: ΔΙΟΙΚΗΣΗ ΕΠΙΧΕΙΡΗΣΕΩΝ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΘΕΜΑ:

«Μελέτη της διαδικασίας μετάβασης του Ίντερνετ στο IPv6»



<u>ΦΟΙΤΗΤΡΙΕΣ</u>: Σαντά Μαρία

Μάγκου Αλεξάνδρα

<u>ΕΙΣΗΓΗΤΗΣ</u>: ΣΤΑΜΟΣ ΚΩΝΣΤΑΝΤΙΝΟΣ

ΠΑΤΡΑ 2016

ΠΕΡΙΕΧΟΜΕΝΑ

ΠΕΡΙΛΗΨΗ

Το Πρωτόκολλο Internet IPv4 αποδείχτηκε ένα σταθερό και δυνατό πρωτόκολλο, που κάλυψε σε πολύ μεγάλο βαθμό τις απαιτήσεις για τις οποίες είχε σχεδιαστεί και επικράτησε τελικά στο παγκόσμιο Internet. Εντούτοις, εδώ και μερικά χρόνια είχαν αρχίσει να διαφαίνονται σημαντικά προβλήματα στα οποία το συγκεκριμένο πρωτόκολλο αδυνατούσε να δώσει λύση. Η έλλειψη διευθύνσεων, η δυσκολία διαχείρισης, η μη υποστήριξη φορητότητας και ζητήματα ασφάλειας οδήγησαν στην δημιουργία του νέου πρωτοκόλλου IPv6.

Μεγάλες εξελίξεις συντελέστηκαν στον τομέα των δικτυακών επικοινωνιών και νέες εφαρμογές ήρθαν στο προσκήνιο, τις οποίες όμως το IPv4 δεν μπορεί να υποστηρίξει και να εκμεταλλευτεί στον απαιτούμενο βαθμό. Όταν ορίστηκε το IPv4 υπήρχαν ελάχιστα δίκτυα υπολογιστών.

Στην παρούσα εργασία μελετάται η διαδικασία της μετάβασης του Internet στο νέο πρωτόκολλο IPv6. Αρχικά παρουσιάζονται οι αδυναμίες του πρωτοκόλλου IPv4 στο να καλύψει τις νέες απαιτήσεις του διαδικτύου και στη συνέχεια παρουσιάζονται αναλυτικά οι μηχανισμοί μετάβασης, και ο τρόπος λειτουργίας του πρωτοκόλλου IPv6, τα πρωτόκολλα δρομολόγησης του και η επίδραση του στις enduser εφαρμογές.

Τέλος γίνεται μία μελέτη της τρέχουσας κατάστασης του πρωτοκόλλου IPv6 και σύμφωνα με επίσημα στατιστικά στοιχεία παρουσιάζεται το ποσοστό της χρήσης του πρωτοκόλλου IPv6 και σε παγκόσμιο επίπεδο αλλά και στην Ελλάδα, όπως επίσης παρουσιάζεται και το ποσοστό εξάντλησης του πρωτοκόλου IPv4.

ABSTRACT

The Internet Protocol IPv4 proved to be until now, stable and strong protocol, which fulfilled the requirements for the initial purposes that was designed for Internet. However, significant problems started last years that IPv4 protocol is unable to solve. The lack of addresses, the management difficulty, the failure to support portability and security issues led to the creation of the new protocol IPv6.

Major developments have occurred in network communications and new applications come to the fore. IPv4 is now unable to support them. When IPv4 was created there were few computer networks and there was no prediction of the extension of the Internet use.

In this study we study we the transition to the new IPv6 protocol. Initially, we present weaknesses of IPv4 protocol to meet the new requirements of the internet and then the transition mechanisms, and the mode of the protocol IPv6, routing protocols and the impact on end user applications.

Finally there current state of IPv6 is presented according to official statistics and we show the percentage of use of IPv6 globally and in the region of Greece. Also there is a presentation of the depletion rate of the IPv4 protocol.

ΕΙΣΑΓΩΓΗ

Το Internet είναι μια τεχνολογία για παγκόσμια επικοινωνία, είναι παγκόσμιο σύστημα διασυνδεδεμένων δικτύων υπολογιστών ένας μηχανισμός για διασπορά πληροφοριών και ένα μέσο για συνεργασία και αλληλεπίδραση ανάμεσα σε ιδιώτες και τους υπολογιστές τους εκμηδενίζοντας αποστάσεις από το ένα άκρο στο άλλο μέσα στον γή αλλά ακόμα και έξω από αυτήν με την χρήση δορυφορικών συνδέσεων. Για να συνδεθούν στο διαδίκτυο οι χρήστες έχουν δημιουργηθεί κατάλληλα πρωτόκολλα.

Το πρωτόκολλο IPv6 είναι η επόμενη γενιά του πρωτόκολλου διαδικτύου IP. Αναπτύχθηκε με σκοπό να λύσει τις αδυναμίες του πρωτοκόλλου IPv4. Το ήδη υπάρχον Πρωτόκολλο Internet IPv4 αποδείχτηκε ένα σταθερό και δυνατό πρωτόκολλο, που κάλυψε σε πολύ μεγάλο βαθμό τις απαιτήσεις για τις οποίες είχε σχεδιαστεί και επικράτησε τελικά στο παγκόσμιο Internet. Εντούτοις, εδώ και μερικά χρόνια είχαν αρχίσει να διαφαίνονται σημαντικά προβλήματα στα οποία το συγκεκριμένο πρωτόκολλο αδυνατούσε να δώσει λύση.

Μεγάλες εξελίξεις συντελέστηκαν στον τομέα των δικτυακών επικοινωνιών και νέες εφαρμογές ήρθαν στο προσκήνιο, τις οποίες όμως το IPv4 δεν μπορεί να υποστηρίξει και να εκμεταλλευτεί στον απαιτούμενο βαθμό. Όταν ορίστηκε το IPv4 υπήρχαν ελάχιστα δίκτυα υπολογιστών.

Το πρωτόκολλοIPV6 διατηρεί πολλά από τα χαρακτηριστικά της σχεδίασης που έκαναν το IPv4 τόσο επιτυχημένο. Αν και διατηρεί τις βασικές έννοιες της τρέχουσας έκδοσης ,το IPV6 αλλάζει όλες τις λεπτομέρειες. Για παράδειγμα το IPv6 χρησιμοποιεί μεγαλύτερες διευθύνσεις. Αντί για 32 bit, κάθε διεύθυνση του IPV6 περιέχει 128bit. Ο χώρος των διευθύνσεων είναι αρκετά μεγάλος ώστε να μπορεί να ανταποκρίνεται στην συνεχιζόμενη ανάπτυξη του internet σε όλο τον κόσμο για πολλές δεκαετίες.

Σημαντικό ρόλο στην διαχείριση διευθύνσεων έχουν οι Οργανισμοί Διαχείρισης του Internet όπως ο IANA ο οποίος συντονίζει το παγκόσμιο απόθεμα των IP και τους ASNumbers, παρέχοντάς τους σε περιφερειακά μητρώα του Internet (RIR). Τα RIRs ελέγχουν την ανάθεση και την κατανομή διευθύνσεων IP και τις κατοχυρώσεις. Καθώς το Διαδίκτυο επεκτάθηκε σε ολόκληρο τον κόσμο, η μεγαλύτερη οργάνωση ήταν απαραίτητη για να αντεπεξέλθει στη ζήτηση για διευθύνσεις IP για τους αυξανόμενους κατά εκατομμύρια online χρήστες

Συγκρίνοντας τα δύο πρωτόκολλα συμπεραίνουμε ότι το IPv6 υπερτερεί του IPv4 σε πολλούς τομείς και ότι είναι το κατάλληλο πρωτόκολλο για να ανταπεξέλθει στις νέες απαιτήσεις που δημιουργούνται διαρκώς.

Λόγω των προβλημάτων συμβατότητας των πρωτοκόλλων IPv4 και IPv6 η ανάγκη ύπαρξης μηχανισμών ήταν επιτακτική. Οι τεχνικές οι οποίες δημιουργήθηκαν για να είναι συμβατά τα δυο πρωτόκολλα. Επίσης όσον αφορά τις εφαρμογές enduser επηρεάζεται η λειτουργία τους όσο θα υπάρχει η διαδικασία μετάβασης στο IPv6.

Γενικά το IPv6 έχει να προσφέρει πολλά οφέλη.Πρώτα απ' όλα , είναι η σημαντική αύξηση των διαθέσιμων διευθύνσεων IP για τη σύνδεση δικτυακών συσκευών στο Διαδίκτυο. Επίσης παρέχει αδιάκοπτα υπηρεσίες υψηλής ταχύτητας διασύνδεσης σε κινούμενους χρήστες. . Η ασφάλεια αποτελεί προϋπόθεση αφού κάθε κόμβος που χρησιμοποιεί το IPv6 παρέχει υποχρεωτικά δυνατότητες κρυπτογράφησης ώστε να μεταδίδονται με ασφάλεια και να εξασφαλίζεται η ακεραιότητα των δεδομένων. Τέλος, το πρωτόκολλο IPv6 υποστηρίζει το μηχανισμό anycast με τον οποίο ένας κόμβος μπορεί να απευθύνει ένα μήνυμα σε ένα σύνολο από παραλήπτες και το μήνυμα να παραδοθεί σε έναν από τους παραλήπτες (τον κοντινότερο στον αποστολέα όπως αυτό εκτιμάται με βάση μετρικές του δικτύου).

Η μετάβαση του IPv6 βρίσκεται ακόμα σε αρχικό στάδιο. Στην Ελλάδα για παράδειγμα το ποσοστό χρήσης είναι 20%.

ΚΕΦΑΛΑΙΟ 1

1. Το Διαδίκτυο και τα πρωτόκολλα διαδικτύου

1.1. Η ιστορία του Internet

Το διαδίκτυο Internet έχει ξεκινήσει εδώ και μερικές δεκαετίες δειλα δειλά και σήμερα έχει κάνει μια τεράστια επανάσταση στον κόσμο των υπολογιστών και των επικοινωνιών όσο τίποτα άλλο μέχρι σήμερα. Η εφεύρεση σημαντικών συσκευών όπως αυτές του τηλεγράφου, του τηλεφώνου, του ραδιοφώνου και του υπολογιστή ήταν το πρώτο έναυσμα για το ξενίκημα μιας άλλης εποχής στην οποία κανείς δεν φανταζόταν τις δυνατότητες και τις τεχνολογίες που σήμερα προσφέρει το διαδίκτυο. Το Internet είναι μια τεχνολογία για παγκόσμια επικοινωνία, είναι παγκόσμιο σύστημα διασυνδεδεμένων δικτύων υπολογιστών ένας μηχανισμός για διασπορά πληροφοριών και ένα μέσο για συνεργασία και αλληλεπίδραση ανάμεσα σε ιδιώτες και τους υπολογιστές τους εκμηδενίζοντας αποστάσεις από το ένα άκρο στο άλλο μέσα στον γή αλλά ακόμα και έξω από αυτήν με την χρήση δορυφορικών συνδέσεων. (Leiner&Cerf&Clark 2009)

Τις απεριόριστες δυνατότητες που προσφέρει το διαδίκτυο μπορούν να τις απολαμβάνουν όλοι οι άνθρωποι παγκοσμίως ανεξαρτήτως ηλικίας και οικονομικής κατάστασης. Στην ουσία ιδιοκτήτης του Internet δεν είναι μόνο ένα άτομο ή κάποιος οργανισμός και δεν υπάρχει η δυνατότηττα κανείς να ελέγχει πλήρως το Internet. Το internet υφίσταται σαν μια έννοια και όχι σαν μια χειροπιαστή οντότητα και στηρίζεται σε μια φυσική υποδομή η οποία διασυνδέει κόμβους- δίκτυα μαζί με άλλα δίκτυα. Υπάρχουν πολλοί οργανισμοί, εταιρείες, κυβερνήσεις, σχολεία, ιδιώτες και παροχείς υπηρεσιών που έχουν στην κατοχή τους ένα κομμάτι αυτής της υποδομής, αλλά δεν υπάρχει κανένας που να το κατέχει ολόκληρο.

Το πρώτο ξεκίνημα- Arpanet (δεκαετία ’60-΄70)

Η πρώτη επίσημη, καταγεγραμμένη περιγραφή επικοινωνίας μέσω διαδικτύου ήταν αυτή του J.C.R. Licklider στο πανεπιστήμιο MIT τον Αύγουστο του 1962, στην οποία περιγράφτηκε το λεγόμενο «Galactic δίκτυο» και οραματίστηκε ένα δίκτυο αποτελούμενο από ένα σύνολο από διασυνδεμένους υπολογιστές όπου ο καθένας θα μπορούσε εύκολα και γρήγορα να έχει πρόσβαση στα δεδομένα και στα προγράμματα από οποιοδήποτε σημείο και αν βρίσκεται. Ο Licklider λοιπόν ήταν η έμπνευση για τη δημιουργία του DARPA, το οποίο ξεκίνησε τον Οκτώβριο του 1962 και ενέπνευσε τους διαδόχους, Ivan Sutherland, Bob Taylor, and MIT researcher Lawrence G. Roberts,

Στις αρχές της δεκαετίας του ’70, στο Υπουργείο Άμυνας των ΗΠΑ μπήκαν τα θεμέλια του Internet το οποίο αποτελούνταν από ένα δίκτυο υπολογιστών γνωστό ως ARPANET (Advanced Research Projects Agency Network). Το ARPANET ήταν το πρώτο δίκτυο μεταγωγής πακέτου και το δίκτυο πυρήνας ενός συνόλου που θα συνέθετε το παγκόσμιο Διαδίκτυο (Internet). Το δίκτυο χρηματοδοτήθηκε από το Γραφείο Ερευνών Αμύνης (DARPA - Defense Advanced Research Projects Agency) του τμήματος άμυνας των Ηνωμένων Πολιτειών για χρήση στα πανεπιστήμια και εργαστήρια ερευνών στις Η.Π.Α. (Raphael 2011)

Αλλά η ευρεία χρήση του διαδικτύου από τους απλούς χρήστες δεν μπορούσε να γίνει μέχρι που δημιουργήθηκε ο Παγκόσμιος Ιστός (World Wide Web) στις αρχές της δεκαετίας του ’90. Εδώ πρέπει να σημειωθεί ότι μέχρι τον Ιούνιο του 1993 είχαν δημιουργηθεί μόνο 120 ιστότοποι, ενώ σήμερα υπάρχουν περίπου 2 δισεκατομμύρια ιστοσελίδες.

Με έτος ίδρυσης το 1969, το ARPANET χρησίμευσε σαν ένα πλαίσιο δοκιμών για τις νέες τεχνολογίες δικτύωσης, διασυνδέοντας πολλά πανεπιστήμια και ερευνητικά κέντρα. Οι δύο πρώτοι κόμβοι (nodes) που σχημάτισαν το ARPANET ήταν το UCLA (University of California, Los Angeles) και το Stanford Research Institute, ακολουθούμενα σύντομα από το Πανεπιστήμιο της Utah.

Από το ARPANET στο Internet

Τον Οκτώβριο του 1972, ο Kahn κατάφερε με απόλυτη επιτυχία να οργανώσει την παρουσίαση του ARPANET πρώτη Διεθνή Διάσκεψη για Θέματα Υπολογιστών και Επικοινωνιών (First International Conference on Computers and Communication). Πραγματοποιήθηκε με επιτυχία μια επίδειξη της λειτουργίας του συστήματος, συνδέοντας υπολογιστές μεταξύ τους από 40 διαφορετικές τοποθεσίες. (Leiner & Cerf & Clark 2009)

Επίσης, το έτος 1972 αποτελεί το ξεκίνημα της εφαρμογής «hot», δηλαδή της εφαρμογής ηλεκτρονικού ταχυδρομείου (email). Ο Ray Tomlinson έκανε την συγγραφή του απαραίτητου κώδικα, για την αποστολή και την λήψη απλών μηνυμάτων, υποκινούμενος από την ανάγκη των σχεδιαστών του ARPANET για ένα εύκολο μηχανισμό συντονισμού στην επικοινωνία. Λίγο αργότερα ο Roberts επέκτεινε τις δυνατότητες του ηλεκτρονικού ταχυδρομείου ώστε να μπορεί να γίνει ταξινόμηση των ηλεκτρονικών μηνυμάτων, προώθηση και απευθείας απάντηση.

Τέλος, στις αρχές της δεκαετίας του ’70, οι επιστήμονες ανέπτυξαν τα πρωτόκολλα host-to-host. Πριν την δημιουργία αυτών των πρωτοκόλλων δεν επιτρεπόταν η πρόσβαση στα αρχεία από πολλούς υπολογιστές παρά μόνο από ένα σύστημα κάθε φορά.

Το έτος 1974, οι άνθρωποι που δημιούργησαν το ARPA, με συντονισμένη και κοινή προσπάθεια με επιστήμονες από το Stanford, ανέπτυξαν μια κοινή γλώσσα που θα επέτρεπε σε διαφορετικά δίκτυα να επικοινωνούν μεταξύ τους. Αυτό έγινε γνωστό με τον όρο transmission control protocol/internet protocol, το πασίγνωστο σήμερα TCP/IP. Το TCP/IP αποτελεί βασικό βήμα στην μετέπειτα εξέλιξη του διαδικτύου. Παρ’ όλα αυτά, χρειάστηκαν αρκετά χρόνια για το TCP/IP και τροποποιήσεις και επανασχεδιάσεις πριν πάρει την ολοκληρωμένη μορφή που έχει σήμερα για την χρήση στο διαδίκτυο.

Οι πρώτες συνδέσεις

Το 1973, ένα νέο ερευνητικό πρόγραμμα κάνει την εμφάνιση του με όνομα «Interneting Project» (Πρόγραμμα Διαδικτύωσης) και στόχο είχε να βρεθεί λύση ώστε κάθε δίκτυο να διακινεί τα δεδομένα του.

Οι Vint Cerf και Bob Kahn το 1974 αναπτύσσουν μια νέα τεχνική, το γνωστό Internet Protocol (IP-Πρωτόκολλο Διαδικτύωσης). Από εκεί πήρε και το όνομα του το σημερινό Internet. Με το πρωτόκολλο IP υπάρχει η δυνατότητα πολλά δίκτυα που βρίσκονται απομακρυσμένα το ένα με το άλλο να μπορούν να συνδέονται και να αποτελούν ένα κοινό διαδίκτυο. Κάθε δίκτυο επίσης, έχει την δυνατότητα να επικοινωνήσει με άλλο δίκτυο, δηλαδή ένα τερματικό που ανήκει σε κάποιο μεμονωμένο δίκτυο επικοινωνεί με ένα άλλο τερματικό το οποίο ανήκει σε ένα άλλο δίκτυο. (Raphael 2011)

Επίσης σε αυτό το σημείο της ιστορικής αναδρομής αναπτύσσεται και μια μέθοδος για την μετάδοση των δεδομένων. Το Πρωτόκολλο Ελέγχου Μετάδοσης, το πασίγνωστο TCP. Επίσης, ορίζονται προδιαγραφές για τη μεταφορά αρχείων μεταξύ υπολογιστών (FTP) και για το ηλεκτρονικό ταχυδρομείο (Email). Σιγά-σιγά στο ήδη υπάρχων ARPANET συνδέονται καινούριες χώρες και καινούρια πανεπιστήμια όπως αυτό του University College of London (Αγγλία) και το Royal Radar Establishment (Νορβηγία).

Ένα παγκόσμιο δίκτυο για την ακαδημαϊκή κοινότητα (Δεκαετία ’80)

Το έτος 1981 αποτελεί σταθμός την ιστορία του διαδικτύου, καθώς καθιερώνεται η έκδοση IPv4 του πρωτοκόλλου του διαδικτύου.

Στη συνέχεια, το 1983, το πρωτόκολλο TCP/IP ορίζεται ως πρότυπο από το Υπουργείο Άμυνας των ΗΠΑ. Επίσης η δημιουργία του λειτουργικού συστήματος Berkeley της UNIX το οποίο εμπεριέχει το TCP/IP αποτέλεσε καθοριστικό παράγοντα στην ταχεία εξάπλωση της διαδικτύωσης των υπολογιστών. Πάρα πολλοί νέοι οργανισμοί, κυρίως πανεπιστήμια συνδέουν

τα συστήματά τους και τους υπολογιστές τους στο ARPANET. Αυτό το γεγονός συντέλεσε στο να χωριστεί το ARPANET σε δύο τμήματα:

i. στο MILNET το οποίο θα βοηθούσε τις επικοινωνίες στον στρατιωτικό τομέα
ii. και στο νέο ARPANET το οποίο θα το χρησιμοποιούσαν μόνο πανεπιστήμια για έρευνα.

Ο κύριος λόγος αυτού του χωρισμού ήταν ο συνολικός αριθμών υπολογιστών στο διαδίκτυο τον οποίο επιβάρυνε πολύ το ARPANET.

Λίγο αργότερα το 1985, ο Διεθνής οργανισμός επιστήμης, (NSF) σχεδιάζει και κατασκευάζει ένα γρήγορο δίκτυο το ονομαζόμενο NSFNET κάνοντας χρήση του πρωτοκόλλου TCP/IP. Σκοπός του ήταν η σύνδεση πέντε super computers με την υπόλοιπη επιστημονική κοινότητα. Στην συνέχεια η Γερμανία, η Ιταλία, η Σουηδία και άλλες χώρες γίνονται μέρος του NSFNET και δημιουργούν ξεχωριστά δίκτυα και πλέον το γνωστό Internet παίρνει την παγκόσμια μορφή του. Αυτό συντέλεσε και στην κατάργηση του ARPANET το 1990.

Από το Internet στο World Wide Web (Δεκαετία ’90)

Ύστερα από την εισχώρηση αρκετών χωρών στο NSFNET, και η Ελλάδα συνδέεται σε αυτό το 1990.

Το 1993, το εργαστήριο CERN στην Ελβετία παρουσιάζει το World Wide Web (WWW-Παγκόσμιο Ιστό) που αναπτύχθηκε από τον Tim Berners-Lee. Πρόκειται για ένα σύστημα διασύνδεσης πληροφοριών σε μορφή πολυμέσων (multimedia) που βρίσκονται αποθηκευμένες σε χιλιάδες υπολογιστές του Internet σε ολόκληρο τον κόσμο και παρουσίασής τους σε ηλεκτρονικές σελίδες, στις οποίες μπορεί να περιηγηθεί κανείς χρησιμοποιώντας το ποντίκι. Το γραφικό αυτό περιβάλλον έκανε την εξερεύνηση του Internet προσιτή στον απλό χρήστη.

Το 1995, το NSFNET καταργείται πλέον επίσημα και το φορτίο του μεταφέρεται σε εμπορικά δίκτυα. Η ανακάλυψη του WWW σε συνδυασμό με την ευκολία απόκτησης

πρόσβασης στο Internet προσέλκυσε έναν μεγάλο αριθμό καινούργιων χρηστών και έφερε την “έκρηξη” που παρακολουθήσαμε τα τελευταία χρόνια.

Το 1996 ανακαλύπτεται το πρωτόκολλο διαδικτύου έκδοση 6 (IPv6) και χαρακτηρίζεται ως το πρωτόκολλο επόμενης γενιάς

Το 1999 γίνονται οι πρώτες χορηγήσεις παραγωγής του IPv6 σε παρόχους υπηρεσιών διαδικτύου (ISP) και σε άλλους φορείς εκμετάλλευσης δικτύου.

Τα 2006 το πρωτόκολλο επόμενης γενιάς περνάει αυτή την περίοδο δοκιμασίας με επιτυχία και έτσι καθιερώνεται.

Σήμερα, το μεγαλύτερο μέρος του πληθυσμού της Γης ζει σε χώρες που είναι συνδεδεμένες στο Internet. Παρατηρούμε ότι καθημερινά περιοδικά και εφημερίδες εκδίδονται “on-line” και μας παραπέμπουν στις διευθύνσεις τους, επιχειρήσεις και ιδιώτες φτιάχνουν τις δικές τους σελίδες στο WWW,κλπ. Είναι προφανές ότι το Internet δεν αποτελεί πλέον το δίκτυο των φοιτητών και των ερευνητών, αλλά επεκτείνεται και επιδρά στην καθημερινότητά μας.

Όπως αναφέραμε και παραπάνω λοιπόν για να υπάρξει διαδίκτυο είναι απαραίτητο να υπάρχει μια καθιερωμένη ομάδα πρωτοκόλλων δηλαδή ένα σύνολο συμβάσεων που καθορίζουν το πώς ανταλλάσσουν μεταξύ τους δεδομένα οι υπολογιστές του δικτύου αλλά και οι υπολογιστές διαφορετικών δικτύων. Το επικρατέστερο μέχρι σήμερα είναι το πρωτόκολλο TCP/IP που είναι συνδυασμός δύο πρωτοκόλλων, του TCP και του IP.

1.2. Internet Protocol (IP)

Το πρωτόκολλο διαδικτύου (IP) αποτελεί το κύριο πρωτόκολλο επικοινωνίας για την μετάδοση πακέτων δεδομένων σε ένα διαδίκτυο. Ο βασικός σκοπός του είναι η δρομολόγηση των πακέτων στην διαδρομή τους που κάνουν μέσω των δικτύων. Σε αυτό το πρωτόκολλο στηρίζεται όλη η υποδομή του διαδικτύου. Το πρωτόκολλο IP είναι αυτό που καθορίζει την μορφή των πακέτων, τις μεθόδους που αυτά μεταδίδονται από έναν υπολογιστή σε ένα άλλον, και στη συνέχεια σε κάποιον άλλο ενδιάμεσο κόμβο ή και περισσότερους, μέχρι τελικά να φτάσουν στον τελευταίο προορισμό τους.

Υπάρχουν συγκεκριμένες μέθοδοι διευθυνσιοδότησης για τα πακέτα προς μετάδοση. Ένα αυτοδύναμο πακέτο IP αποτελείται από ένα κομμάτι κεφαλίδας και ένα κομμάτι κειμένου. Η κεφαλίδα έχει ένα σταθερό τμήμα μεγέθους 20 byte και ένα προαιρετικό τμήμα μεταβλητού μήκους. Μεταδίδεται με σειρά μεγάλου άκρου (big endian): από τα αριστερά προς τα δεξιά, με το σημαντικότερο bit του πεδίου «Έκδοση» να μεταδίδεται πρώτο. Πιο συγκεκριμένα, το πεδίο «Έκδοση» αντιπροσωπεύει την έκδοση του πρωτοκόλλου την οποία ακολουθεί το αυτοδύναμο πακέτο.

Μέχρι σήμερα έχει χρησιμοποιηθεί με μεγάλη επιτυχία η έκδοση IPv4. Βέβαια για τους λόγους που θα αναφερθούν παρακάτω σε άλλη ενότητα ήταν αναγκαία η δημιουργία μιας άλλης έκδοσης, αυτής της IPv6 και η μετάβαση στην έκδοση IPv6 βρίσκεται σε εξέλιξη, αλλά λόγω διάφορων προβλημάτων ίσως διαρκέσει αρκετά χρόνια. Ο βασικός στόχος είναι η σταδιακή κατάργηση της έκδοσης 4 και η αντικατάσταση της από την έκδοση 6. Όσον αφορά το IPv5, ήταν ένα πρωτόκολλο δοκιμαστικού σκοπού συνεχούς ροής δεδομένων πραγματικού χρόνου, το οποίο όμως δεν χρησιμοποιήθηκε σε μεγάλη κλίμακα.

Οποιαδήποτε συσκευή που θέλει να έχει πρόσβαση στο διαδίκτυο, είτε αυτή είναι υπολογιστής, κινητό, router αποκτάει με αυτόματο τρόπο μια διεύθυνση IP η οποία είναι μια αριθμητική ακολουθία μοναδική για κάθε συσκευή στο δίκτυο.

Το πεδίο “Εκδοση” (Version) δείχνει την έκδοση του πρωτοκόλλου την οποία ακολουθεί το αυτοδύναμο. Στον παρακάτω πίνακα παρουσιάζεται η γενική μορφή ενός αυτοδύναμου πακέτου IP .

<table>
<tr><td>Version</td><td>IHL</td><td>Type of Service</td><td colspan="2">Total Length</td></tr>
<tr><td colspan="3">Identification</td><td>Flags</td><td>Fragment Offset</td></tr>
<tr><td>Time to Live</td><td colspan="2">Protocol</td><td colspan="2">Header Checksum</td></tr>
<tr><td colspan="5">Source Address</td></tr>
<tr><td colspan="5">Destination Address</td></tr>
<tr><td colspan="5">TCP Header, then your data...</td></tr>
</table>

Πίνακας 1 – Γενική μορφή πακέτου IP

1.2.1. Το Πρωτόκολλο Διαδικτύου - IPv4

Το IPv4 είναι η τέταρτη έκδοση του πρωτοκόλλου Internet, αλλά είναι το πρώτο που χρησιμοποιείται ευρέως. Το IPv4 κάνει χρήση ενός συστήματος 32 bit με αποτέλεσμα να έχει την δυνατότητα να δώσει 4.294.967.296 μοναδικές διευθύνσεις IP.

Στην έκδοση πρωτοκόλλου διαδικτύου IPv4 υπάρχουν τέσσερις διαφορετικές κλάσεις που είναι χωρισμένες στις κατηγορίες A, B, C και D. Το IPv4 χρησιμοποιεί την λεγόμενη μάσκα υποδικτύου διότι ο αριθμός των υπολογιστών και των συσκευών που χρειάζεται να συνδεθούν σήμερα στο διαδίκτυο είναι δισεκατομμύρια σε αριθμό.

Παρατηρώντας το σχήμα 1 και τον πίνακα 2 θα μπορούσε κάποιος εύκολα να καθορίσει την κλάση στην οποία ανήκει μια διεύθυνση IP, όπως επίσης και το Net id και το Host id. Ένας υπολογιστής όμως για να καθορίσει το Net id και το Host id κάνει χρήση της μάσκας η οποία είναι μια ακολουθία ενός δυαδικού αριθμού 32 bit. Η χρήση της μάσκας γίνεται με σκοπό να καθοριστεί η δομή κάποιας διεύθυνσης IP. Για το Host id χρησιμοποιείται η τιμή «0» και για το Net id χρησιμοποιείται η τιμή «1» και γίνεται χρήση του δυαδικού συστήματος. Στη συνέχεια εκτελώντας την λογική πράξη «AND», μπορούμε να υπολογίσουμε την τελική διεύθυνση IP. Βέβαια, για έναν άνθρωπο το δυαδικό σύστημα δεν είναι και ότι καλύτερο, και για αυτό το λόγο κάθε ομάδα των 8 bit (1 byte) μετατρέπεται στον αντίστοιχο δεκαδικό αριθμό.

- Class A - 255.0.0.0 - 11111111.00000000.00000000.00000000
- Class B - 255.255.0.0 - 11111111.11111111.00000000.00000000
- Class C - 255.255.255.0 - 11111111.11111111.11111111.00000000

Σχήμα 1

Class of Address	Size of Network Part of Address, in Bits	Size of Host Part of Address, in Bits	Default Mask for Each Class of Network
A	8	24	255.0.0.0
B	16	16	255.255.0.0
C	24	8	255.255.255.0

Πίνακας 2- Προκαθορισμένες μάσκες για κάθε κλάση – IPv4

Η ΔΟΜΗ ΕΝΟΣ ΠΑΚΕΤΟΥ IPv4

Ένα αυτοδύναμο πακέτο IP, στην πραγματικότητα είναι μια ακολουθία από bytes το οποίο συνιστούν η κεφαλίδα και το κυρίως μέρος. Στην επικεφαλίδα υπάρχει καταχωρημένος ο προορισμός στον οποίο θα μεταδοθεί το πακέτο και είναι αναγκαίο να τον γνωρίζουν οι δρομολογητές μέσα από τους οποίους θα «ταξιδέψει» το πακέτο ώστε να φτάσει τελικά στον προορισμό του. Στον πίνακα 3 παρουσιάζεται η μορφή της επικεφαλίδας ενός πακέτου IPv4.

IPv4 Header Format

Offsets	Octet	0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Version				IHL				DSCP						ECN		Total Length															
4	32	Identification																Flags				Fragment Offset											
8	64	Time To Live								Protocol								Header Checksum															
12	96	Source IP Address																															
16	128	Destination IP Address																															
20	160	Options (if IHL > 5)																															

Πίνακας 3- Η κεφαλίδα ενός πακέτου IPv4

Όπως μπορούμε να διακρίνουμε στον παραπάνω πίνακα 3, η επικεφαλίδα ενός πακέτου IPv4 αποτελείται από 14 πεδία στο σύνολο της. Τα 13 από αυτά είναι απαραίτητα, ενώ το 14^{ο} είναι προαιρετικό. Κάθε πεδίο έχει προκαθορισμένο μέγεθος.

Version: Το πρώτο πεδίο της επικεφαλίδας σε ένα IP πακέτο είναι το πεδίο της έκδοσης του πρωτοκόλλου, με μήκος 4-bit.

IHL: Το δεύτερο πεδίο, το οποίο έχει και αυτό μέγεθος 4-bits προσδιορίζει το μήκος της επικεφαλίδας (IHL-Internet Header Length). Αυτό μας δίνει το μήκος της επικεφαλίδας σε λέξεις των 32 bit. Επειδή η επικεφαλίδα του IPv4 μπορεί να περιέχει μεταβλητό αριθμό επιλογών, αυτό το πεδίο παρέχει το μήκος της επικεφαλίδας. Η μικρότερη τιμή του πεδίου είναι 5 (RFC 791), που σημαίνει ότι το μήκος είναι 5×32 = 160 bits = 20 bytes. Επειδή το πεδίο είναι 4 bit, το μέγιστο μήκος είναι 2^4-1=15 λέξεις (15×32 bits) ή 480 bits = 60 bytes.

DSCP: Το πεδίο αυτό προσδιορίζει τον τύπο της υπηρεσίας που θα χρησιμοποιηθεί για την δρομολόγηση του πακέτου. Σήμερα καθορίζεται στο RFC 2474 για διαφοροποιημένες υπηρεσίες. Όσο γίνεται η εμφάνιση νέων τεχνολογιών στην χρήση στο διαδίκτυο αυτό το πεδίο αλλάζει και είναι απαραίτητος ο καθορισμός του, για παράδειγμα η χρήση της τεχνολογίας VoIP , η οποία χρησιμοποιείται για συνομιλία μέσα από το διαδίκτυο

ECN: Το πεδίο αυτό ορίζεται στο RFC 3168 και επιτρέπει την χρήση end-to-end όταν υπάρχει συμφόρηση στο δίκτυο χωρίς να υπάρξει απώλεια πακέτων. Το πεδίο αυτό είναι προαιρετικό και χρησιμοποιείται μόνο στην περίπτωση που τα τερματικά που επικοινωνούν θέλουν να το χρησιμοποιήσουν. Η χρήση του έχει νόημα όταν υποστηρίζεται κάποιο underlying δίκτυο.

Total Length: Το πεδίο αυτό παίρνει μια ακέραια τιμή (16 bits), ο οποίος καθορίζει το συνολικό αριθμό οκτάδων που περιέχει το αυτοδύναμο πακέτο, όπου περιλαμβάνονται και η κεφαλίδα και τα δεδομένα.

Identification: Το πεδίο αυτό είναι απαραίτητο για την ταυτοποίηση των κομματιών του αρχικού πακέτου, δηλαδή το αρχικό πακέτο κατακερματίζεται σε πακέτα και στην συνέχεια μεταδίδονται προς τον προορισμό τους, Άρα για να αναγνωριστούν και να συνθέσουν το αρχικό πακέτο, χρειάζεται ένας μοναδικός αριθμός 16 bit για να ταυτοποιηθούν.

Flags: Αυτό το πεδίο αποτελείται από 3 bit, αλλά μόνο τα 2 χρησιμοποιούνται για να προσδιορίσουν αν το πακέτο είναι ολόκληρο ή αποτελεί μέρος κατακερματισμένου πακέτου. Η σημασία των τιμών που παίρνει αυτό το πεδίο είναι η εξής:

- Τιμή bit 0: Δεσμευμένο, πρέπει να είναι 0
- Τιμή bit 1: Απαγόρευσης διάσπασης του αυτοδύναμου πακέτου (DF=Don't Fragment)
- Τιμή bit 2: Ένδειξη ύπαρξης περισσότερων κομματιών (MF=More Fragments)

Εάν η σημαία DF έχει τεθεί στο 1 και για την δρομολόγηση του πακέτου είναι απαραίτητη η διάσπασή του, τότε το πακέτο απορρίπτεται. Σε πακέτα που δεν έχουν διασπαστεί η σημαία MF είναι 0. Για διασπασμένα πακέτα όλα τα κομμάτια έχουν το MF=1, εκτός από το τελευταίο πού έχει το MF=0.

Fragments Offset: Το πεδίο αυτό αποτελείται από 13 bit και καθορίζει την σειρά του κερματισμένου πακέτου. Με το Ethernet II το μέγιστο επιτρεπτό μέγεθος είναι 1500 bytes. Αυτό αποκαλείται ως MTU (Maximum Transmission Unit).

Time to Live: Η τιμή του πεδίου αυτού, η οποία έχει μέγεθος 8 bit, περιέχει τον χρόνο ζωής του αυτοδύναμου πακέτου. Σκοπός του είναι όταν μετά από καθορισμένο χρόνο το πακέτο δεν φτάσει στον προορισμό του να καταστραφεί διότι δεν θα έχει νόημα η συνεχής μετάδοση από δρομολογητή σε δρομολογητή. Μια περίπτωση να συμβεί αυτό, είναι όταν υπάρξει κάποιο σφάλμα στο λογισμικό ή στους δρομολογητές. Για να γίνει η καταστροφή ενός πακέτου, υπάρχει ένας μετρητής, ο οποίος λαμβάνει μια αρχική τιμή, και στην συνέχεια κάθε δρομολογητής μειώνει αυτήν την τιμή κατά 1 μονάδα. Όταν λοιπόν αυτός ο μετρητής φτάσει στο 0 τότε το αυτοδύναμο πακέτο αποβάλλεται και στέλνεται ένα μήνυμα σφάλματος πίσω στην αφετηρία.

Protocol: Το πεδίο αυτό καθορίζει το πρωτόκολλο με το οποίο το αυτοδύναμο πακέτο θα μεταδοθεί. Συνήθως το πρωτόκολλο μετάδοσης είναι το UDP ή το TCP, αλλά υπάρχουν και άλλα πρωτόκολλα που χρησιμοποιούνται ενίοτε.

Header Checksum: Το πεδίο αυτό με μέγεθος 16 bit, χρησιμοποιείται για να ελέγξει την ακεραιότητα του αυτοδύναμου πακέτου IP. Για να γίνει αυτό ο αποστολέας του πακέτου υπολογίζει το άθροισμα (συμπλήρωμα ως προς 1) και η τιμή αυτή αποθηκεύεται. Στη συνέχεια κάθε φορά που το πακέτο φτάνει σε έναν δρομολογητή, ο δρομολογητής υπολογίζει ξανά αυτό το άθροισμα.

Source IP Address: Αυτό το πεδίο περιέχει την διεύθυνση IPv4 του πακέτου του αποστολέα.

Destination IP Address: Αυτό το πεδίο περιέχει την διεύθυνση IPv4 του πακέτου του αποστολέα

IP Options: Αυτό το πεδίο τις περισσότερες φορές δεν χρησιμοποιείται. Όταν η τιμή του πεδίου είναι 5 , σημαίνει πως το πεδίο δεν χρησιμοποιείται, ενώ σε περίπτωση που η τιμή του είναι διαφορετική το πρωτόκολλο IP ορίζει ένα σύνολο από επιλογές IP.

Γενικά το πρωτόκολλο IPv4, αν και γνώρισε και συνεχίζει να γνωρίζει μεγάλη επιτυχία, δεν θεωρείται αξιόπιστο πρωτόκολλο και αυτό διότι δεν εγγυάται την παράδοση του αυτοδύναμου πακέτου στον προορισμό του. Με άλλα λόγια, η έκδοση πρωτοκόλλου IPv4 δεν διαθέτει τους απαραίτητους μηχανισμούς για σφάλματα, ούτε παρέχει λύσεις σε περίπτωση συμφόρησης του δικτύου.

1.2.2. Πρωτόκολλο Διαδικτύου Έκδοση 6 - IPv6

Το πρωτόκολλο IPv6 (Internet Protocol Version 6) είναι η επόμενη γενιά του πρωτόκολλου διαδικτύου IP. Αναπτύχθηκε με σκοπό να λύσει τις αδυναμίες του πρωτοκόλλου IPv4, οι οποίες θα αναφερθούν αναλυτικά σε επόμενη ενότητα. Για να καταλάβει κανείς την υπεροχή του IPv6 σε σχέση με το IPv4, όσον αφορά τον χώρο διευθύνσεων , θα υπάρχουν ακριβώς 2^{128}, ή περίπου $3{,}403 \times 10^{38}$ μοναδικές διευθύνσεις. Δηλαδή, ο ακριβής αριθμός των IPV6 διευθύνσεων είναι:

340.282.366.920.938.463.463.374.607.431.768.211.456

Το ξεκίνημα του έγινε το 1992, όταν το Internet Activities Board (IAB) διερεύνησε την πρόταση του Christian Huitema για το IPng (next generation). Η πρόταση βασιζόταν στο Connectionless Network Protocol (CLNP) και απέτυχε εξαιτίας της εμπορικής αποτυχίας του CLNP.

Λίγο αργότερα, το 1992 με 1994 παρουσιάστηκαν κάποιες ιδέες όπως αυτή του TUBA, TP/IX και SIPP. Το TUBA είναι TCP και UDP πάνω από μεγαλύτερες διευθύνσεις, ενώ το TP/IX συμπεριλαμβάνει και αλλαγές στο TCP. Τελικά υιοθετείται το SIPP αλλά με μερικές αλλαγές. Ονομάστηκε IPv6 και όχι IPv5 γιατί τοIPv5 ήταν το όνομα ενός πειραματικού real-time πρωτοκόλλου. Η πρόταση για το IPng δημοσιεύτηκε στο RFC 1752 , τον Ιανουάριο του 1995.

ΜΟΡΦΗ ΔΙΕΥΘΥΝΣΗΣ IPv6

Οι διευθύνσεις του πρωτοκόλλου IPv6 είναι σε δεκαεξαδική μορφή και παριστάνονται από οκτάδες χωρισμένες από στήλες(άνω και κάτω τελεία). Το μέγεθος μιας διεύθυνσης IPv6 είναι 128 Bits. Ένα παράδειγμα μιας έγκυρης διεύθυνσης IPv6 είναι η παρακάτω.

fe80:0000:0000:0000:0260:0000:97ff:64aa

Για λόγους συντομίας, οι διευθύνσεις μπορούν να απλοποιηθούν με τους εξής δύο τρόπους:

i. Τα λήγοντα μηδενικά μπορούν να παραληφθούν, οπότε το παράδειγμα της διεύθυνσης παραπάνω μπορεί να γραφτεί ως εξης:

fe80:0:0:0:260:0:97ff:64aa

ii. Τα συνεχόμενα μηδενικά μπορουν να αντικατασταθούν με διπλή άνω και κάτω τελεία, οπότε μπορεί να γραφτεί ως εξής:

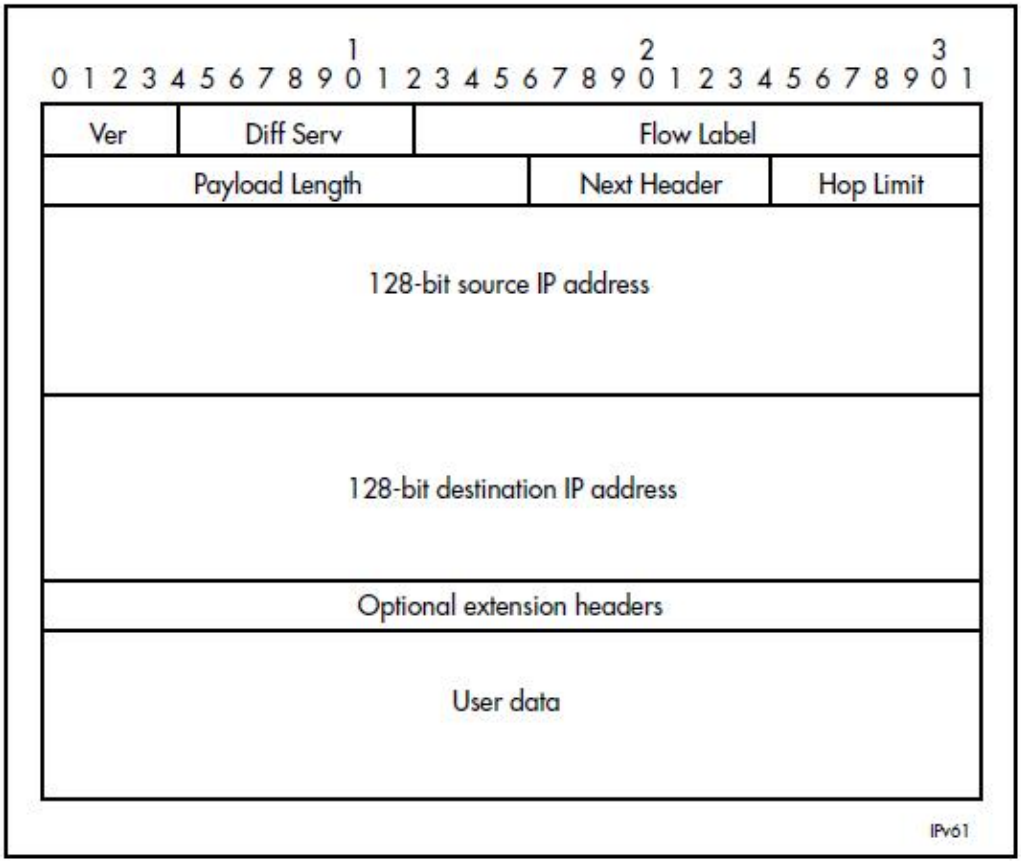
fe80::260:0:97ff:64aa

Εδώ πρέπει να σημειωθεί πως η διπλή άνω κάτω τελεία μπορεί να αντικαταστήσει οποιοδήποτε αριθμό ακολουθίας συνεχόμενων μηδενικών, όμως, μια διεύθυνση μπορεί να περιέχει μόνο μια διπλή άνω-κάτω τελεία.

Όπως συμβαίνει και στις διευθύνσεις , στην έκδοση πρωτοκόλλου IPv4, μερικά Bits στα αριστερά χρησιμοποιούνται για να προσδιορίσουν την μάσκα. Αυτό το μέρος της διεύθυνσης IPv6 ονομάζεται «πρόθεμα». Ένα πρόθεμα παρέχει την ισοδύναμη λειτουργικότητα μιας μάσκας υποδικτύου IPv4.

Η ΔΟΜΗ ΕΝΟΣ ΠΑΚΕΤΟΥ IPv6

Η δομή ενός πακέτου IPv6 είναι αρκετά διαφορετική σε σχέση με αυτή ενός πακέτου IPv4. Όπως φαίνεται και στον πίνακα 4, σε ένα αυτοδύναμο πακέτο IPv6, τα πεδία της κεφαλίδας flags, fragment offset και header checksum δεν περιέχονται πλέον σε αυτό. Επίσης, το πεδίο «Time to Live» αντικαταστάθηκε από το πεδίο «Hop Limit» και το πεδίο «Type of Service Field» του IPv4 αντικαταστάθηκε με το πεδίο «Differentiated Services Field».



Πίνακας 4 – Δομή ενός πακέτου IPv6

Όπως μπορούμε να διακρίνουμε στον παραπάνω Πίνακα 4, η επικεφαλίδα ενός πακέτου IPv4 αποτελείται από 9 πεδία στο σύνολο της. Τα 8 από αυτά είναι απαραίτητα, ενώ το 9ο είναι προαιρετικό. Κάθε πεδίο και σε αυτήν την έκδοση έχει προκαθορισμένο μέγεθος.

Version: Το πεδίο αυτό έχει μέγεθος 4 bits και προσδιορίζει την έκδοση του πρωτοκόλλου με την οποία δημιουργήθηκε το πακέτο, δηλαδή έχει την τιμή « 6».

Differentiated Services: Το πεδίο αυτό αποτελείται από μία τιμή 8 bits και χρησιμοποιείται ώστε να διαχειριστεί την κυκλοφορία σαν μέρος του συστήματος Quality of Service

Flow Label: Μία τιμή με μέγεθος 20 bits η οποία προσδιορίζει την ροή των δεδομένων στην οποία ανήκει το πακέτο. Το είδος της ροής αυτομάτως σημαίνει και διαφορετική μεταχείριση του πακέτου.

Playload Length: Το συγκεκριμένο πεδίο αποτελείται από 16 bits και αναφέρεται στο πεδίο των δεδομένων χωρίς όμως την επικεφαλίδα.

Next Header: Αυτό το πεδίο καθορίζει τον τύπο της επικεφαλίδας η οποία ακολουθεί την βασική κεφαλίδα IP. Ο τύπος της κεφαλίδας μπορεί να είναι προαιρετικά επέκταση της κεφαλίδας IPv6, ή μία σχετική κεφαλίδα IPv4 ή ακόμη και κάποιο άλλο πρωτόκολλο, όπως το TCP ή ICMPv6.

Οι τιμές που μπορεί να πάρει η κεφαλίδα επέκτασης είναι οι εξής:

- 0 (Hop-by-Hop Options Header)
- 43 (IPv6 Routing Header)
- 44 (IPv6 Fragment Header)
- 50 (Encapsulating Security Payload)
- 51 (IPv6 Authentication Header)
- 59 (No Next Header)
- 60 (Destination Options Header).

Hop Limit: Όπως αναφέρθηκε παραπάνω, αυτό το πεδίο αντικαθιστά το αντίστοιχο πεδίο του IPv6 «Time to Live». Το μέγεθος του είναι 8 bits. Αρχικά λαμβάνει μια τιμή και στην συνέχεια μειώνεται κατά ένα κάθε φορά που το πακέτο προωθείται στον επόμενο κόμβο. Η βασική διαφορά του με το IPv4 είναι ότι η τιμή στο πεδίο αυτό εκφράζεται με μορφή βημάτων και όχι δευτερολέπτων όπως στο TTL. Αν το όριο βημάτων γίνει 0 και δεν έχει φτάσει στο προορισμό του το πακέτο, τότε απορρίπτεται.

Source Address (Διεύθυνση Αποστολέα): Καταλαμβάνει 128 bits και μας δίνει την διεύθυνση του αποστολέα.

Destination Address (Διεύθυνση Παραλήπτη): Καταλαμβάνει 128 bits και μας δίνει την διεύθυνση του παραλήπτη. Σε αυτό το πεδίο μπορεί και να μην υπάρχει κάποια διεύθυνση ορισμένες φορές με την προϋπόθεση ότι υπάρχει επικεφαλίδα δρομολόγησης.

Όσον αφορά τις κεφαλίδες επέκτασης του IPv6 μπορούν να χρησιμοποιηθούν οι ακόλουθες:

- Hop by hop option header
- Routing header
- Fragment header
- Destination option header
- Authentication header
- Encapsulation security payload
- Mobility header

ΔΕΔΟΜΕΝΑ

Το τμήμα των δεδομένων του πακέτου προσδιορίζεται από το πεδίο μήκος ωφέλιμου φορτίου (Pay Load Header), στο οποίο το μήκος της κεφαλίδας εξαιρείται και φαίνεται μόνο το μέγεθος των δεδομένων που μεταφέρονται.

Στην συνέχεια θα παρουσιαστούν αναλυτικά οι διαφορές των εκδόσεων πρωτοκόλλου IPv4 και IPv6.

1.3. Λόγοι μετάβασης στο IPV6

Το ήδη υπάρχον Πρωτόκολλο Internet IPv4 αποδείχτηκε ένα σταθερό και δυνατό πρωτόκολλο, που κάλυψε σε πολύ μεγάλο βαθμό τις απαιτήσεις για τις οποίες είχε σχεδιαστεί και επικράτησε τελικά στο παγκόσμιο Internet. Εντούτοις, εδώ και μερικά χρόνια είχαν αρχίσει να διαφαίνονται σημαντικά προβλήματα στα οποία το συγκεκριμένο πρωτόκολλο αδυνατούσε να δώσει λύση.

Μεγάλες εξελίξεις συντελέστηκαν στον τομέα των δικτυακών επικοινωνιών και νέες εφαρμογές ήρθαν στο προσκήνιο, τις οποίες όμως το IPv4 δεν μπορεί να υποστηρίξει και να εκμεταλλευτεί στον απαιτούμενο βαθμό. Όταν ορίστηκε το IPv4 υπήρχαν ελάχιστα δίκτυα υπολογιστών.

Στη συνεχεία θα αναφερθούν οι σημαντικότερες απαιτήσεις που κατέστησαν επιτακτική την ανάγκη για ένα νέο πρωτόκολλο δικτύου.

1.3.1. Έλλειψη Διευθύνσεων IP

Οι σχεδιαστές όταν δημιουργήθηκε το IPv4 τότε πήραν την απόφαση να χρησιμοποιήσουν 32 bit για μια διεύθυνση IP,επειδή με τα τότε δεδομένα τα ένα εκατομμύριο δίκτυα τα οποία μπορούσε να καλύψει αυτό το πρωτόκολλο σε όλο το διαδίκτυο τους φαινόταν πολύ μεγάλο νούμερο και δεν θεωρούνταν απαραίτητο.

Ωστόσο η αύξηση του παγκόσμιου διαδικτύου αυξάνεται με εκθετικό ρυθμό έτσι ώστε το μέγεθός του να διπλασιάζεται σε λιγότερο από ένα χρόνο. Με το σημερινό ρυθμό αύξησης όλα τα διαθέσιμα προθέματα δικτύων που υπάρχουν σύντομα θα αποδοθούν με αποτέλεσμα τη μη δυνατή περεταίρω ανάπτυξη του διαδικτύου. Έτσι το πρωτεύον κίνητρο για αυτή την αλλαγή είναι ο περιορισμένος χώρος διευθύνσεων. Χρειάζονται μεγαλύτερες διευθύνσεις έτσι ώστε να λυθεί το πρόβλημα αυτό και να συνεχιστεί η αύξηση του μεγέθους του διαδικτύου. (Davies 2012)

Το μέγεθος της IPv6 διεύθυνσης είναι 16 bytes (128 bits), το τετραπλάσιο δηλαδή της μέχρι τώρα χρησιμοποιούμενης IPv4 διευθύνσεως δηλαδή, περίπου 6x1020 διευθύνσεις σε κάθε τετραγωνικό μέτρο της επιφάνειας της γης. Με αυτόν τον τρόπο, ένας χρήστης έχει την

δυνατότητα να έχει ταυτόχρονα στην κατοχή του πολλές IP διευθύνσεις, δηλαδή σε συσκευές όπως τα smart phones, εκτυπωτές, laptops και άλλα.

1.3.2. Δυσκολία Διαχείρισης

Το πρόβλημα στην έκδοση 4 του πρωτοκόλλου διαδικτύου δεν είναι μόνο η εξάντληση των διευθύνσεων. Χρειαζόταν και άλλες βελτιώσεις πέρα από αυτό. Ένα άλλο πρόβλημα που αντιμετωπίζει είναι η δυσκολία στην διαχείρισή του τόσο από την μεριά του χρήστη όσο και από την μεριά του ίδιου του διαχειριστή. Αυτό οφείλεται στο ότι όταν σχεδιάστηκε αυτό το πρωτόκολλο σκοπός των διαχειριστών ήταν η δημιουργία του και η σωστή λειτουργία του ώστε να καταφέρει να καλύψει τις τότε ανάγκες χωρίς να τους ενδιαφέρει το πόσο εύκολη ή δύσκολη ήταν η διαχείριση αυτού, έχοντας έτσι ως αποτέλεσμα την αύξηση της πολυπλοκότητας αλλά και του κόστους.

Σήμερα όμως στην εποχή μας που τα πάντα εξελίσσονται με γοργούς ρυθμούς και η τεχνολογία έχει προχωρήσει πολύ μπροστά ο καθένας έχει ως στόχο να βρίσκει τους καλύτερους δυνατούς τρόπους ώστε να κάνει τη ζωή του πιο εύκολη. Έτσι και οι διαχειριστές των πρωτοκόλλων σήμερα προσπαθούν να φτιάχνουν τα πάντα με τέτοιο τρόπο έτσι ώστε να απλοποιούν τα πράγματα και για τους ίδιους αλλά και για τους χρήστες, οι οποίοι αποτελούν βασικό παράγοντα για την δημιουργία όλων αυτών. Για το πρόβλημα λοιπόν αυτό, είχαν δημιουργηθεί δύο πρωτόκολλα. Το αρχικό ήταν το πρωτόκολλο BOOTP, με το οποίο ένας κόμβος μπορούσε να πάρει σχετικά απλά τα στοιχεία του μέσω ενός εξυπηρετητή BOOTP αλλά η δυσκολία για τον διαχειριστή αυξανόταν κατά πολύ. Εκτός αυτού όμως, με αυτό το πρωτόκολλο αυξανόταν πολύ και το κόστος ,αφού απαιτούνταν περισσότερες διευθύνσεις IP καθώς η κάθε διεύθυνση IP έπρεπε να αντιστοιχείται με κάθε κόμβο ανεξάρτητα από το αν ήταν συνδεδεμένος στο διαδίκτυο ή όχι.

Ένα άλλο πρωτόκολλο που χρησιμοποιήθηκε στο IPv4 για αυτό το πρόβλημα είναι το DHCP, το οποίο αποτελεί εξέλιξη του BOOTP. Με αυτό το πρωτόκολλο ένα μηχάνημα μπορούσε να πάρει αυτόματα μια διεύθυνση. Επίσης μπορούσε σε κάποιους κόμβους να αποδοθεί χειρονακτικά IP διεύθυνση από τον διαχειριστή αυτό όμως περιπλέκει την κατάσταση

καθώς θα πρέπει να είναι απαραίτητη η παρουσία DHCP εξυπηρετητή και επίσης είναι δύσκολο να ορίζονται λεπτομερώς στον εξυπηρετητή όλα τα στοιχεία των κόμβων του από έναν άνθρωπο και πολύ χρονοβόρο.

Με το IPv6 πρωτόκολλο αναβαθμίστηκε και το DHCP σε DHCP6 στο οποίο περιλαμβάνονται επιπλέον ρυθμίσεις για την αυτόματη ρύθμιση διεύθυνσης, όπως η stateless, δηλαδή χωρίς διατήρηση κατάστασης, και η statefull, δηλαδή κατάσταση διατηρήσιμη, κατά την οποία όλες οι συσκευές που είναι συνδεδεμένες στο διαδίκτυο έχουν ένα κοινό πρόθεμα 64bit. Τα υπόλοιπα 64 bit που απομένουν μέχρι τα 128 που πρέπει να είναι συνολικά συμπληρώνονται αντίστοιχα, τα 48 από την mac διεύθυνση των συσκευών και τα υπόλοιπα 16 bit συμπληρώνονται με άσσους. Με αυτόν τον τρόπο δεν χρειάζεται να παίρνει καινούρια διεύθυνση ο ίδιος υπολογιστής που συνδέεται κάθε φορά στο ίδιο δίκτυο. Διατηρεί την αρχική IP διεύθυνση που του δόθηκε και συνδέεται όποτε θέλει με αυτήν.

Επίσης ένα ακόμα πράγμα που έχει βελτιωθεί στο IPv6 πρωτόκολλο είναι η μέθοδος αριθμοδότησης του δικτύου η οποία έχει γίνει πολύ εύκολη και πολύ απλή σε σύγκριση με πριν. Ο διαχειριστής μπορεί να αλλάξει τις διευθύνσεις όλων των κόμβων που είναι συνδεδεμένοι σε ένα δίκτυο ,αλλάζοντας το πρόθεμα του δικτύου στον κεντρικό δρομολογητή.

1.3.3. Υποστήριξη Φορητότητας

Με τον όρο «φορητότητα», εννοούμε την δυνατότητα των συσκευών να συνδέονται στο δίκτυο από διαφορετικά μέρη οποιαδήποτε στιγμή. Πιο παλιά δεν μπορούσαμε να αναφερθούμε στην φορητότητα καθώς όλες οι συσκευές που μπορούσαν να συνδεθούν σε ένα δίκτυο ήταν τεράστιες σε όγκο με αποτέλεσμα να είναι αδύνατη η μετακίνηση τους. Πλέον όμως έχουν δημιουργηθεί εκατοντάδες μικρές φορητές συσκευές όπως laptops, netbooks, tablets, κινητά και πολλές άλλες που υποστηρίζουν τα πρωτόκολλο διαδικτύου οι οποίες απαιτούν σύνδεση σε πολλά και διαφορετικά δίκτυα, που σημαίνει ότι θα πρέπει να αλλάζουν διαρκώς και οι ρυθμίσεις του IP αλλά και να υπάρχει διαρκής ενημέρωση για τις αλλαγές αυτές με τους κόμβους που επικοινωνούν.

Το IPv4 έχει τις υποδομές για να υποστηρίξει την φορητότητα αλλά υπάρχουν πολλοί λόγοι που το περιορίζουν. Κάποιοι από αυτούς είναι, ο περιορισμένος αριθμός IP διευθύνσεων,

οι φορητές συσκευές είναι πολύ περισσότερες από τις IPv4 διευθύνσεις που απομένουν, έτσι ώστε να καθιστά αδύνατη την αντιστοίχιση της κάθε φορητής συσκευής με μία IPv4 διεύθυνση. Ένας άλλος λόγος είναι η έλλειψη ασφάλειας και επίσης η μεγάλη φόρτωση του δικτύου διότι για κάθε συσκευή θα πρέπει να υπάρχει και διαφορετική διεύθυνση. Έτσι με την είσοδο του IPv6 δημιουργήθηκε και η εφαρμογή MobileIPv6 στην οποία είναι ενσωματωμένη η MobileIPv4 με πολλές βελτιώσεις βέβαια με σκοπό να καλύψει τις υπάρχουσες ανάγκες.

Η MobileIP είναι μια εφαρμογή που δίνει την δυνατότητα σε μια συσκευή να αλλάξει το σημείο μέσω του οποίου συνδέεται στο Internet. Όταν ένα κινητός κόμβος (MobileNode) βρίσκεται σε διαφορετικό δίκτυο παίρνει μια τοπική διεύθυνση Care of Address (CoA). Έπειτα ο κινητός κόμβος στέλνει την CoA στο τοπικό δίκτυο (Home Agent) του νέου δικτύου προκειμένου αυτός να την δεσμεύσει ώστε να μην δοθεί αυτή η διεύθυνση κάπου αλλού προσωρινά. Μόλις ολοκληρωθεί η δέσμευση ο Home Agent προωθεί πακέτα στον Κινητό Κόμβο μέσω ενός τούνελ (tunnel) στην διεύθυνση CoA που έχει δηλώσει. Καθώς ο κινητός κόμβος (MN) κινείται μεταξύ διαφορετικών δικτύων στέλνει ενημερώσεις δέσμευσης (Binding Updates) με την CoA. Για να εξαλειφθούν προβλήματα δρομολόγησης το IPv6 έχει ενσωματωμένα συστήματα ασφαλείας τα οποία εξακριβώνουν ποιος είναι ο κινητός κόμβος και με ποια διεύθυνση επικοινωνεί. Ο κινητός κόμβος μπορεί να ειδοποιεί και οποιονδήποτε άλλο κόμβο του στέλνει πακέτα, έτσι ώστε να του τα στέλνει στην προσωρινή και όχι στην home διεύθυνση.

1.3.4. Αύξηση Αποδοτικότητας

Μαζί με τις άλλες βελτιώσεις που παρατηρούμε στο νέο πρωτόκολλο συναντάμε και βελτίωση στην αποδοτικότητα. Η αποδοτικότητα αυξήθηκε κατά πολύ στο νέο πρωτόκολλο καθώς διατηρήθηκαν τα θετικά στοιχεία από το IPv4, άλλα με μικρές αλλαγές και άλλα βελτιωμένα, τα ανεπιθύμητα χαρακτηριστικά αφαιρέθηκαν και προστέθηκαν νέα και καλύτερα.

Κάποια από αυτά είναι:

- σταθερό μήκος κεφαλίδας που έχει ως αποτέλεσμα την εύκολη διαχείριση και την μείωση της πολυπλοκότητας.
- στη δρομολόγηση το πακέτο δεν χρειάζεται να διασπάται σε μικρότερα κομμάτια και επίσης μπορούν να ενημερώνουν ώστε να δέχονται πακέτα μικρότερου μεγέθους
- στο IPV4 όταν μια συσκευή ήθελε να επεξεργαστεί ένα μήνυμα διακόπτονταν όλες οι συσκευές που ήταν συνδεδεμένες εκείνη την στιγμή, στο IPV6 όμως λόγω του μηχανισμού Multicast διακόπτονται μόνο αυτές που θέλουν να κάνουν την επεξεργασία και οι άλλες παραμένουν συνδεδεμένες.

1.3.5. Ασφάλεια

Αρχικός σκοπός σχεδίασης του IPv4 ήταν η επικοινωνία μεταξύ των ακαδημαϊκών ιδρυμάτων για αυτό δεν φάνηκε απαραίτητο εξαρχής στους σχεδιαστές να περιλάβουν τον τομέα της ασφάλειας στο σχεδιασμό του πρωτοκόλλου. Στην συνέχεια όμως, που άρχισε να επεκτείνεται η χρήση του και να χρησιμοποιείται σε διάφορους τομείς, όπως είναι οι επιχειρήσεις, οι οργανισμοί, το εμπόριο και άλλα, η ασφάλεια έγινε βασικός παράγοντας. Έτσι ο IETF άρχισε να ερευνά για προσαρμογές εργαλείων και τροποποιήσεις ώστε να εξασφαλισθεί η ασφάλεια των δεδομένων στο διαδίκτυο. Έγιναν πολλές προσπάθειες ώσπου δημιούργησαν το IPSecurity (IPSec). Η IPSec χρησιμοποιείται για την ασφαλή μετάδοση δεδομένων μεταξύ υπολογιστών και εφαρμόζεται στο επίπεδο δικτύου 3. Το πρωταρχικό όφελος της διασφάλισης των πληροφοριών στο επίπεδο 3 είναι ότι όλα τα προγράμματα και οι υπηρεσίες που

χρησιμοποιούν το πρωτόκολλο IP για μεταφορά δεδομένων μπορούν να προστατευτούν κι έτσι δεν υπάρχει κίνδυνος αυτά τα δεδομένα να τροποποιηθούν ή να αλλοιωθούν μετά την μεταφορά τους.

Αυτό που κάνει δηλαδή είναι να κρυπτογραφεί τα δεδομένα. Η χρήση του διαφέρει από το πρωτόκολλο IPv4 στο IPv6 και αυτό γιατί στο IPv4 η υποστήριξη ασφάλειας είναι προαιρετική και έτσι η υποστήριξη του πρωτοκόλλου IPSec είναι κάτι επιπλέον άρα χρησιμοποιείται το πεδίο IPOptions πράγμα που αυξάνει την πολυπλοκότητα. Επίσης ένα άλλο πρόβλημα στο IPv4 είναι ότι η χρήση του NAT (Network Address Translation) διακόπτει την λειτουργία που λέγεται endtoend επικοινωνία του IPSec, πράγμα που είναι απαραίτητο για να είναι πλήρως αποδοτικό. Αυτό γίνεται γιατί με την μετάφραση που κάνει ο NAT η αρχική IP διεύθυνση αλλάζει και δεν είναι η ίδια με την τελική και έτσι η IPSec δεν μπορεί να ανταπεξέλθει.

Στο IPv6 δεν αντιμετωπίζουμε τέτοια προβλήματα καθώς η υποστήριξη της ασφάλειας είναι ενσωματωμένη. Ακόμα οι μηχανισμοί ασφαλείας που χρησιμοποιεί το IPv6 μπορούν να χρησιμοποιηθούν και από άλλους μηχανισμούς ενώ στο IPv4 για κάποια αλλαγή όπως μια επέκταση ή μια τροποποίηση του, πρέπει ο μηχανισμός να εξασφαλίζει μηχανισμούς ασφαλείας. Ένα άλλο θέμα όσον αφορά την ασφάλεια, που είναι καλύτερο το IPv6 είναι οι ιοί και συγκεκριμένα οι ιοί worm, δηλαδή κακόβουλα προγράμματα που προκαλούν πολλές βλάβες στους υπολογιστές καθώς και στα δεδομένα αυτών, επιβραδύνουν την ταχύτητα των υπολογιστών και τους χρησιμοποιούν για δικούς τους σκοπούς όπως για παράδειγμα να μεταδώσουν τον ιό σε άλλο υπολογιστή. Επειδή στο IPv4 οι συσκευές σε ένα υποδίκτυο μπορούσαν να έχουν το πολύ 16bit ήταν πολύ εύκολο για έναν ιό να σαρώσει όλες τις συσκευές του υποδικτύου σε πολύ λίγο χρόνο ενώ στο IPv6 η διεύθυνση υποδικτύου είναι 64 bit με αποτέλεσμα να είναι αδύνατη η επίθεσή του, καθώς είναι σαν να πρέπει να σαρώσει δύο φορές όλο το IPv4 διαδίκτυο.

1.3.6. Quality of Service (QoS)

Ένας βασικός τομέας που χρειαζόταν αναβάθμιση στο IPv4 ήταν αυτός της ποιότητας των υπηρεσιών (Quality of Service ή QoS) γιατί υπήρχαν κάποια προβλήματα που έπρεπε να αντιμετωπισθούν. Το IPv4 μπορούσε να υποστηρίξει μηχανισμούς QoS στο επίπεδο δικτύου χρησιμοποιώντας το πεδίο type of service που βρίσκεται στην επικεφαλίδα του, το οποίο φανερώνει ποιο είδος υπηρεσίας απαιτεί η κάθε εφαρμογή, κάτι που δυσκόλευε το έργο των διαχειριστών του πρωτοκόλλου αλλά και των κατασκευαστών των εφαρμογών καθώς ο κάθε δρομολογητής έπρεπε να ξέρει λεπτομέρειες για τον αριθμό των μονοπατιών που έπρεπε να ακολουθήσει το πακέτο ώστε να φτάσει στον προορισμό του, έχοντας ως αποτέλεσμα την μείωση της απόδοσης.

Ακόμα στο IPv4 αν κάποιος δρομολογητής ήθελε να ενημερωθεί για μια ροή τότε έπρεπε να κάνει αναγνώριση και ανάλυση των κόμβων που εμπλέκονταν στην επικοινωνία καθώς επίσης και να ακολουθήσει την ίδια διαδικασία και για τη θύρα στην επικεφαλίδα του πρωτοκόλλου μεταφοράς. Με όλη αυτή την επεξεργασία που έπρεπε να κάνουν οι δρομολογητές αύξαναν το φόρτο και κατά συνέπεια το κόστος, έχοντας ως αποτέλεσμα την αλλοίωση της ποιότητας της υπηρεσίας.

Το IPv6 για να αντιμετωπίσει αυτά τα προβλήματα σχεδιάστηκε με τέτοιο τρόπο ώστε να είναι πιο αποτελεσματικό και πιο εύχρηστο. Στην επικεφαλίδα του εισήχθησαν δύο νέα πεδία για αυτό το σκοπό, τα οποία είναι τα Traffic class και Flow label (Ετικέτα ροής), και είναι απαραίτητα για την υποστήριξη μηχανισμών και υπηρεσιών με συγκεκριμένες απαιτήσεις ποιότητας. Στην ετικέτα ροής βρίσκονται όλα τα στοιχεία που χρειάζεται ένας δρομολογητής προκειμένου να δρομολογήσει ένα πακέτο στον προορισμό του και έτσι δε χρειάζεται να ψάχνει τα άλλα πεδία. Αυτό έχει ως αποτέλεσμα την καλύτερη απόδοση σε σύντομο χρόνο με λιγότερο κόστος.

Ένας άλλος λόγος που χρήζει απαραίτητη και αποδοτική την QoS είναι οι συνεχής αύξηση νέων δικτυακών εφαρμογών πολυμέσων. Οι εφαρμογές αυτές επί το πλείστον περιλαμβάνουν εικόνα και ήχο καθώς και αλληλεπίδραση μεταξύ των συμμετεχόντων, πράγμα που απαιτεί επικοινωνία σε πραγματικό χρόνο (real time). Αυτό σημαίνει ότι ο όγκος των πληροφοριών είναι πολύ μεγάλος και για να διατηρείται η ροή αυτών των πληροφοριών μέσω του Internet χωρίς διακοπές, το IP πρέπει να αποφεύγει την συχνή αλλαγή δρομολογίων και

πρέπει να διατηρεί ένα σταθερό ρυθμό bit, σε τακτά χρονικά διαστήματα κατά τη διάρκεια της μετάδοσης.

Επίσης η ποιότητα του αποτελέσματος επηρεάζεται κατά πολύ από την καθυστέρηση που μπορεί να υπάρξει κατά την μεταφορά της πληροφορίας. Αυτοί είναι οι δύο λόγοι οι οποίοι δυσκολεύουν τη χρήση των εφαρμογών αυτών από το IPv4 το οποίο δεν έχει σχεδιαστεί για μεταφορά πληροφοριών σε πραγματικό χρόνο. Έτσι το IPv6 σχεδιάστηκε με τέτοιο τρόπο ώστε να μπορεί να ανταπεξέλθει σε αυτές τις ανάγκες αναπτύσσοντας ειδικούς μηχανισμούς για αυτό το σκοπό.

1.4. Σύγκριση IPv4 - IPv6

Το πρωτόκολλο IPv6 διατηρεί πολλά από τα χαρακτηριστικά της σχεδίασης που έκαναν το IPv4 τόσο επιτυχημένο. Όπως και το IPv4, το IPv6 είναι ασυνδεσμικό (connectionless) δηλαδή κάθε αυτοδύναμο πακέτο περιέχει μια διεύθυνση προορισμού, και δρομολογείται ανεξάρτητα. Η κεφαλίδα ενός αυτοδύναμου πακέτου περιέχει έναν μέγιστο αριθμό αλμάτων τα οποία μπορεί να κάνει το αυτοδύναμο πακέτο πριν αποβληθεί και ακόμα το IPv6 διατηρεί τις περισσότερες από τις γενικές λειτουργίες που παρέχονται από τις επιλογές του IPv4.

Αν και διατηρεί τις βασικές έννοιες της τρέχουσας έκδοσης ,το IPv6 αλλάζει όλες τις λεπτομέρειες. Για παράδειγμα το IPv6 χρησιμοποιεί μεγαλύτερες διευθύνσεις. Αντί για 32 bit, κάθε διεύθυνση του IPv6 περιέχει 128bit. Ο χώρος των διευθύνσεων είναι αρκετά μεγάλος ώστε να μπορεί να ανταποκρίνεται στην συνεχιζόμενη ανάπτυξη του Internet σε όλο τον κόσμο για πολλές δεκαετίες. Ακόμα η κεφαλίδα του αυτοδύναμου πακέτου εκτός του ότι είναι σταθερή σε αντίθεση με το IPv4 που μεταβάλλεται είναι και εντελώς διαφορετική, αφού σχεδόν όλα τα πεδία έχουν αλλάξει, κάποια έχουν αντικατασταθεί και άλλα έχουν αφαιρεθεί.

Συγκρίνοντας την επικεφαλίδα του IPv6 με την επικεφαλίδα του IPv4, αμέσως παρατηρούμε την απλοποίηση που έχει γίνει στην μορφή της επικεφαλίδας κρατώντας μόνο τις άκρως απαραίτητες πληροφορίες. Σαν αποτέλεσμα έχουμε διπλάσιο μήκος σε bit της επικεφαλίδας του IPv6 σε σχέση με το IPv4 παρόλο που το μέγεθος των διευθύνσεων έχει

τετραπλασιαστεί. Η επιλογές πλέον προστίθενται σαν επιπλέον επικεφαλίδες που ακολουθούν την επικεφαλίδα του IPv6 όταν αυτές χρειάζονται.

Οι σχεδιαστές, για να μειώσουν το χρόνο που ένας δρομολογητής χρειάζεται για να επεξεργαστεί ένα πακέτο, φρόντισαν ώστε:

- Οι δρομολογητές να χρειάζεται να επεξεργαστούν το πολύ μια επιπλέον επιλογή, ενώ οι υπόλοιπες να ελέγχονται μόνο από τον παραλήπτη του πακέτου.
- Το πακέτο να ξεκινάει από τον αποστολέα με κατάλληλο μέγεθος, ώστε να είναι δυνατή η μετάδοση του από όλες της τεχνολογίες δικτύου που πρόκειται να συναντήσει στην πορεία του, χρησιμοποιώντας την τεχνική αναζήτησης της μέγιστης δυνατής μονάδας πληροφορίας (Path MTU Discover).

Ένα αυτοδύναμο πακέτο στο IPv6 αποτελείται από την βασική κεφαλίδα, μια ή καμία κεφαλίδα επέκτασης (extension header) και τα δεδομένα, και αυτό γίνεται γιατί το νέο πρωτόκολλο κωδικοποιεί τα δεδομένα σε ξεχωριστές κεφαλίδες. Το IPv6 περιέχει μηχανισμούς που μπορούν να του παρέχουν υψηλής ποιότητας μετάδοση εικόνας και ήχου (real time) και τέλος είναι ένα επεκτάσιμο πρωτόκολλο. Αντίθετα από το IPv4, το πρωτόκολλο IPv6 δεν ορίζει όλα τα χαρακτηριστικά του. Οι σχεδιαστές το έχουν εφοδιάσει με έναν μηχανισμό που επιτρέπει σε έναν αποστολέα να τοποθετεί πρόσθετες πληροφορίες σε ένα αυτοδύναμο πακέτο. Ο μηχανισμός επέκτασης κάνει το IPv6 πιο ευέλικτο από το IPv4 και σημαίνει ότι μπορούν να προστίθενται νέα χαρακτηριστικά στην σχεδίαση, ανάλογα με τις ανάγκες.

Η δυνατότητα μεγάλων IP πακέτων (Jumbograms) που επιτρέπει το μεγέθους του IP πακέτου να ξεπεράσει το όριο των 65kb που θέτει το IPv4 επιτρέπει την καλύτερη εκμετάλλευση των νέων τεχνολογιών δικτύων υψηλών ταχυτήτων όπως ATM, GigaBit Ethernet, κ.α.

Τέλος, το IPv6 προσφέρει:

- Απλοποίηση της διαχείρισης και του configuration του IPv6 multicast, παρέχοντας επιπλέον και καλύτερη κλιμάκωση (scaling) με χρήση του Rendezvous Point (PR).
- Καλύτερες προϋποθέσεις για multihoming, λόγω των πολλαπλών unicast διευθύνσεων ανά Interface, της χρήσης των site-local διευθύνσεων εντός του site και των πλέον καθορισμένων και διαχωρισμένων TLAs για τον κάθε ISP.

Συγκρίνοντας τα δύο πρωτόκολλα συμπεραίνουμε ότι το IPv6 υπερτερεί του IPv4 σε πολλούς τομείς και ότι είναι το κατάλληλο πρωτόκολλο για να ανταπεξέλθει στις νέες απαιτήσεις που δημιουργούνται διαρκώς.

ΚΕΦΑΛΑΙΟ 2

2.Οργανισμοί Διαχείρισης του Internet (RIRs)

2.1. Τι είναι ο IANA

Ο IANA (Internet Assigned Numbers Authority) είναι ένας οργανισμός υπό την εποπτεία του ICANN, που είναι υπεύθυνος για το συντονισμό μερικών βασικών στοιχείων που διατηρούν την ομαλή λειτουργία του Διαδικτύου. Ενώ το Διαδίκτυο είναι γνωστό ως ένα παγκόσμιο δίκτυο χωρίς κεντρικό συντονισμό, υπάρχει τεχνική ανάγκη για ορισμένα βασικά τμήματα του Διαδικτύου να συντονίζονται σε παγκόσμιο επίπεδο, και αυτός ο συντονιστικός ρόλος έχει αναληφθεί από τον IANA. Συγκεκριμένα, ο IANA διαθέτει και διατηρεί μοναδικούς κωδικούς και συστήματα αρίθμησης που χρησιμοποιούνται στις τεχνικές προδιαγραφές (πρωτόκολλα) που οδηγούν το Διαδίκτυο. Οι διάφορες δραστηριότητες του IANA μπορούν γενικά να ομαδοποιηθούν σε τρεις κατηγορίες (Davies 2008) :

Ονοματοδοσία: Ο IANA διαχειρίζεται το DNS roots δηλαδή ένα δίκτυο από εκατοντάδες servers σε πολλές χώρες σε όλο τον κόσμο. Έχουν διαμορφωθεί στη DNS root zone ως 13 ονομαζόμενες αρχές, μια εκ των οποίων είναι και ο ICANN με hostname l.root-servers.net και IP διεύθυνση 199.7.83.42, 2001:500:3::42 .

Το DNS(Domain Name System) είναι ένα σύστημα με το οποίο αντιστοιχίζονται οι διευθύνσεις IP σε hostnames. Τα ονόματα περιοχών όπως και οι διευθύνσεις IP που αναπαριστούν είναι μοναδικά, έχουν μια ιεραρχία και διαβάζονται από αριστερά προς τα δεξιά. Η σχέση μεταξύ ενός ονόματος και μιας διεύθυνσης δεν είναι 1 προς 1, δηλαδή σε ένα όνομα μπορεί να αντιστοιχούν πολλές IP διευθύνσεις. Για παράδειγμα η διεύθυνση www.google.gr αντιστοιχεί σε τρείς IP διευθύνσεις, την 66.102.9.99, την 66.102.9.104 και την 66.102.9.147. Σε αυτήν την περίπτωση έχουμε τρεις εξυπηρετητές που λειτουργούν ταυτόχρονα εκτελώντας την ίδια εργασία αλλά μοιράζονται το φόρτο εργασίας δια τρία .

Αριθμός Πόρων: Ο IANA συντονίζει το παγκόσμιο απόθεμα των IP και τους ASNumbers, παρέχοντάς τους σε περιφερειακά μητρώα του Internet (RIR).

Εργασίες πρωτοκόλλου:

Τα συστήματα αρίθμησης πρωτοκόλλων του Διαδικτύου διαχειρίζονται από τον IANA σε συνεργασία με τους οργανισμούς τυποποίησης. Ο IANA είναι ένα από τα παλαιότερα ιδρύματα του Διαδικτύου , με τις δραστηριότητές του να χρονολογούνται από τη δεκαετία του 1970.

Σήμερα είναι ένα σύνολο υπηρεσιών που παρέχονται από τον Internet Corporation for Assigned Names and Numbers (ICANN), έναν διεθνώς οργανωμένο μη κερδοσκοπικό οργανισμό που έχει συσταθεί από την κοινότητα του Διαδικτύου για να βοηθήσει στο συντονισμό των περιοχών που είναι υπό την ευθύνη του IANA .

2.2. Τι είναι ο ICANN

Η αποστολή του ICANN είναι να εξασφαλίσει ένα σταθερό και ενιαίο παγκόσμιο διαδίκτυο. Για να εντοπίσεις ένα άλλο πρόσωπο στο διαδίκτυο θα πρέπει να πληκτρολογήσεις μια διεύθυνση στον υπολογιστή είτε όνομα είτε αριθμό. Η διεύθυνση θα πρέπει να είναι μοναδική, έτσι οι υπολογιστές γνωρίζουν που θα βρουν ο ένας τον άλλο. Ο ICANN συντονίζει αυτά τα μοναδικά αναγνωριστικά σε όλο τον κόσμο. Χωρίς αυτό το συντονισμό δεν θα είχαμε ένα παγκόσμιο Internet.

Ο ICANN ιδρύθηκε το 1998. Είναι ένας μη κερδοσκοπικός οργανισμός κοινής ωφέλειας με συμμετέχοντες απ’ όλο τον κόσμο, αφιερωμένος στην ασφαλή σταθερή και διαλειτουργική διατήρηση του διαδικτύου. Προωθεί τον ανταγωνισμό και αναπτύσσει πολιτική μοναδικών αναγνωριστικών του διαδικτύου. Ο ICANN δεν ελέγχει το περιεχόμενο του διαδικτύου και δεν ασχολείται με την πρόσβαση σε αυτό. Επίσης δεν μπορεί να σταματήσει τα σπαμ. Παρόλα αυτά όμως λόγω του σημαντικού ρόλου του στην ονοματοδοσία του συστήματος του διαδικτύου, δεν έχουν σημαντικό αντίκτυπο στην ανάπτυξη και την εξέλιξη του διαδικτύου.

Στον παρακάτω πίνακα παρουσιάζεται μια λίστα από διευθύνσεις IPv6 τις οποίες διαχειρίζεται ο ICANN.

PREFIX	DESIGNATION	DATE	STATUS
5F00::/8	IANA	2008-04	Reserved
3FFE::/16	IANA	2008-04	Reserved
2C00:0000::/12	AFRINIC	2006-10	Allocated
2A00:0000::/12	RIPE NCC	2006-10	Allocated
2800:0000::/12	LACNIC	2006-10	Allocated
2600:0000::/12	ARIN	2006-10	Allocated
2400:0000::/12	APNIC	2006-10	Allocated
2620:0000::/12	ARIN	2006-09	Allocated
2001:B000::/12	APNIC	2006-03	Allocated

Πίνακας 5 - Μια λίστα δείγματος από κρατημένες διευθύνσεις IPv6 διατιθέμενες από τον ICANN

2.3. Τι είναι τα RIRS

Κάθε υπολογιστής που θέλει να συνδεθεί στο διαδίκτυο απαιτεί την δίκη του διεύθυνση IP είτε είναι στην Αφρική είτε είναι στην Αμερική. Αυτό είναι μια ακραία πρόκληση. Πως μπορεί ένας χρήστης με υπολογιστή στην Αφρική ή στην Αμερική να πάρει μια διεύθυνση IP; Μπορεί ένα σύστημα να τα χειριστεί όλα για όλους σε όλο τον κόσμο; Η απάντηση είναι πως δεν γίνεται και γι'αυτό το λόγο υπάρχει η Περιφερειακή Γραμματεία του Διαδικτύου (Regional Internet Registry ή RIR).

Μια RIR είναι ένας οργανισμός που διαχειρίζεται και ελέγχει τις διευθύνσεις στο Internet σε μια συγκεκριμένη περιοχή, συνήθως μια χώρα και μερικές φορές μια ολόκληρη ήπειρο. Τα RIRs ελέγχουν την ανάθεση και την κατανομή διευθύνσεων IP και τις κατοχυρώσεις. Καθώς το Διαδίκτυο επεκτάθηκε σε ολόκληρο τον κόσμο, η μεγαλύτερη οργάνωση ήταν

απαραίτητη για να ανταπεξέλθει στη ζήτηση για διευθύνσεις IP για τους αυξανόμενους κατά εκατομμύρια online χρήστες .

Υπάρχουν πέντε περιφερειακά μητρώα του Internet.

1) American Registry for Internet Number (ARIN): Ο οργανισμός αυτός είναι υπεύθυνος για την διαχείριση των διευθύνσεων και την ονοματοδοσία του διαδικτύου για την Βόρεια Αμερική, συμπεριλαμβανομένου του Καναδά, των Ηνωμένων Πολιτειών και τμημάτων της Καραϊβικής.

2) Réseaux IP Européens Network Coordination Centre (RIPENCC): αυτός ο οργανισμός είναι υπεύθυνος για την διαχείριση και την ονοματοδοσία του διαδικτύου για την Ευρώπη, τη Μέση Ανατολή και την Κεντρική Ασία. Ο RIPE NCC θεωρείται το πρώτο επίσημο μητρώο IP.

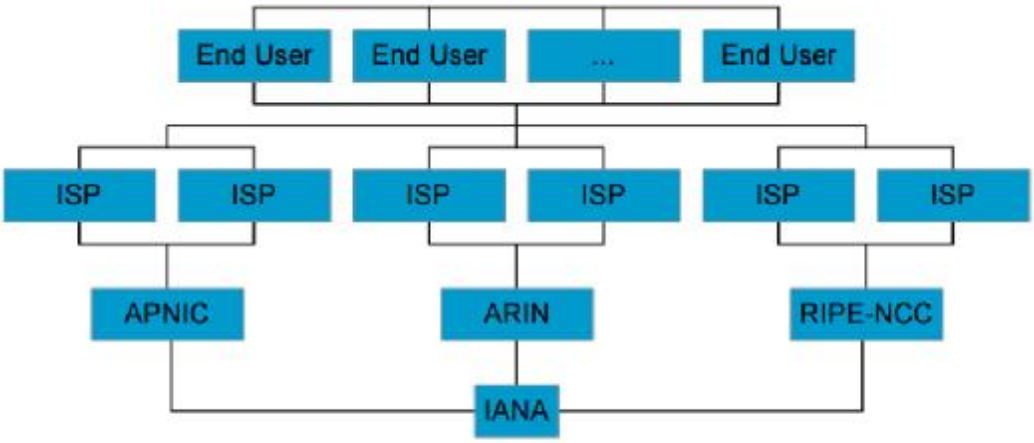
3) The Asia Pacific Network Information Centre (APNIC)**:** Υπεύθυνος για τη διαχείριση των διευθύνσεων του Διαδικτύου και την ονοματοδοσία για την Ασία και τον Ειρηνικό. Ο APNIC ήταν ο δεύτερος RIR που καθιερώθηκε. Ιδρύθηκε στο Τόκιο, Ιαπωνία αλλά μεταφέρθηκε στο Brisbane της Αυστραλίας, το 1998 .

4) Latin American and Caribbean Internet Address Registry (LACNIC): Υπεύθυνος για την διαχείριση των διευθύνσεων και την ονοματοδοσία του Διαδικτύου για τη Λατινική Αμερική και την Καραϊβική. Με έδρα στο Μοντεβιδέο της Ουρουγουάης.

5) The African Network Information Centre (AFRINIC): Υπεύθυνος για την διαχείριση και την ονοματοδοσία των διευθύνσεων του Διαδικτύου για την αφρικανική ήπειρο. ΟAFRINIC άρχισε να λειτουργεί το 2005.

Registry	Area Covered
AFRINIC	Africa Region
APNIC	Asia/Pacific Region
ARIN	North America Region
LACNIC	Latin America and some Caribbean Islands
RIPE NCC	Europe, the Middle East, and Central Asia

Στο παρακάτω σχήμα παρουσιάζεται η ιεραρχία του διαδικτύου όσον αφορά τους οργανισμούς διαχείρισης παγκοσμίως:



Σχήμα 2 - Internet Hierarchy (Bottom Up View)

2.3.1. Οι στόχοι των οργανισμών RIRS

Υπάρχουν εκατομμύρια διαθέσιμες διευθύνσεις IP, αλλά ο αριθμός αυτός δεν είναι απεριόριστος. Η τρέχουσα έκδοση της διεύθυνσης IP, η IPv4 δεν έχει έναν άπειρο αριθμό διαθέσιμων διευθύνσεων. Το γεγονός αυτό έκανε τον οργανισμό διαχείρισης του διαδικτύου να συνειδητοποιήσει ότι υπάρχει επείγουσα ανάγκη για έξυπνη απογραφή των διευθύνσεων IP. Με άλλα λόγια ο κόσμος των IP κατάλαβε ότι έπρεπε να υπάρξει ένα σύστημα για την αποτελεσματική τους κατανομή έτσι ώστε να φτάσουν για όλους. Γι'αυτό είναι υπεύθυνα τα RIRS. Κάθε ένα από τα πέντε RIRS που υπάρχουν οφείλει να ακολουθήσει μια ουδέτερη πολιτική εκχώρησης διευθύνσεων IP και διανομής αυτών. Έτσι λοιπόν χωρίς την διαρκή πρόσβαση σε διευθύνσεις IP, η οποία επιτρέπει στους ανθρώπους να επικοινωνούν με άλλους χρήστες σε τοπικό όσο και σε παγκόσμιο επίπεδο, ένα δίκτυο είναι καταδικασμένο.

Το RFC 2050 που δημοσιεύτηκε τον Νοέμβριου του 1996, παρουσίασε μια συνεργασία της παγκόσμιας κοινότητας διευθυνσιοδότησης του διαδικτύου ώστε να περιγράψει τους στόχους και τις κατευθυντήριες οδηγίες των οργανισμών RIRs. Ενώ ο IANA προοριζόταν ως ο μοναδικός οργανισμός που θα ήταν υπεύθυνος για ολόκληρη την λίστα διευθύνσεων, το RFC 2050 θεώρησε ότι οι οργανισμοί RIR θα εργάζονται κάτω από την επίβλεψη ολόκληρης της κοινότητας regional Internet. Αυτή η δημοσίευση με τον συνδυασμό του συντονισμού των RIR ήταν καθοριστικής σημασίας για να στηθεί η βάση των παγκόσμιων αρχών.
Οι τρείς βασικοί στόχοι των συστημάτων RIR είναι:

- Διατήρηση: Η εξασφάλιση της αποδοτικής χρήσης των πόρων (που δεν είναι απεριόριστοι) ώστε να αποφευχθεί οποιαδήποτε δυσλειτουργία στις υπηρεσίες και στην αγορά.
- Συσσωμάτωση: Η υποστήριξη της διατήρησης της λειτουργίας δρομολόγησης του διαδικτύου με την χρήση ενός διαχειρίσιμου σε μέγεθος πίνακα δρομολόγησης, όπως επίσης και η χρήση των τεχνικών CIDR ώστε να διασφαλισθεί η σταθερότητα στο διαδίκτυο.
- Καταχώρηση: Η παροχή ενός ενιαίου χώρου διευθυνσιοδότησης με κατάλληλη υποστήριξη οδηγιών, με κατάλληλες διανομές και αναθέσεις, απαραίτητες για να

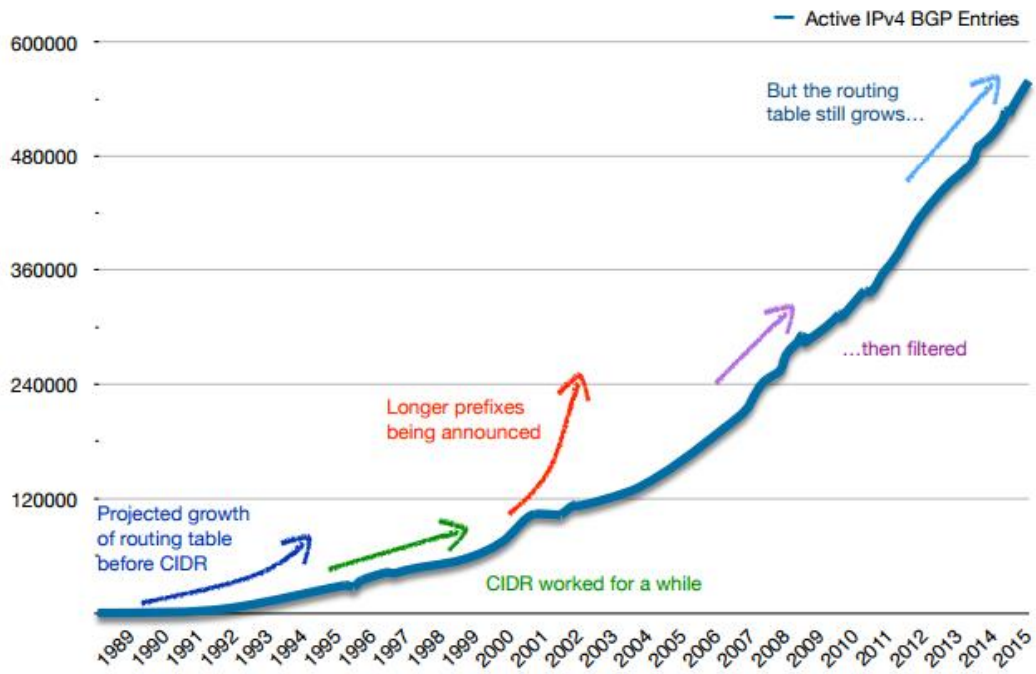
διασφαλισθεί η μοναδικότητα και η παροχή πληροφοριών σε περίπτωση οποιονδήποτε προβλημάτων που θα παρουσιαζόταν σε όλα τα επίπεδα.

Οι οργανισμοί RIR στην πραγματικότητα δεν δημιουργούν οι ίδιοι τις διευθύνσεις τους. Ο IANA είναι ο οργανισμός ο οποίος που μπορεί να αναθέσει τις IP διευθύνσεις σε κάθε ένα από τους πέντε οργανισμούς RIR και στην συνέχεια ο εκάστοτε οργανισμός RIR διαχειρίζεται τις διευθύνσεις με ανάλογο τρόπο στο επόμενο επίπεδο της κατανομής. Οι φορείς παροχής υπηρεσιών, ή αλλιώς οι λεγόμενοι ISP, άλλοι μεγάλοι οργανισμοί, εταιρίες εξυπηρετούνται από τους πέντε οργανισμούς RIR .

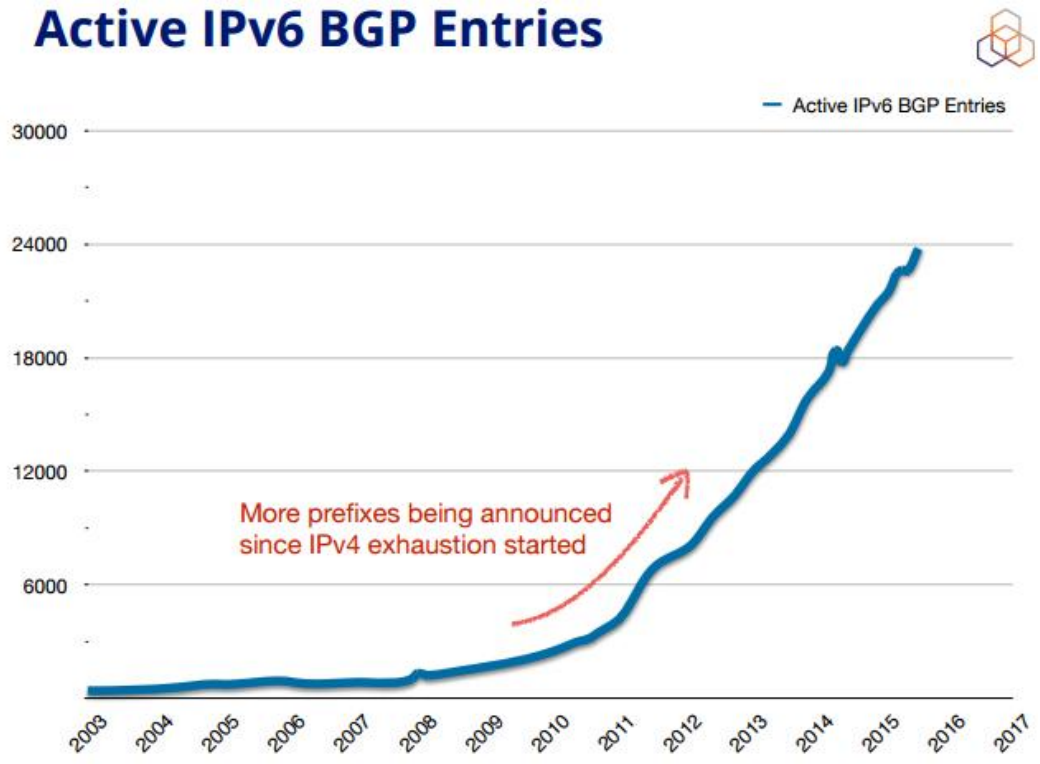
2.4. Τι είναι τα LIRS

Ένα τοπικό μητρώο στο Internet (Local Internet Registry ή LIR) είναι ένας οργανισμός στον οποίο εκχωρείται ένα μπλοκ διευθύνσεων IP από ένα περιφερειακό μητρώο Διαδικτύου (RIR) και αποδίδει περισσότερα μέρη αυτού του μπλοκ στους δικούς του πελάτες. Είναι υπεύθυνος για την κατανομή του χώρου διευθύνσεων και την καταγραφή αυτών σε τοπικό επίπεδο. Οι περισσότεροι LIRs είναι πάροχοι υπηρεσιών Διαδικτύου, επιχειρήσεις, ή ακαδημαϊκά ιδρύματα. Η συμμετοχή σε ένα περιφερειακό μητρώο στο Internet (RIR) είναι απαραίτητη για να γίνει ένα LIR .

2.5. Τρόποι διαχείρισης της εξάντλησης του IPv4.



Σχήμα3- Η σταδιακή εξάντληση των διευθύνσεων IP4



Σχήμα4- Ενεργές δοσμένες διευθύνσεις IPv6

2.5.1 Το πρόβλημα διευθυνσιοδότησης στο IPv4

Στον αρχικό σχεδιασμό του IPv4 η διευθυνσιοδότηση ήταν βασισμένη σε κλάσεις. Δηλαδή υπήρχαν 5 κατηγορίες διευθύνσεων, γνωστές ως κλάσεις, οι οποίες διακρίνονται από τα αρχικά bit της διεύθυνσης ως εξής:

ΚΛΑΣΕΙΣ	ΕΥΡΟΣ ΔΙΕΥΘΥΝΣΕΩΝ
A	0.0.0.0-127.255.255.255=0
B	128.0.0.0-191.255.255.255=10
C	192.0.0.0-223.255.255.255=110
D	224.0.0.0-239.255.255.255=1110
E	240.0.0.0-247.255.255.255=11110

Πίνακας 6 – Κλάσεις IPv4

Από αυτές τις κλάσεις οι τρείς πρώτες είναι οι κύριες και από αυτές δίδονται διευθύνσεις στους υπολογιστές υπηρεσίας. Η κλάση D χρησιμοποιείται για πολυεκπομπή (multicasting), κατά την οποία μπορούν να αποσταλούν τα ίδια δεδομένα σε πολλούς παραλήπτες-υπολογιστές ταυτόχρονα και η κλάση E είναι δεσμευμένη για μελλοντική χρήση.

Ο αριθμός των δικτύων και των υπολογιστών υπηρεσίας ανά δίκτυο για τις τρείς κύριες κλάσεις είναι οι εξής:

ΚΛΑΣΗ ΔΙΕΥΘΥΝΣΕΩΝ	**BIT ΣΤΟ ΠΡΟΘΕΜΑ**	**ΜΕΓΙΣΤΟΣ ΑΡΙΘΜΟΣ ΔΙΚΤΥΩΝ**	**BIT ΣΤΟ ΕΠΙΘΕΜΑ**	**ΜΕΓΙΣΤΟΣ ΑΡΙΘΜΟΣ ΥΠΟΛΟΓΙΣΤΩΝ ΥΠΗΡΕΣΙΑΣ ΑΝΑ ΔΙΚΤΥΟ**
A 1	7	$126(2^7-2)$	24	$16777216(2^{24}-2)$
B 10	14	$16384(2^{14}-2)$	16	$65536(2^{16}-2)$
C 110	21	$2097152(2^{21}-2)$	8	$256(2^8-2)$

Πίνακας 7

Όπως βλέπουμε λοιπόν η ανάθεση στο IPv4 γινόταν σε τμήματα σταθερού και προκαθορισμένου μεγέθους με αποτέλεσμα να δημιουργούνται κάποια προβλήματα. Τα προβλήματα αυτά είναι καταρχήν ότι με την ανάθεση μιας διεύθυνσης σε ένα φυσικό δίκτυο δεσμευόταν μια ολόκληρη περιοχή διευθύνσεων. Αυτός ο τρόπος ανάθεσης δεν είχε ευελιξία ώστε να μπορεί να προσαρμόζεται στις πραγματικές ανάγκες του δικτύου έχοντας ως αποτέλεσμα ότι ακόμα και σε ένα δίκτυο 255 υπολογιστών να πρέπει να παραχωρείται ένα δίκτυο της Β κλάσης το οποίο μπορούσε να υποστηρίξει 65.536 υπολογιστές δηλαδή 65.536-255=65.281 διευθύνσεις έμεναν ανεκμετάλλευτες.

Επίσης στην περίπτωση που κάποιος χρειαζόταν 70.000 διευθύνσεις θα έπρεπε να πάρει μία Κλάση Α δικτύου, κάνοντας σπατάλη πάνω από 16.700.000 διευθύνσεις δηλαδή δεσμευόταν ένα μεγάλο πλήθος διευθύνσεων, οι οποίες δεν πρόκειται να χρησιμοποιούνταν ποτέ. Αυτό είχε ως συνέπεια τη γρήγορη εξάντληση των διευθύνσεων κυρίως της Β κλάσης και την υπερφόρτωση των πινάκων δρομολόγησης, οι οποίοι διαρκώς γίνονταν πολυπλοκότεροι, αφού υπήρχαν περισσότερα δίκτυα και κατά συνέπεια περισσότερες διαδρομές. Προσπάθησαν ακόμα και να αυξήσουν τις λίστες των δρομολογητών αλλά το μέγιστο όριο εγγραφών δεν ξεπερνούσε τις 60.000. Όλα αυτά έπρεπε με κάποιο τρόπο να αντιμετωπιστούν διότι θα ήταν αναπόφευκτη η γρήγορη εξάντληση των IPv4 διευθύνσεων.

2.5.2. Τρόποι παράτασης ζωής του IPv4

Η εξάπλωση του διαδικτύου και η εξάντληση των IPv4 διευθύνσεων προχωρούσε με ραγδαίους ρυθμούς και έπρεπε οπωσδήποτε να βρεθεί μια λύση. Έτσι δόθηκαν κάποιες προσωρινές λύσεις από τους διαχειριστές ώστε να συνεχίσει να λειτουργεί σωστά το διαδίκτυο μέχρις ότου βρεθεί μια μόνιμη και καθοριστική λύση του προβλήματος. Οι κυριότερες λύσεις απ' αυτές ήταν:

- Η Υποδικτύωση
- Η Αντικατάσταση της Ταξικής από την Αταξική Δρομολόγηση Δικτυακών Περιοχών (Classless Inter Domain Routing ή CIDR)
- Η Μετάφραση Διευθύνσεων Δικτύου (Network Address Translation ή NAT).

2.5.2.1. Υποδικτύωση

Για να λυθεί το πρόβλημα της άσκοπης σπατάλης των διευθύνσεων δημιουργήθηκαν τα υποδίκτυα. Υποδικτύωση είναι η διαδικασία κατά την οποία από κάθε δίκτυο A,B ή C κλάσης προκύπτουν πολλά μικρότερα που λέγονται υποδίκτυα. Έτσι, με αυτό τον τρόπο, μειώνονται οι διευθύνσεις δικτύου που χρησιμοποιούνται και έχουμε εξοικονόμηση διευθύνσεων IP.

Για παράδειγμα: Ας πούμε ότι μια εταιρεία είχε 5 δίκτυα τοπικά τα οποία ήταν ανεξάρτητα μεταξύ τους και το κάθε ένα από αυτά είχε 24 κόμβους. Χωρίς την υποδικτύωση θα έπρεπε να δεσμευθούν 5 διαφορετικές διευθύνσεις από την κλάση C δηλαδή 256 διευθύνσεις και κατά συνέπεια 256-20=236 διευθύνσεις θα δεσμεύονταν για το κάθε δίκτυο άσκοπα. Με την υποδικτύωση όμως χρειάζεται μόνο μια διεύθυνση της τάξης C και οι 256 διευθύνσεις θα διαμοιρασθούν σε 2^5<= 32 για το κάθε δίκτυο της εταιρείας. Έτσι λοιπόν η δευθυνσιοδότηση γίνεται τριών επιπέδων και για να φτιάξουμε τα υποδίκτυα αφήνουμε τον αριθμό δικτύου ως έχει και παίρνουμε από τον αριθμό κόμβου όσα bit χρειαζόμαστε ανάλογα με τα υποδίκτυα που θέλουμε να δημιουργήσουμε. Έτσι ο αριθμός κόμβου μοιράζεται σε δύο:

i. στον αριθμό υποδικτύου

ii. και στον αριθμό κόμβου, όπως βλέπουμε και στον πίνακα.

Αριθμός δικτύου	Αριθμός κόμβου	
Αριθμός δικτύου	Αριθμός υποδικτύου	Αριθμός κόμβου

Πίνακας 7

Αυτό που βοηθάει στο να φτιάξουμε τα υποδίκτυα είναι η μάσκα υποδικτύου, η οποία μας δείχνει το πλήθος των bit που χρειάζονται για το υποδίκτυο. Τα bit που αντιστοιχούν στο πεδίο δικτύου και υποδικτύου παίρνουν την τιμή 1 ενώ στο πεδίο κόμβου παίρνουν την τιμή 0.

Κλάσεις	Bits δικτύου /κόμβου	Subnet Mask			
A	8/24	11111111	00000000	00000000	00000000
B	16/16	11111111	11111111	00000000	00000000
C	24/8	11111111	11111111	11111111	00000000

Πίνακας 8

Ένα παράδειγμα υποδικτύωσης είναι το εξής:

Έστω IP 195.148.100.0 και θέλουμε να δημιουργήσουμε 10 υποδίκτυα και να βρούμε την μάσκα υποδικτύου.

- Από το 195 φαίνεται ότι βρισκόμαστε στη κλάση C άρα τα 24bit είναι του δικτύου και τα 8 του κόμβου.
- Για να φτιάξουμε τα υποδίκτυα θα χρησιμοποιήσουμε κάποια bit από του κόμβου σύμφωνα με τον τύπο $2^n-2>=10$
- Για n=4 τα υποδίκτυα είναι 16, άρα θα χρησιμοποιήσω 4 bit από τον αριθμό κόμβου.
- Η προκαθορισμένη μάσκα για την C κλάση είναι η εξής:

11111111.11111111.11111111.00000000

Εμείς χρειαζόμαστε 4 bit από τον αριθμό κόμβου, άρα η μάσκα υποδικτύου θα είναι η εξής:

11111111.11111111.11111111.11110000 ή 255.255.255.240

Για να μετατρέψουμε τον δυαδικό σε δεκαδικό ακολουθούμε την εξής μέθοδο:

128	64	32	16	8	4	2	1
1	1	1	1	0	0	0	0

Πίνακας 9 – Κλάσεις IPv4

Γράφουμε το δυαδικό αριθμό και από πάνω βάζουμε αυτά τα νούμερα τα οποία είναι σταθερά και βρίσκονται πολλαπλασιάζοντας τον κάθε αριθμό με το 2 από δεξιά προς τα αριστερά κάθε φορά. Στην συνέχεια προσθέτουμε τα νούμερα που βρίσκονται πάνω από τους άσσους και έχουμε το δεκαδικό αριθμό που αντιστοιχεί στο δυαδικό, δηλαδή 128+64+32+16=240.

Η υποδικτύωση λοιπόν βοήθησε αρκετά στην άσκοπη διάθεση των διευθύνσεων αλλά αυτό δεν ήταν αρκετό από μόνο του έτσι αποφάσισαν να αλλάξουν και τον τρόπο ανάθεσης των διευθύνσεων προκειμένου να γίνεται ακόμα καλύτερη διαχείριση αυτών.

2.5.2.2. Αταξική Δρομολόγηση Δικτυακών Περιοχών (Classless Inter Domain Routing)

Το 1993 αναδομήθηκε ο τρόπος ανάθεσης των διευθύνσεων και από Ταξική Δρομολόγηση Δικτυακών Περιοχών περάσαμε στην αταξική. Αυτή η μέθοδος προσφέρει αποδοτικότερη διαχείριση των διευθύνσεων και μείωση του όγκου των πληροφοριών που αποθηκεύονται στους δρομολογητές. Δεν υφίσταται η έννοια της κλάσης με αποτέλεσμα τα τμήματα Δικτύου και Υπολογιστή κάθε διεύθυνσης να καθορίζονται κατά περίπτωση με βάση τις ανάγκες κάθε οργανισμού. Το μέγεθος των τμημάτων δικτύου και υπολογιστή μιας διεύθυνσης προσδιορίζονται από έναν αριθμό που συνοδεύει την διεύθυνση και δηλώνει το μέγεθος της μάσκας δικτύου. Αυτός ο αριθμός λέγεται πρόθεμα.

Για παράδειγμα: Την διεύθυνση 200.18.60.48/25, το /25 είναι το πρόθεμα δικτύου και σημαίνει ότι τα πρώτα 25 bits χρησιμοποιούνται για τον προσδιορισμό του δικτύου και τα υπόλοιπα 7 για τον προσδιορισμό του συγκεκριμένου υπολογιστή. Στην αταξική δρομολόγηση για να μην υπάρχουν πολλές καταχωρήσεις και γεμίζουν οι πίνακες δρομολόγησης γίνεται συσσωμάτωση των διευθύνσεων μέσω του προθέματος, δηλαδή όταν φτάνει ένα πακέτο απομονώνεται η διεύθυνση προορισμού του και με βάση τη μάσκα της εξετάζονται οι καταχωρήσεις στη λίστα

δρομολόγησης μία προς μία και όταν βρεθούν διευθύνσεις που να ταιριάζουν, το πακέτο αποστέλλεται στο δίκτυο που έχει το μακρύτερο πρόθεμα.

Και αυτή η τεχνική όμως δεν μπόρεσε να δώσει μακροχρόνια λύση στο πρόβλημα διότι δεν μπορούσε να εφαρμοστεί σε δίκτυα που είχαν αποδοθεί διευθύνσεις πριν την χρησιμοποίησή του, παρά μόνο σε αυτά που παραχωρήθηκαν διευθύνσεις μετά την εφαρμογή του, με αποτέλεσμα να έχει χαθεί άσκοπα μεγάλο πλήθος διευθύνσεων.

2.5.2.3. Μετάφραση Διευθύνσεων Δικτύου (Network Address Translation)

Ο Μεταφραστής Διευθύνσεων Δικτύου (ή NAT) σχεδιάστηκε για απλοποίηση και διατήρηση των IP διευθύνσεων αφού αυτό που κάνει είναι να επιτρέπει σε ιδιωτικά δίκτυα που χρησιμοποιούν μη εγγεγραμμένες IP διευθύνσεις να έχουν σύνδεση με το Internet. Το σύστημα NAT λειτουργεί σε κάποιον δρομολογητή, ο οποίος συνδέει συνήθως δύο δίκτυα και μεταφράζει τις ιδιωτικές (μη μοναδικές στον παγκόσμιο ιστό) διευθύνσεις του εσωτερικού δικτύου σε νόμιμες διευθύνσεις προτού τα πακέτα προωθηθούν σε άλλο δίκτυο. Σαν μέρος αυτής της λειτουργίας το NAT μπορεί να ρυθμιστεί να κάνει γνωστή μόνο μία διεύθυνση στον έξω κόσμο για ολόκληρο το δίκτυο που συνδέεται με αυτόν.

Αυτό το χαρακτηριστικό παρέχει επιπλέον ασφάλεια αφού κρύβει ολόκληρο το εσωτερικό δίκτυο από το κόσμο πίσω από μία διεύθυνση. Πιο αναλυτικά, όταν ένας υπολογιστής στο εσωτερικό δίκτυο ενός οργανισμού στέλνει ένα UDP/TCP πακέτο σ'έναν υπολογιστή στο διαδίκτυο, ο router του οργανισμού που λαμβάνει το πακέτο αποθηκεύει την source IP address και port number σε μια διαθέσιμη εγγραφή του πίνακα μετάφρασης διευθύνσεων. Ο router αντικαθιστά την source IP address με την δικιά του IP στο πακέτο και το source port number με ένα virtual port number, το οποίο είναι δείκτης στην εγγραφή του πίνακα που περιέχει τα στοιχεία διεύθυνσης του υπολογιστή-αποστολέα. Το πακέτο με τα αλλαγμένα IP και port number προωθείται από τον router προς τον παραλήπτη ενώ παράλληλα ο πίνακας μετάφρασης των διευθύνσεων παρέχει μια απεικόνιση από το virtual port number στη πραγματική IP address και port number του αποστολέα υπολογιστή στο εσωτερικό δίκτυο.

Αντίστροφα όταν ο router λαμβάνει ένα πακέτο χρησιμοποιεί το destination port number στο πακέτο για να βρει τη κατάλληλη εγγραφή στο πίνακα μετάφρασης. Έπειτα αντικαθιστά τα IP address και port number προορισμού στο πακέτο, με αυτά που κρατά ο

πίνακας για τον εσωτερικό υπολογιστή παραλήπτη του πακέτου και έτσι το πακέτο αποστέλλεται στον συγκεκριμένο υπολογιστή. Με αυτόν τον τρόπο πραγματοποιείται επικοινωνία με το πρωτόκολλο NAT. Αν και η χρήση του NAT είναι ευρεία, ο ρυθμός εξάντλησης των διευθύνσεων IPv4 εξακολουθεί να γίνεται επικίνδυνα υψηλός και αυτό διότι ολοένα και νέοι χρήστες συνδέονται στο Internet.

Το βασικό μειονέκτημα του NAT είναι ότι με την χρήση του ορισμένες εφαρμογές δεν λειτουργούν σωστά. Ένα άλλο μειονέκτημα του είναι ότι δημιουργεί προβλήματα πολυλπλοκότητας με τα πρωτόκολλα tunneling. Επίσης το NAT παραβιάζει την end to end συνδεσιμότητα η οποία είναι μία από τις αρχές του Internet.

2.6. Μηχανισμοί μετάβασης στο IPV6

Λόγω των προβλημάτων συμβατότητας των πρωτοκόλλων IPv4 και IPv6 η ανάγκη ύπαρξης μηχανισμών ήταν επιτακτική. Οι τεχνικές οι οποίες δημιουργήθηκαν για να είναι συμβατά τα δυο πρωτόκολλα είναι οι ακόλουθες :

- Οι μηχανισμοί «διπλής στοίβας»(dualstack)
- Οι μηχανισμοί «σήραγγας» (tunneling) και
- Οι μηχανισμοί «μετάφρασης» (translation).

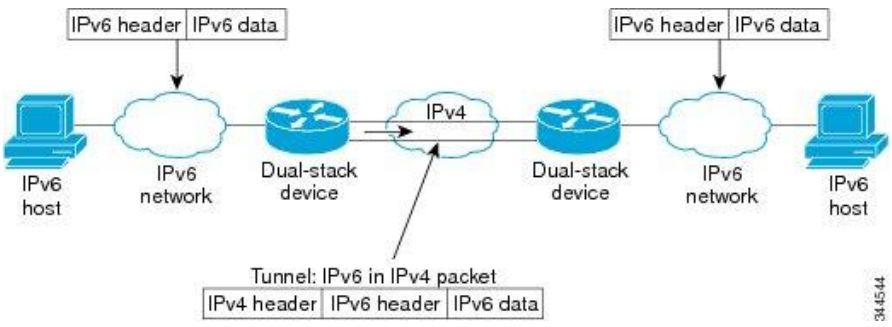
2.6.1. Μηχανισμοί Dual Stack (Διπλής Στοίβας)

Οι μηχανισμοί αυτοί θεωρούνται από τους πιο απλούς στην εφαρμογή τους και το μόνο που προϋποθέτουν είναι εγκατάσταση και των δύο πρωτοκόλλων στα λειτουργικά συστήματα των υπολογιστών ή δρομολογητών. Έτσι μπορούν να λάβουν και να προωθήσουν πακέτα και από τα δύο πρωτόκολλα και η επιλογή της στοίβας που θα χρησιμοποιηθεί κάθε φορά καθορίζεται από το ποιο θα είναι το αποτέλεσμα της DNS αναζήτησης, δηλαδή αν ο κόμβος που επικοινωνεί έχει μόνο IPv6 διεύθυνση τότε θα χρησιμοποιηθεί και η αντίστοιχη στοίβα IPv6 ενώ αν υπάρχει μόνο IPv4 διεύθυνση τότε θα χρησιμοποιηθεί IPv4 στοίβα. Τώρα στη περίπτωση που υπάρχουν εγγραφές και των δύο διευθύνσεων θα επιλεγεί επικοινωνία με τη στοίβα IPv6. Αυτός

ο μηχανισμός όμως, παρουσιάζει κάποια προβλήματα στην παρούσα φάση που βρισκόμαστε λόγω του πεπαλαιωμένου εξοπλισμού, καθώς για να εγγράψει ένας κόμβος την IPv6 την σύνδεση του δεν αρκεί μόνο η αρχική εγκατάσταση του IPv6 πρωτοκόλλου αλλά είναι απαραίτητη και η παροχή σύνδεσης IPv6 με κάποιο τρόπο και αυτό επιτυγχάνεται μόνο με την διαμεσολάβηση κάποιου άλλου μηχανισμού μετάβασης όπως του tunneling, μέχρις ότου εξαπλωθεί το IPv6 και οι περισσότερες συσκευές να μπορούν να το υποστηρίξουν. Τότε ο μηχανισμός Dual Stack θα γίνει ο κυρίαρχος μηχανισμός μετάβασης.

2.6.2.Μηχανισμοί Tunneling (Σήραγγας - IPv6 in IPv4)

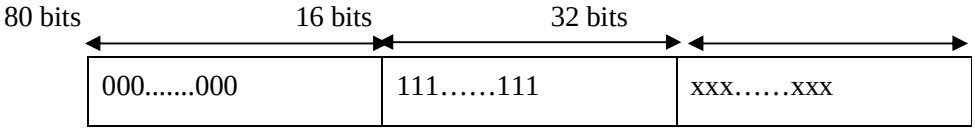
Οι μηχανισμοί tunneling είναι τεχνικές κατά τις οποίες γίνεται ενθυλάκωση IPv6 πακέτων σε IPv4 έτσι ώστε να επιτευχθεί επικοινωνία μεταξύ των δύο πρωτοκόλλων. Τα πακέτα αυτά, αφού ενθυλακωθούν προωθούνται και ταξιδεύουν μέσα στο δίκτυο έως ότου βρεθεί κάποιος κόμβος ο οποίος υποστηρίζει το IPv6 πρωτόκολλο και μπορέσει να τα επεξεργαστεί. Υπάρχουν διάφορες τεχνικές tunneling οι οποίες διαφέρουν λίγο μεταξύ τους αλλά όλες έχουν κάτι κοινό. Αυτό είναι ότι θα πρέπει να υπάρχει ένας κόμβος IPv6 που θα έχει την δυνατότητα να μεταδίδει πακέτα IPv4 και στις δυο άκρες του «τούνελ». Ουσιαστικά αυτό που γίνεται πραγματικά είναι ότι από τη μια άκρη του tunnel ο κόμβος παίρνει ένα πακέτο IPv6 και εργάζεται σαν να είναι κομμάτι από τα δεδομένα ενός πακέτου IPv4 το οποίο πρέπει να φτάσει στην άλλη άκρη του tunnel. Έτσι δημιουργείται μια σειρά από IPv4 πακέτα που περιέχουν IPv6.



Σχήμα 4- Μηχανισμοί Tunneling

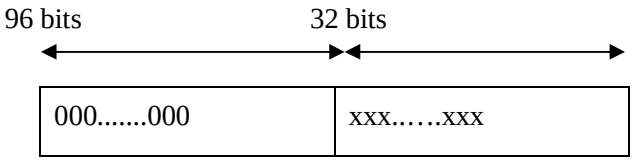
Στις κατηγορίες των διευθύνσεων IPv6 εντάσσεται και μία, στην οποία εμπεριέχονται και IPv4 διευθύνσεις. Αυτή η κατηγορία αποτελείται από δύο ειδών διευθύνσεις οι οποίες είναι γνωστές ως χαρτογραφημένες (mapped) και συμβατές (compatible) IPv4 διευθύνσεις.

- Οι IPv4-mappedIPv6 διευθύνσεις χρησιμοποιούνται από τους κόμβους που υποστηρίζουν μόνο IPv4 και όχι IPv6. Ένας IPv6 κόμβος χρησιμοποιεί μία τέτοια διεύθυνση για να επικοινωνήσει με έναν κόμβο που υποστηρίζει μόνο IPv4. Αυτές οι διευθύνσεις είναι τύπου unicast και αποτελούνται από 128 bits εκ των οποίων τα 80 πρώτα bits είναι ίσα με το 0, τα επόμενα 16 ίσα με 1 και τα τελευταία 32 bits περιέχουν την IPv4 διεύθυνση.



Σχήμα 5-Οι IPv4-mappedIPv6 διευθύνσεις

- Οι IPv4-compatibleIPv6 διευθύνσεις χρησιμοποιούνται από τους κόμβους διπλής στοίβας ώστε να πραγματοποιούν αυτόματη σηραγγοποίηση των πακέτων IPv6 σε δίκτυα του IPv4. Αυτού του τύπου unicast διευθύνσεις αποτελούνται από 128bits εκ των οποίων τα πρώτα 96bits αποτελούνται από 0 και τα υπόλοιπα 32bits είναι μια διεύθυνση IPv4.



Σχήμα 6-Οι IPv4- compatibleIPv6 διευθύνσεις

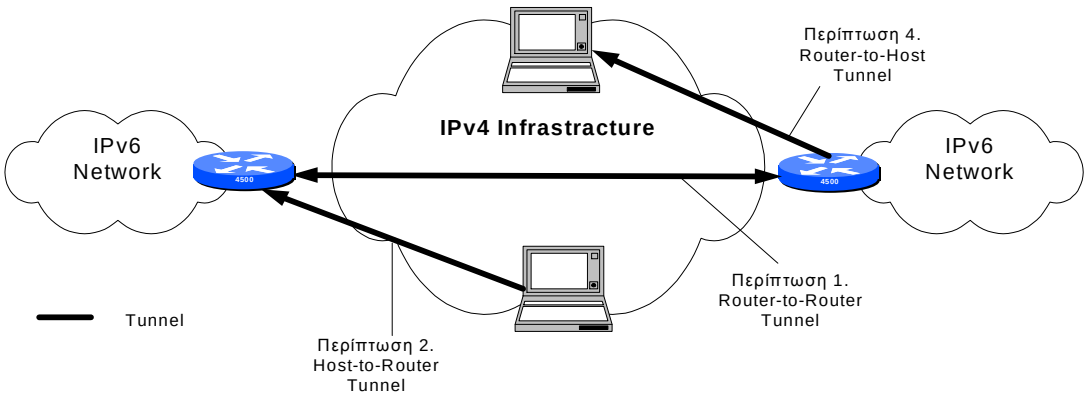
Οι μηχανισμοί tunneling χωρίζονται σε δυο κατηγορίες με βάση το μηχανισμό με τον οποίο ο κόμβος εισόδου, ο οποίος κάνει την ενθυλάκωση, καθορίζει την διεύθυνση του κόμβου εξόδου. Αυτές είναι το **configured tunneling** και το **automatic tunneling**. Η διαφορά αυτών των δύο κατηγοριών είναι ότι το automatic tunneling χρησιμοποιεί δρομολογητές διπλής στοίβας είτε με IPv4-compatible διευθύνσεις είτε με 6to4 είτε με κάποια άλλη διεύθυνση στην οποία η IPv4 εμπεριέχεται στην IPv6, στις άκρες του tunnel και έτσι δεν χρειάζεται παραμετροποίηση για να δουλέψουν οι IPv4 διευθύνσεις των δρομολογητών διπλής στοίβας.

Αντίθετα στο configured tunneling για να παρέχονται οι IPv4 διευθύνσεις των κόμβων της στοίβας θα πρέπει να υπάρχει κάποιου είδους μηχανισμός όπως είναι για παράδειγμα ο DHCP ή να καθορίζονται μέσω των διαχειριστών. Η ομοιότητα αυτών των δύο κατηγοριών tunnels είναι στη λειτουργία τους, καθώς και στους δύο, ο κόμβος εισόδου στον οποίο γίνεται η ενθυλάκωση δημιουργεί την IPv4 επικεφαλίδα με τιμή 41 στο πεδίο Protocol, έπειτα ενθυλακώνει το πακέτο IPv6 και το προωθεί κανονικά μέσω IPv4 δρομολόγησης έχοντας ως διεύθυνση προορισμού την IPv4 διεύθυνση του κόμβου εξόδου, όπου γίνεται η απενθυλάκωση. Όταν το ενθυλακωμένο πακέτο φτάσει στον κόμβο εξόδου επανασυναρμολογείται σε περίπτωση τεμαχισμού και αφού δει την τιμή 41 αφαιρεί την επικεφαλίδα IPv4. Στη συνέχεια εάν η διεύθυνση προορισμού του IPv6 πακέτου είναι διαφορετική από αυτή του κόμβου εξόδου όπου βρίσκεται, προωθεί το πακέτο στον προορισμό του με IPv6 δρομολόγηση. Κατά την απενθυλάκωση του πακέτου το μόνο που μεταβάλλεται στην επικεφαλίδα IPv6 είναι το hoplimit που μειώνεται κατά μια μονάδα σε περίπτωση επαναπροώθησης του πακέτου. Κάποια χαρακτηριστικά σχετικά με το MTU και HOPLIMIT αποθηκεύονται στο κόμβο εισόδου έτσι ώστε να είναι πιο εύκολη η IPv6 δρομολόγηση.

Είδη επικοινωνίας tunnels

- Router- to -Router και Host-to-Router: Συγκαταλέγονται στο configured tunneling, διότι τα πακέτα προωθούνται σε έναν ενδιάμεσο Router όπου και απενθυλακώνονται. Στην περίπτωση αυτή η διεύθυνση του άκρου του τούνελ είναι διαφορετική από τη διεύθυνση προορισμού του πακέτου άρα απαιτείται η χρήση αυτού του είδους tunneling, αφού η διεύθυνση του τελικού Router, δηλαδή του άκρου του τούνελ, δεν προκύπτει από την διεύθυνση προορισμού του πακέτου.

- Host-to-Host και Router-to-Host: εντάσσονται στο automatic tunneling καθώς το πακέτο μεταδίδεται μέσω του τούνελ στον τελικό προορισμό. Σε αυτή την περίπτωση η διεύθυνση προορισμού του IPv6 πακέτου περιέχει με κάποιο τρόπο τη IPv4 διεύθυνση προορισμού που θα χρησιμοποιηθεί στην εξωτερική IPv4 επικεφαλίδα. Έτσι δεν χρειάζεται να έχει καθοριστεί από την αρχή το άλλο άκρο του τούνελ.



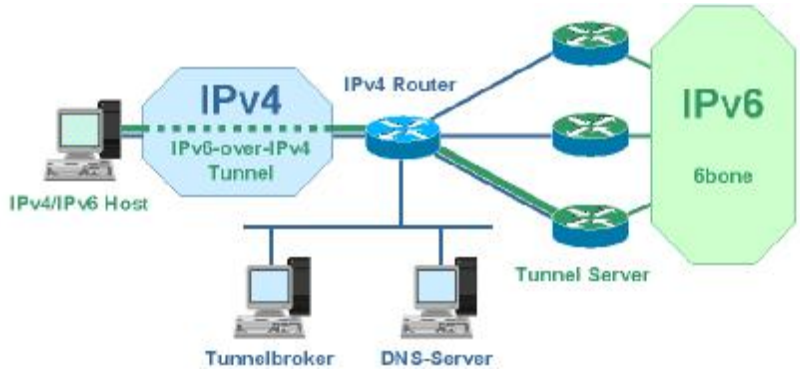
Σχήμα 7 – Περίπτωση Host to Host

2.6.2.1. Tunnel Broker Tunneling

Ο μηχανισμός Tunnel Broker επιτρέπει σε ένα dual stack host ενός IPv4 δικτύου να επικοινωνεί με IPv6 κόμβους σχετικά απλά. Η διαδικασία έχει ως εξής:

Αυτός που επιθυμεί IPv6 σύνδεση, συνδέεται σε ένα web server και αιτείται IPv6 σύνδεση. Στη συνέχεια ο web server του αναθέτει μια IPv6 διεύθυνση, κάνει αυτόματη ενημέρωση του DNS, ενημερώνει τον Tunnel Broker Tunnel server και τέλος στέλνει ένα script στο χρήστη. Όταν ο χρήστης το τρέξει γίνεται εγκατάσταση ενός IPv6 over IPv4 tunnel με τον broker server και μετά η επικοινωνία πραγματοποιείται μέσω αυτού.

Το πλεονέκτημα που έχει αυτός ο μηχανισμός είναι ότι μπορεί να εξυπηρετήσει μεγάλο αριθμό χρηστών. Όμως δεν μπορεί να υποστηρίξει χρήστες με ιδιωτικές διευθύνσεις ή διευθύνσεις στο NAT.



Σχήμα 8 – Tunnel Broker Tunneling

2.6.2.2. 6over4 Tunneling

Με τον μηχανισμό αυτό οι απομονωμένοι IPv6 hosts, που δεν είχαν σύνδεση σε κάποιο δρομολογητή IPv6, μπορούν να συνδεθούν μέσω ενός IPv4 multicast υποδικτύου και να λειτουργήσουν σαν ολοκληρωμένοι IPv6 hosts. Οι ίδιοι οι host ενθυλακώνουν τα πακέτα και επικοινωνούν μεταξύ τους μέσω tunnels μέσα στο IPv4 δίκτυο ή στέλνουν τα πακέτα σε κάποιο δρομολογητή με IPv6 σύνδεση που αναγνωρίζει το 6over4 για να μπορέσει να επικοινωνήσει με φυσικούς IPv6 κόμβους ή 6over4 άλλων δικτύων. Απαραίτητη προϋπόθεση για να λειτουργήσει αυτός ο μηχανισμός είναι το διαχειριστικό κομμάτι του IPv4 να υποστηρίζει multicast. Ο μηχανισμός 6over4 δεν απαιτεί κάποια παραμετροποίηση, παρα μόνο την ενεργοποίηση IPv4 multicasting και την υποστήριξη 6to4 από τους σταθμούς.

Ο συγκεκριμένος μηχανισμός λόγω της απαίτησης για IPv4multicast, κάτι που οι περισσότεροι πάροχοι ISP και διαχειριστές δεν παρέχουν, δεν χρησιμοποιήθηκε πολύ και περιορίστηκε μόνο στα πανεπιστημιακά δίκτυα.

2.6.2.3. ISATAP Tunneling

Το πρωτόκολλο ISATAP (Intrasite Automatic Tunnel addressing Protocol), που σημαίνει πρωτόκολλο διευθυνσιοδότησης αυτόματου τούνελ υποδικτύου, χρησιμοποιείται για να συνδέει τους απομονωμένους κόμβους διπλής στοίβας με το IPv6. Αποτελεί εναλλακτική του 6 over 4 καθώς και αυτός ο μηχανισμός κάνει χρήση της ipv4 υποδομής αλλά σε αυτόν δεν χρειάζεται η IPv4 Multicast. Ακόμα αυτό το πρωτόκολλο είναι συμβατό με το NAT. Μέσα σε ένα υποδίκτυο χρησιμοποιείται τις περισσότερες φορές ένας ISATAP δρομολογητής, ο οποίος λειτουργεί σαν server και παρέχει IPv6 σύνδεση σε όλους τους κόμβους που ανήκουν στο ISATAP υποδίκτυο. Πρόκειται για έναν αυτόματο μηχανισμό καθώς το μόνο που χρειάζεται είναι η διαμόρφωση των κόμβων όταν υπάρχει δρομολογητής.

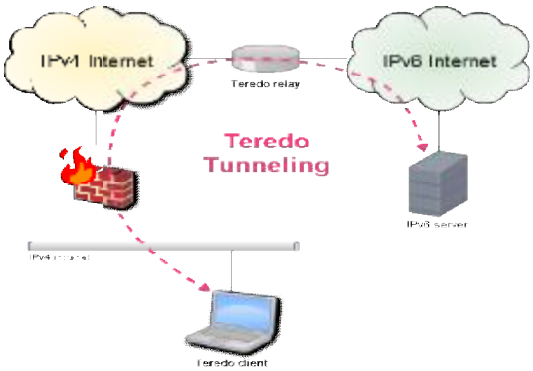
Η link local διεύθυνση για επικοινωνία με τον ISATAP Router σχηματίζεται από το link local πρόθεμα 64 και τον interface identifier. Όταν γίνει αρχικοποίηση του ISATAP κόμβου κάνει αναζήτηση μέσω DNS για το «ISATAP» και έτσι λαμβάνει τις διευθύνσεις από όλους τους ISATAP Routers και δημιουργείται η Potential Router list. Στη συνέχεια ο κόμβος στέλνει ένα μήνυμα στο Router για να λάβει το πρόθεμα έτσι ώστε να φτιάξει την global IPv6 ISATAP διεύθυνση του. Έτσι ο Router στέλνει ένα μήνυμα router advertisement στο κόμβο στο οποίο

περιλαμβάνεται και το πρόθεμα που χρειάζεται για να φτιάξει την δική του μοναδική παγκόσμια διεύθυνση. Όταν επιτυγχάνεται επικοινωνία εντός του site,τα πακέτα ενθυλακώνονται στον ISATAP κόμβο και ως διεύθυνση προορισμού τίθεται η IPv4 που προκύπτει από τον interface identifier, δηλαδή τα τελευταία 4 bytes της διεύθυνσης ενώ όταν γίνεται επικοινωνία με ISATAP κόμβους άλλων δικτύων τα πακέτα ενθυλακώνονται και στέλνονται στον ISATAP Routers.

2.6.2.4.TEREDO Tunneling

Αυτός ο μηχανισμός χρησιμοποιείται όταν δεν μπορεί να υπάρξει διασύνδεση με κάποιο άλλο τρόπο. Βασίζεται στην αυτόματη δημιουργία tunnels και στην αυτόματη απόδοση διευθύνσεων. Επιτρέπει σε host που βρίσκονται πίσω από NAT μηχανισμούς να επικοινωνούν με IPv6 κόμβους. Δημιουργεί tunnels μέσω των οποίων μεταφέρεται κίνηση IPv6 στις συσκευές του υποδικτύου . Ο μηχανισμός αυτός ενθυλακώνει IPv6 πακέτα ως UDP IPv4 μηνύματα με UDP και IPv4 επικεφαλίδες έτσι ώστε να μπορούν να περνάνε σε όλα τα NAT, καθώς τα ενθυλακωμένα πακέτα IPv6 σε IPv4 με πρωτόκολλο 41 δεν υποστηρίζονται από το NAT.

Tunnel Broker Tunneling



Σχήμα 9 – Teredo Tunneling

2.6.2.5. 6to4 Tunneling

Ο μηχανισμός 6to4 επιτρέπει σε απομονωμένες περιοχές IPv6 να συνδέονται μέσω ενός δικτύου IPv4 σε IPv6 απομακρυσμένα δίκτυα. Μοιάζει αρκετά με τον μηχανισμό 6in4 αλλά διαφέρει στο πρόθεμα καθώς επίσης και στο ότι είναι αυτόματος μηχανισμός και δεν χρειάζεται ρύθμιση για κάθε τούνελ για να φτάσει το πακέτο στον προορισμό του καθώς μπορεί να λάβει και να στείλει πακέτα σε πολλούς προορισμούς άλλων τούνελ.

Για να επιτευχθεί αυτή η επικοινωνία χρειάζεται ένας 6to4 Router. Το πρόθεμα του δικτύου στον μηχανισμό αυτό δημιουργείται συνδυάζοντας το 6to4 2002::/16 πρόθεμα που έχει οριστεί από τον οργανισμό IANA για το συγκεκριμένο μηχανισμό και την IPv4 διεύθυνση που έχουμε κάθε φορά. Έτσι το πρόθεμα αποτελείται από 48 bits εκ των οποίων τα 16 bits είναι προκαθορισμένα για τον μηχανισμό και τα 32 bits είναι της IPv4 διεύθυνσης. Στην ουσία αυτό που γίνεται είναι ο ορισμός της IPv4 διεύθυνσης ως ένα unicast σημείο προς σημείο επίπεδο διασύνδεσης και με τη χρήση διάφορων τεχνικών ενθυλάκωσης υλοποιείται το IPv6 δίκτυο.

Δεν χρειάζεται καθορισμός της IPv4 διεύθυνσης προορισμού καθώς εμπεριέχεται μέσα στην IPv6. Ακόμα μια συσκευή που παίζει σημαντικό ρόλο σε αυτή την επικοινωνία είναι η 6to4 relay, η οποία είναι στην ουσία ένας δρομολογητής ο οποίος μεταδίδει κίνηση 6to4 σε άλλους δρομολογητές και κόμβους του IPv4 δικτύου. Αυτός ο relay Royter συνδέεται πάντα με ένα IPv4 δίκτυο, με τουλάχιστον ένα IPv6 interface καθώς και ένα pseudo-interface το οποίο είναι προκαθορισμένο σε αυτή τη συσκευή.

2.6.3. Μηχανισμοί Translation (Μετάφρασης)

Όταν θέλουν να επικοινωνήσουν δύο σταθμοί, οι οποίοι υποστηρίζουν διαφορετικό πρωτόκολλο, τότε η λύση που εφαρμόζεται είναι οι τεχνικές μετάφρασης διευθύνσεων. Η ιδέα αυτής της τεχνικής δεν είναι κάτι νέο, καθώς αποτελεί μια από τις πιο σημαντικές τεχνικές για την εξοικονόμηση διευθύνσεων στο IPv4 πρωτόκολλο. Μία από τις πιο γνωστές τεχνικές αυτού του είδους είναι αυτή που πραγματοποιείται μέσω του μηχανισμού NAT-PT (Network Address Translation-Protocol Translation), ο οποίος είναι ένας μηχανισμός μετάφρασης IPv6-to-IPv4 και επιτρέπει στις IPv6 μόνο συσκευές να επικοινωνούν με τις IPv4 μόνο συσκευές αλλά και το

αντίστροφο. Κάθε NAT-PT μηχανισμός έχει στη κατοχή του ένα σύνολο από παγκόσμιες IPv4 δρομολογήσιμες διευθύνσεις, οι οποίες εκχωρούνται δυναμικά στους IPv6 κόμβους.

Οι μηχανισμοί αυτοί εμπεριέχουν Application Level Gateways(ALG), τα οποία είναι ενημερωμένα πρωτόκολλα που αποτελούνται από πρωτόκολλα όπως το DNS που είναι αρμόδια για την επανεγγραφή IPv6 διευθύνσεων χρησιμοποιώντας τις IPv4 διευθύνσεις που είναι ορισμένες για το NAT-PT.

Η διαδικασία έχει ως εξής: ο IPv4 κόμβος κάνει ένα DNS ερώτημα για μια IPv4 διεύθυνση και ο NAT-PT μεταφράζει αυτό το ερώτημα και το γενικεύει για κάθε τύπο διευθύνσεων της ζητούμενης διεύθυνσης. Όταν ο DNS λάβει απάντηση από κάποια IPv6 διεύθυνση, τότε το ερώτημα υποκλέπτεται από το μηχανισμό. Έπειτα γίνεται δυναμική χαρτογράφιση μεταξύ της IPv6 διεύθυνσης, της ζητούμενης IPv4 και της IPv4 διεύθυνσης της NAT-PT.

ΚΕΦΑΛΑΙΟ 3

3.Στοιχεία χρήσης και δρομολόγησης του IPv6

3.1. Τι είναι το Autonomous System

Ένα αυτόνομο σύστημα (AS) είναι ένα δίκτυο ή μια συλλογή δικτύων τα οποία βρίσκονται όλα υπό τη διαχείριση και την εποπτεία ενός μόνο φορέα ή οργανισμού. Κάθε αυτόνομο σύστημα έχει πολλά διαφορετικά υποδίκτυα και σε κάθε ένα από αυτά, έχει εκχωρηθεί ένα παγκοσμίως μοναδικό δεκαεξαδικό νούμερο γνωστό ως Autonomous System Number από την αρχή Internet Assigned Numbers (IANA).

Τα αυτόνομα συστήματα εισήχθησαν με σκοπό την καλύτερη ρύθμιση των οργανισμών, όπως οι πάροχοι υπηρεσιών διαδικτύου (ISP), τα εκπαιδευτικά ιδρύματα και οι κρατικοί φορείς. Τα συστήματα αυτά αποτελούνται από πολλά διαφορετικά δίκτυα, αλλά λειτουργούν κάτω από την ομπρέλα ενός ενιαίου φορέα για εύκολη διαχείριση. Η σύνδεση μεταξύ των διαφορετικών αυτόνομων συστημάτων επιτυγχάνεται με ένα πρωτόκολλο, γνωστό ως Border Gateway Protocol (BGP). Το πρωτόκολλο αυτό είναι ένα τυποποιημένο πρωτόκολλο εξωτερικής δρομολόγησης που επιτρέπει την δρομολόγηση πακέτων και την ανταλλαγή πληροφοριών προσβασημότητας μεταξύ των αυτόνομων συστημάτων στο διαδίκτυο.

Το BGP ανήκει στην κατηγορία των πρωτοκόλλων διανύσματος (path vector) και οι αποφάσεις δρομολόγησης βασίζονται στα διαθέσιμα μονοπάτια δρομολόγησης, στις πολιτικές που ακολουθούνται από κάθε αυτόνομο σύστημα καθώς και τους κανόνες που εφαρμόζονται τοπικά από τους διαχειριστές κάθε αυτόνομου συστήματος για την διαχείριση της εισερχόμενης και εξερχόμενης ροής δικτύου. Ακόμα το πρωτόκολλο αυτό τρέχει πάνω από το TCP επομένως κατατάσσεται στα πρωτόκολλα επιπέδου εφαρμογής . Αυτό σημαίνει πως το λογισμικό που υλοποιεί το BGP δε λαμβάνει αποφάσεις δρομολόγησης στο επίπεδο δικτύου αλλά χρησιμοποιείται για τη κατασκευή των πινάκων δρομολόγησης που στη συνέχεια θα χρησιμοποιήσουν οι δρομολογητές για τη δρομολόγηση του δικτυακού φορτίου.

Υπάρχουν τρεις τύποι Autonomous Systems:

a) Multi-homed

b) Stub

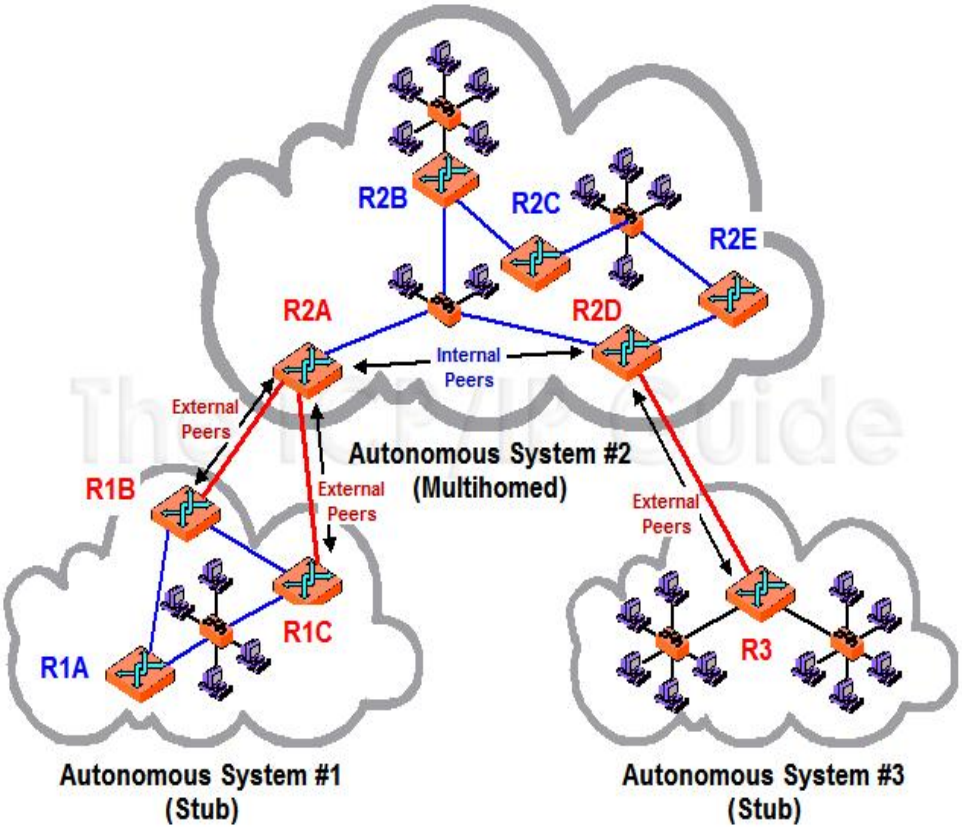
c) Transit

Ένα αυτόνομο σύστημα τύπου multi-homed είναι συνδεδεμένο με δύο ή περισσότερα αυτόνομα δίκτυα. Αυτό επιτρέπει την διατήρηση της σύνδεσης στο διαδίκτυο όταν κάποιο αυτόνομο σύστημα χάσει την σύνδεση του.

Ένα αυτόνομο σύστημα τύπου stub είναι συνδεδεμένο μόνο με ένα αυτόνομο σύστημα. Βέβαια σε αυτού του τύπου τα συστήματα επιτρέπεται να έχουν και άλλες ιδιωτικές συνδέσεις, αλλά δημοσίως στο διαδίκτυο φαίνεται να έχουν μόνο μια σύνδεση.

Τέλος τα αυτόνομα συστήματα τύπου transit συνδέει ένα αυτόνομο σύστημα με ένα άλλο, επιτρέποντας την επικοινωνία στο πέρασμα του. Οι πάροχοι δικτύου για παράδειγμα, οι οποίοι προσφέρουν στους πελάτες τους και στην πρόσβαση των δικτύων τους από άλλα δίκτυα στο διαδίκτυο μέσω του αυτόνομου συστήματος transit.

Το παρακάτω σχήμα δείχνει τους διαφορετικούς τρόπους σύνδεσης δρομολογητών και αυτόνομων συστημάτων. Οι εσωτερικοί δρομολογητές αναπαριστούνται με μπλε χρώμα ενώ τα όρια των δρομολογητών με κόκκινο. Οι BGP ομιλητές οι οποίοι επικοινωνούν μέσω των αυτόνομων συστημάτων είναι οι εσωτερικοί χρήστες ενώ αυτοί που επικοινωνούν μεταξύ των αυτόνομων συστημάτων είναι οι εξωτερικοί χρήστες



Σχήμα 10 - Παράδειγμα τοπολογίας αυτόνομων συστημάτων

3.2. **Πρωτόκολλα Δρομολόγησης στο** IPv6

Με την υιοθέτηση του IPv6 εκτός των νέων μηχανισμών μετάβασης που αναφέρθηκαν στο προηγούμενο κεφάλαιο, χρειάστηκαν να γίνουν και σημαντικές αλλαγές στα πρωτόκολλα δρομολόγησης. Τα πρωτόκολλα δρομολόγησης του IPv6 χωρίζονται σε 2 κατηγορίες :

- **Interior Gateway Protocols (IGPs)**. Είναι υπεύθυνα για την τη δρομολόγηση σε εσωτερικό επίπεδο, δηλαδή μέσα στα Α**υτόνομα Συστήματα (AS-Autonomous Systems)**
- **Exterior Gateway Protocols (EGPs).** Είναι υπεύθυνα για την δρομολόγηση μεταξύ των αυτόνομων συστημάτων.

Τα σημαντικότερα πρωτόκολλα δρομολόγησης είναι τα RIP και OSPF (IGPs) και το BGP (EGP). Όλα τα παραπάνω πρωτόκολλα επεκτάθηκαν με σκοπό την υποστήριξη του IPv6.

3.2.1. Πρωτόκολλο RIPng

Το πρωτόκολλο δρομολόγησης RIP χρησιμοποιείται σε μεγάλη κλίμακα από τα ευρέως γνωστά IGPs.

Για να βρεθεί το καλύτερο μονοπάτι χρησιμοποιείται ο αλγόριθμος Bellman-Ford. Το συγκεκριμένο πρωτόκολλο είναι κατασκευασμένο με τέτοιο τρόπο ώστε να εκτελείται σε δρομολογητές στους οποίους υπάρχουν Interfaces συνδεδεμένα με κάποια άλλα δίκτυα.

Ωστόσο στο πρωτόκολλο RIP υπάρχει ένας αριθμός περιορισμών οι οποίοι αναφέρονται παρακάτω:

Α) Η χρήση του γίνεται σε δίκτυα με μέγιστη διάμετρο. Χρήση σε δίκτυα με διάμετρο 15 hops.

Β) Υπάρχει μία παράμετρος η λεγόμενη “count to infinity” που είναι πολύ πιθανόν να προκαλέσει καθυστερήσεις και εξάντληση του εύρους ζώνης.

Γ) Ο υπολογισμός του καλύτερου μονοπατιού γίνεται με βάσει προκαθορισμένες σταθερές και αυτό το γεγονός προκαλεί τη μη προσαρμογή άλλων παραμέτρων όπως αυτή της καθυστέρησης ή της ποιότητας της σύνδεσης.

Ένας πίνακας δρομολογητής είναι απαραίτητος να χρησιμοποιηθεί από κάθε δρομολογητή ώστε να υλοποιήσει το πρωτόκολλο RIPng. Ο πίνακας περιέχει τις ακόλουθες απαραίτητες εγγραφές.

· Το IPv6 πρόθεμα του προορισμού.

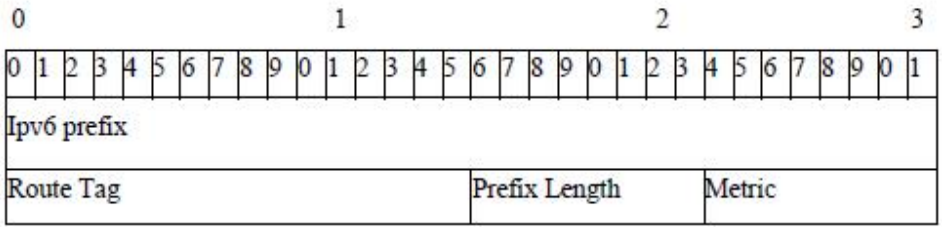
· Μία μετρική η οποία υπολογίζει το συνολικό κόστος του της διαδρομής του πακέτου από τον δρομολογητή έως τον προορισμό. Το συνολικό κόστος υπολογίζεται από το άθροισμα όλων αυτών.

· Την IPv6 διεύθυνση του επόμενου δρομολογητή της διαδρομής του πακέτου.

· Μία σημαία (flag) , η οποία αντιπροσωπεύει αν άλλαξε κάποιο δεδομένο στον δρομολογητή.

· Διάφορες άλλες μετρητές οι οποίες έχουν σχέση με την διαδρομή του πακέτου.

Το πρωτόκολλο RIPng στηρίζεται στο πρωτόκολλο UDP και κάνει χρήση της θύρας 521. Στον παρακάτω πίνακα παρουσιάζεται η μορφή ενός πακέτου που δρομολογείται με το πρωτόκολλο RIP:



Πίνακας 11 – μορφή toy πίνακα **Route Table Entry**

Το πεδίο command ορίζει τον τύπο του μηνύματος.

Υπάρχουν 2 είδη μηνυμάτων:

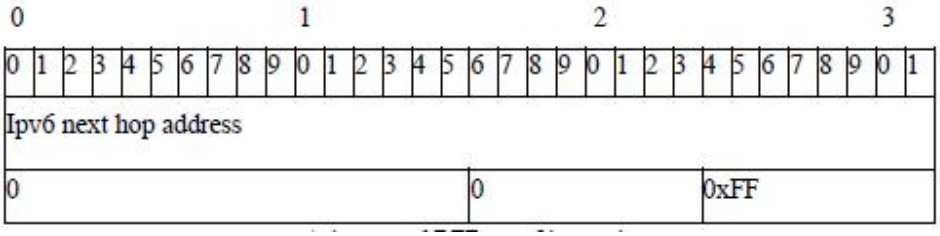
Request μήνυμα: Ζητά από τον παραλήπτη του μηνύματος να αποστείλει τον πίνακα δρομολόγησης του.

Response μήνυμα: Μεταδίδει κάποιο μέρος του πίνακα ή ολόκληρο τον πίνακα δρομολόγησης του αποστολέα ως απάντηση στο μήνυμα request.

Η διεύθυνση του προορισμού έχει μέγεθος 128bit καθώς αυτό ορίζει η έκδοση IPv6, και είναι χωρισμένη σε 16 οκτάδες. Το πεδίο route tag είναι αυτό το οποίο χρησιμοποιεί μία μέθοδο διαχωρισμού μονοπατιών εσωτερικών στο domain που διαχειρίζεται το RIPng και "εξωτερικών" , εισαγμένων από άλλο IGP ή από BGP. Το πεδίο prefix length περιέχει το μήκος σε bits (0-128) του σημαντικού μέρους του προθέματος αρχίζοντας από αριστερά.

Στο πεδίο metric υπάρχει αποθηκευμένο το υπολογισμένο κόστος για την διαδρομή του πακέτου μέχρι αυτό να φτάσει στον τελικό προορισμό του.

Στο πρωτόκολλο RIPng μπορεί να οριστεί η IPv6 διεύθυνση του επόμενου κόμβου στην διαδρομή μονοπάτι με την χρήση ενός ειδικού RTE, του **Next Hop Route Table Entry**. Αυτός ο πίνακας έχει την εξής μορφή:



Πίνακας 12 – Next Hop Route Table

Το πεδίο prefix είναι αυτό που περιέχει τις πληροφορίες του επόμενου κόμβου που το πακέτο θα ακολουθήσει. Το πεδίο route tag και το πεδίο prefix length λαμβάνουν την τιμή μηδέν όταν γίνει η αποστολή του πακέτου. Η τιμή 0:0:0:0:0:0:0:0 στο πεδίο prefix length σημαίνει ότι η διεύθυνση του επόμενου κόμβου αποτελεί και τον αποστολέα του μηνύματος.

3.2.2. Το πρωτόκολλο OSPF

Το OSPF έχει αλλαχτεί και αυτό ώστε να μπορεί να υποστηρίξει το IPv6. Ο γνωστός αλγόριθμος **Dijkstra** έχει αρκετά πλεονεκτήματα σε σύγκριση με τον αλγόριθμο Bellman-Ford του RIP . Τα πλεονεκτήματα αυτά είναι τα εξής :

- Δυνατότητα για ρύθμιση των επιπέδων διευθύνσεων.
- Χρήση σε δίκτυα, μεγάλα σε μέγεθος.
- Υπολογισμός πολλών βέλτιστων μονοπατιών ώστε να ομαλοποιηθεί η κίνηση.
- Δυνατότητα χρήσης subnet masks μεταβλητού μήκος.

Στην συνέχεια θα παρουσιαστούν οι πιο σημαντικές αλλαγές που πραγματοποιήθηκαν στο πρωτόκολλο OSPF ώστε να υποστηρίζει το IPv6. Αν και γενικά οι μηχανισμοί του πρωτοκόλλου αυτού παραμένουν ίδιοι, ωστόσο έχουν γίνει τροποποιήσεις σε αρκετά σημεία. Οι διαφορές αυτής της έκδοσης του OSPF είναι οι εξής:

- Μία πολύ σημαντική αλλαγή είναι το γεγονός ότι το πρωτόκολλο τρέχει τώρα πάνω στη λογική των συνδέσεων και όχι των υποδικτύων (subnets). Μία σύνδεση μπορεί να περιλαμβάνει περισσότερα του ενός υποδικτύων και δύο κόμβοι μπορούν να επικοινωνούν απευθείας αν βρίσκονται στην ίδια σύνδεση, ακόμα και αν ανήκουν σε διαφορετικά υποδίκτυα.
- Επίσης, ο πυρήνας του OSPF είναι πλέον ανεξάρτητος από το επίπεδο δικτύου, και αυτό διότι τα πακέτα του δεν περιέχουν τις IPv6 διευθύνσεις.
- Η εμβέλεια στην οποία ο αλγόριθμος “πλημμυρίζει” την πληροφορία κωδικοποιείται στο πεδίο LS type του LSA. Τρείς είναι οι κατηγορίες του flooding scope:
  - **ü** Link-local
  - **ü** Area scope
  - **ü** AS scope

Υπάρχει η ευελιξία να εκτελούνται ταυτόχρονα πολλές διεργασίες (instances) κατά τη διάρκεια μιας σύνδεσης. Χρησιμοποιούνται οι link-local διευθύνσεων του IPv6 για να πραγματοποιηθεί autoconfiguration σε μια σύνδεση.

Δεν είναι αναγκαίο και δεν πραγματοποιείται ταυτοποίηση (authentication) διότι το IPv6 διαθέτει από μόνο του τους κατάλληλους μηχανισμούς. Επίσης, το πρωτόκολλο OSPF χρησιμοποιεί το πεδίο IP Authentication Header και το πεδίο IP Encapsulating Security Payload ώστε να προστατευτεί η αλλοίωση των δεδομένων και η διαρροή ιδιωτικών πληροφοριών. Επίσης για να αποφευχθεί η τροποποίηση των πληροφοριών λόγων λαθών γίνεται χρήση του 16-bit checksum του IPv6.

Η κεφαλίδα ενός πακέτου PSPF εμπεριέχει πλέον το πεδίο «Instance ID» το οποίο όπως αναφέρθηκε παραπάνω δίνει την ευελιξία να εκτελούνται ταυτόχρονα πολλές διεργασίες (instances) κατά τη διάρκεια μιας σύνδεσης.

Η κεφαλίδα του LSA (Link State Algorithm) δεν περιέχει σημειολογία διευθύνσεων, και αυτό την καθιστά ανεξάρτητη από πρωτοκόλλο δικτύου. Επίσης, έχουν δημιουργηθεί νέοι LSA ώστε να διανείμουν την πληροφορία για τις IPv6 διευθύνσεις, και τα δεδομένα για τον προσδιορισμό του επόμενου hop, όπως αυτό του Link-LSA, το οποίο χρησιμοποιείται ώστε να :

- Δίνει την link-local διεύθυνση του δρομολογητή στους άλλους δρομολογητές στην ίδια σύνδεση.
- Ενημερώνει τους άλλους δρομολογητές της σύνδεσης για τη λίστα των IPv6 προθεμάτων που πρέπει να σχετίζουν με τη σύνδεση.

Τέλος στην έκδοση του OSPF έχει αλλάξει ο τρόπος διαχείρισης άγνωστων τύπων του LSA.

3.2.3 Το πρωτόκολλο BGP

Το πιο ευρέως χρησιμοποιούμενο EGP είναι το πρωτόκολλο BGP. Το πρωτόκολλο αυτό είναι υπεύθυνο για την ανταλλαγή πληροφοριών ανάμεσα στα αυτόνομα συστήματα . Καθορίζει κάθε δίκτυο αν μπορεί να έχει πρόσβαση σε κάποιο άλλο δίκτυο και δημιουργεί ένα αντίστοιχο γράφημα με τα δυνατές διαδρομές.

Η πιο πρόσφατη έκδοση του BGP είναι η έκδοση 4. Το header του πρωτοκόλλου BGP μπορεί να περιέχει τους εξής τέσσερις δυνατούς τύπους μηνυμάτων :

1. **OPEN** : Εκκίνηση της επικοινωνίας.
2. **UPDATE** : Μεταδίδει πληροφορίες σχετικά με την τη δρομολόγηση.
3. **KEEPALIVE** : Αυτό το μήνυμα στέλνεται συχνά ώστε να διαπιστωθεί αν είναι εφικτή η επικοινωνία.
4. **NOTIFICATION** : Αποστέλλεται σε περίπτωση κάποιου προβλήματος και διακόπτει την σύνδεση BGP.

Επειδή το πρωτόκολλο BGP-4 είναι ανεξάρτητο από το πρωτοκόλλου δικτύου, είναι και κατάλληλο για το IPv6 με μικρές τροποποιήσεις. Υπάρχει βέβαια μια διαφορά η οποία έχει να κάνει με την εμβέλεια των unicast διευθύνσεων και το πότε πρέπει να χρησιμοποιείται (link-local, site-local, global – οικουμενική).

3.3 Τι είναι οι πάροχοι υπηρεσιών Διαδικτύου (ISP)

Ένας πάροχος υπηρεσιων Internet (ISP) είναι μια εταιρεία η οποία με το ανάλογο αντίτιμο, σε μερικές περιπτώσεις είναι δωρεάν, παρέχει πρόσβαση στο Internet.

Ο πιο συνηθισμένος τρόπος σύνδεσης σε μια υπηρεσία παροχής Internet (ISP) είναι μέσω μιας τηλεφωνικής γραμμής (σύνδεση μέσω τηλεφώνου) ή μέσω σύνδεσης ευρείας ζώνης (καλωδιακή ή DSL). Βέβαια δεν αποτελεί το μοναδικό τρόπος παροχής internet, μετά τις εξελίξεις της τεχνολογίας και της εισαγωγής των smartpones και των νέων δορυφορικών συνδέσεων. Πολλές υπηρεσίες παροχής Internet προσφέρουν πρόσθετες υπηρεσίες, όπως λογαριασμούς ηλεκτρονικού ταχυδρομείου, προγράμματα περιήγησης Web και χώρο για τη δημιουργία μιας ιστοσελίδας

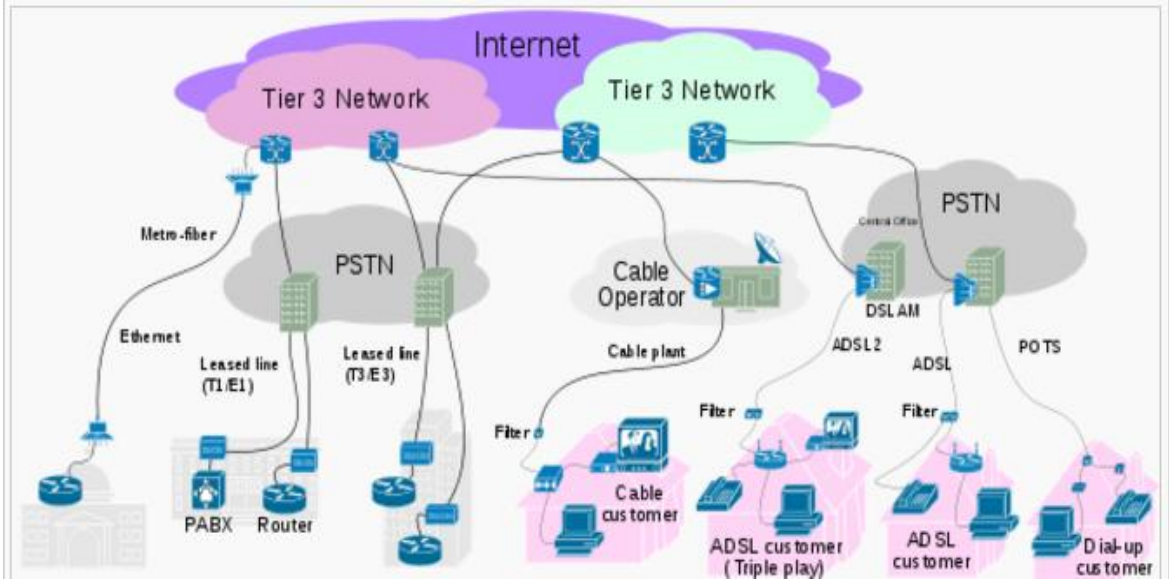
Όταν κάποια συσκευή συνδέεται στο διαδίκτυο μέσω ενός παρόχου ISP, εγκαθιδρύεται η επικοινωνία μεταξύ του ISP χρησιμοποιώντας ένα απλό πρωτόκολλο: PPP (Point to Point Protocol), ώστε να γίνεται δυνατή η σύνδεση απομακρυσμένων υπολογιστών χωρίς να έχουν λάβει IP διεύθυνση. Στην πραγματικότητα, ένα υπολογιστής δεν έχει διεύθυνση IP. Παρ' όλα αυτά, η διεύθυνση IP είναι αναγκαία αν θέλει κάποιος να συνδεθεί στο Internet διότι το γνωστό πρωτόκολλο TCP/IP θέλει κάθε υπολογιστής να έχει μια μοναδική διεύθυνση στο διαδίκτυο, διαφορετικά θα ήταν αδύνατη η επικοινωνία μεταξύ τους.

Η τελική επιλογή ενός χρήστη για τον πάροχο που θα του προσφέρει σύνδεση στο Internet και διάφορες άλλες υπηρεσίες εξαρτάται από τα παρακάτω κριτήρια:

- **Κάλυψη:** Μερικοί πάροχοι (ISPs) μπορούν να καλύψουν μικρές πόλεις, άλλοι μπορούν να καλύψουν ολόκληρη χώρα, ή και περισσότερες χώρες μαζί.
- **Εύρος Ζώνης:** Συνιστά την συνολική ταχύτητα μετάδοσης των δεδομένων. Το εύρος ζώνης μοιράζεται ανάμεσα στους συνδρομητές (πελάτες) των παρόχων, οπότε όσους περισσότερους πελάτες έχει ένας πάροχος τόσο ελαττώνεται η ταχύτητα που θα μοιραστεί ένας συνδρομητής.
- **Τιμή:** Εξαρτάται από την ταχύτητα και τις υπηρεσίες που παρέχει ο κάθε πάροχος.
- **Πρόσβαση:** Κάποιοι πάροχοι επιτρέπουν πρόσβαση στο διαδίκτυο με χρέωση ανά ώρα και κάποιοι άλλοι παρέχουν πρόσβαση απεριόριστη.

· **Τεχνική υποστήριξη:** Μια ομάδα υπαλλήλων της εταιρίας του παρόχου είναι διαθέσιμη για την εξυπηρέτηση των πελατών σε περίπτωση τεχνικών προβλημάτων. Η τηλεφωνική εξυπηρέτηση σε μερικούς παρόχους είναι δωρεάν και σε άλλους με χρέωση που κυμαίνεται από 0.35 € το λεπτό, ή κάποιο πάγιο κόστος ανά κλήση.

Στο παρακάτω σχήμα παρουσιάζονται τα διάφορα είδη συνδέσεων διαδικτύου για πελάτες και εταιρίες:



Σχήμα 13 - διάφορα είδη συνδέσεων διαδικτύου για πελάτες και εταιρίες

Στην Ελλάδα υπάρχουν οι ακόλουθοι πάροχοι υπηρεσιών Internet:

1) **Cosmote**
2) **Cyta**
3) **Otenet**
4) **Wid Hellas**

3.4 **Η επίδραση του** IPv6 **στις** end user **εφαρμογές**

Στην ανάπτυξη ενός προϊόντος λογισμικού, ένας end user είναι το άτομο εκείνο το οποίο βοηθάει στο να ολοκληρωθεί το τελικό προϊόν. Το άτομο αυτό διαχωρίζεται από τους χρήστες ή υπάλληλους της εταιρίας που κατασκευάζει το προϊόν, δηλαδή τους διαχειριστές, διαχειριστές της βάσης δεδομένων ή τους τεχνικούς. Οι χρήστες End users μπορεί να μην διαθέτουν τις απαραίτητες τεχνικές γνώσεις ή δεξιότητες όπως αυτές κατέχονται από τους σχεδιαστές του προϊόντος.

Μία εφαρμογή end-user συχνά μεταδίδει ή λαμβάνει δεδομένα από μία βάση δεδομένων μιας εταιρίας. Το αποτέλεσμα των υπολογισμών end-user μπορεί να είναι η δημιουργία spreadsheets, βάσεων δεδομένων, εξαγωγή ερωτημάτων, data, εξειδεικευμένες αναφορές και διάφορες ιστοσελίδες. Ειδικότερα, τα spreadsheets είναι απαραίτητα για τις διαδικασίες των επιχειρήσεων. Πρόσφατη έρευνα έδειξε ότι το 70% των εταιριών βασίζονται στα spreadsheets για την ολοκλήρωση των οικονομικών αναφορών τους.

Ανάμεσα στους πόρους που χρειάζονται οι end users , οι εφαρμογές λογισμικού είναι αυτές που επηρεάζουν σημαντικά την παραγωγή. Εργασίες που απαιτούν μεγάλη προσπάθεια, όπως η ετοιμασία αναφοράς προϋπολογισμού ή διαχείριση της λίστας ταχυδρομείου, μπορούν να πραγματοποιηθούν πιο γρήγορα και με μεγαλύτερη ακρίβεια με την καλή και προσεγμένη σχεδίαση ενός προγράμματος-εφαρμογής. Οι end users εκτελούν μία σειρά εφαρμογών λογισμικού οι οποίες χωρίζονται στις εξής δέκα κατηγορίες:

1. Ηλεκτρονικό ταχυδρομείο (Electronic mail and instant messaging)
2. Φυλλομετρητής (Web browser)
3. Επεξεργασία λέξεων (word processing)
4. Spreadsheets
5. Διαχείριση Βάσης δεδομένων (database management)
6. Γραφικά (graphics)
7. Σχεδιασμός κ προγραμματισμός (planning and scheduling)
8. Desktop Publishing
9. Ανάπτυξη ιστοσελίδας (web site development)
10. Educational and Entertainment Software

Γενικά υπήρξε και συνεχίζει να υπάρχει μια περίοδος προσαρμογής των End user εφαρμογών όσο θα υπάρχει η διαδικασία μετάβασης στο IPv6. Η απόδοση των εφαρμογων επηρεάζεται από τους μηχανισμούς IPv6. Σύμφωνα με μία έρευνα του akamai, η αδράνεια (latency) στο IPv6 ήταν μεγαλύτερη από αυτή του IPv4. Ειδικότερα, στην βόρεια Αμερική τα latencies πλησίαζαν το 80%. Υπάρχουν αρκετές αιτίες οι οποίες δημιουργούν προβλήματα στην απόδοση των end user εφαρμογών.

Από την στιγμή που δεν υπάρχει συμβατότητα μεταξύ του IPv6 και του IPv4, τα δυο δίκτυα αναγκαστικά θα συνυπάρχουν σε dual stack περιβάλλοντα κατά την διάρκεια της μεταβατικής περιόδου. Παρ' όλα αυτά, πολύ λίγα δίκτυα είναι πλήρως εξοπλισμένα για την υποστήριξη του IPv6 και οι περισσότεροι πάροχοι δεν μπορούν να παρέχουν ακόμη συνδεσιμότητα end-to-end IPv6. Αυτό σημαίνει ότι μερική ροή του IPv6 traffic θα πρέπει να οδηγηθεί μέσω του IPv4, και οι δρομολογητές θα πρέπει με την σειρά τους να ενθυλακώνουν την ροή και στη συνέχεια οι επόμενοι δρομολογητές να εξάγουν την ενθυλακωμένη ροή με αποτέλεσμα την μείωση της απόδοσης του δικτύου και την δημιουργία προβλημάτων διαθεσιμότητας.

Επίσης, μέχρι να αυξηθεί η ζήτηση του IPv6, τα CDNs (Content Delivery Networks) δεν έχουν το ίδιο επίπεδο διαθεσιμότητας για το IPv6 όπως έχουν για το IPv4. Οπότε το περιεχόμενο θα στέλνεται από μεγαλύτερη απόσταση οδηγώντας σε μεγαλύτερους χρόνους ανταπόκρισης από την μεριά του χρήστη.

Κεφάλαιο 4

4. Τρέχουσα κατάσταση IPv6 και IPv4

4.1 Χρησιμότητα ipv6 σήμερα

Όπως αναφέρθηκε και σε προηγούμενη ενότητα, είναι μεγάλη η χρησιμότητα και πολλά τα οφέλη από την εφαρμογή της τεχνολογίας IPv6. Πρώτα απ' όλα, είναι η σημαντική αύξηση των διαθέσιμων διευθύνσεων IP για τη σύνδεση δικτυακών συσκευών στο Διαδίκτυο.

Τα τελευταία χρόνια, το πρωτόκολλο Network Address Translation – NAT και η τεχνική του τεμαχισμού των διευθύνσεων IP σε κάθε δίκτυο Classless Inter-Domain Routing - CIDR ήταν απλά κάποιες λύσεις όχι μόνιμες, αλλά προσωρινές ώστε να μπορεί να χρησιμοποιηθεί το πρωτόκολλο IPv4, ενώ παράλληλα θα γίνεται η μετάβαση το πρωτόκολλο IPv6. Με την εμφάνιση όμως του πρωτόκολλου IPv6, πολλά πράγματα έχουν αλλάξει και έχει επιφέρει σημαντικότατες βελτιώσεις στο τρόπο με τον οποίο λειτουργεί το Διαδίκτυο.

4.1.1. Απεριόριστος αριθμός διευθύνσεων

Η πιο Σημαντική χρησιμότητα του πρωτοκόλλου IPv6 είναι ότι υποστηρίζει 2128 (ή ισοδύναμα, 3,4 * 1038) ξεχωριστές διευθύνσεις. Είναι πραγματικά απεριόριστη η χρήση διευθύνσεων αφού με πλέον κάθε άνθρωπος μπορεί να χρησιμοποιήσει 50 τρισεκατομμύρια τρισεκατομμυρίων διευθύνσεις . Άρα στο πρωτόκολλο αυτό δεν πρόκειται ποτέ να εξαντληθούν οι διαθέσιμες διευθύνσεις IP.

Συμφωνα με το πρωτόκολλο IPv4 , για να μπορεί να συνδεθεί μια συσκευή σε κάποιο δίκτυο χρειάζονται αρκετές ρυθμίσεις. Τέτοιες ρυθμίσεις έχουν να κάνουν με την ονοματολογία του, τη διεύθυνση IP, τη μάσκα του δικτύου, τη διεύθυνση IP για τον δρομολογητή-πύλη του δικτύου (network gateway).

Ακόμη και στην περίπτωση ενός μικρού δικτύου, όλος ο τρόπος σύνδεσης, ρύθμισης και εγκατάστασης είναι πολύπλοκο. Αν και υπάρχουν κάποια βοηθητικά πρωτόκολλα όπως το DHCP η το BOOTP, η διαδικασία σύνδεσης εξακολουθεί να είναι δύσκολη.

Το IPv6 δημιουργήθηκε για να λύσει τα παραπάνω προβλήματα καθώς ορίζει τις διαδικασίες εκείνες που χρειάζεται μια συσκευή να συνδεθεί αυτόματα, χωρίς δυσκολία και αυτό το καθιστά εύκολο για τον απλό χρήστη και έτσι να αποφεύγονται τα ανθρώπινα λάθη, όπως για παράδειγμα η απόδοση της ίδιας διεύθυνσης IP ταυτόχρονα σε δύο συσκευές. Λειτουργίες του IPv6 όπως αυτή του stateless auto-configuration, ή λειτουργία statefull autoconfiguration αυτοματοποιούν την διαδικασία απόδοσης της διεύθυνσης IP,χωρίς να χρειάζεται ο χρήστης να επέμβει σε κάποια ρύθμιση.

Επίσης , το πρωτόκολλο IPv6 δίνει την δυνατότητα να δημιουργηθούν περισσοτέρες από μια διευθύνση. Με άλλα λόγια, αν χρειάζεται ένας κόμβος να επικοινωνήσει με άλλο κόμβο στο ίδιο τοπικό δίκτυο ή στην ίδια διαχειριστική περιοχή ή γενικά στο Διαδίκτυο, ο κομβος IPv6 θα χρησιμοποιήσει ανάλογα μία από τις διαθέσιμες διευθύνσεις IPv6 που έχει συγκροτήσει

π.χ. μία από τις διευθύνσεις link local, ULA (πρώην site local) ή global.

Η ύπαρξη διαφορετικών τύπων καθιστά εύκολη την δημιουργία, διευκολύνει τις δικτυακές υπηρεσίες και συνάμα αυξάνει την ευρωστία (robustness) του δικτύου και την ασφάλεια των δικτυακών κόμβων.

4.1.2. Κινητικότητα χρηστών

Το IPv6 είναι χρήσιμο και για ακόμη ένα λόγο. Παρέχει αδιάκοπτα υπηρεσίες υψηλής ταχύτητας διασύνδεσης σε κινούμενους χρήστες και με αυτό τον τρόπο βελτιώνει την «κινητικότητα» (mobility) των χρηστών και υποστηρίζει στο μέγιστο την αδιάλειπτη περιαγωγή (roaming) μεταξύ ασύρματων δικτύων και δικτύων κινητής τηλεφωνίας (GSM/GPRS, UMTS).

Το IPv6 έχει προνοήσει τις απαιτήσεις που έχουν οι χρήστες που χρειάζεται να κινούνται και είναι βασισμένο στην υποδομή του IPv4 (Mobile IP). Βέβαια, η υποστήριξη στο IPv6 έχει βελτιωθεί κατά πολύ σε σχέση με το IPv4 αφού διαθέτει κατάλληλους μηχανισμούς όπως ο μηχανισμός που ρυθμίζει αυτόματα τους σταθμούς εργασίας

4.1.3. Ασφάλεια

Όσον αφορά τα θέματα ασφάλειας, το πρωτόκολλο IPv6 έχει διευκολύνει σε μεγάλο βαθμό την μετάδοση πληροφοριών ανάμεσα στις συσκευές που είναι συνδεδεμένες σε κάποιο δίκτυο. Κάθε κόμβος που χρησιμοποιεί το IPv6 παρέχει δυνατότητες κρυπτογράφησης ώστε να μεταδίδονται με ασφάλεια και να εξασφαλίζεται η ακεραιότητα των δεδομένων.

Συγκεκριμένα, είναι υποχρεωτική η χρήση του πρωτοκόλλου IPsec (IP security) από το IPv6 σε αντίθεση με το πρωτόκολλο IPv4 όπου η χρήση είναι προαιρετική.

4.1.4. Anycasting

Το πρωτόκολλο IPv6 υποστηρίζει το μηχανισμό anycast με τον οποίο ένας κόμβος μπορεί να απευθύνει ένα μήνυμα σε ένα σύνολο από παραλήπτες και το μήνυμα να παραδοθεί σε έναν από τους παραλήπτες (τον κοντινότερο στον αποστολέα όπως αυτό εκτιμάται με βάση μετρήσεις του δικτύου). Ο μηχανισμός αυτός επιτρέπει τη υλοποίηση εύρωστων υπηρεσιών αφού μπορούν να υπάρχουν περισσότεροι από ένας εξυπηρετητές που αντιστοιχούν σε μια διεύθυνση και εάν ένας δεν είναι διαθέσιμος τότε το δίκτυο θα φροντίσει να παραδώσει το μήνυμα σε κάποιον άλλο ώστε να εξυπηρετηθεί. Παράλληλα, επιτρέπει την (αυτόματη) κατανομή του φόρτου εργασίας σε περισσότερους από ένα εξυπηρετητές χωρίς να χρειάζεται καν ο αποστολέας να έχει γνωρίζει αν υπάρχει ένας η περισσότεροι εξυπηρετητές.

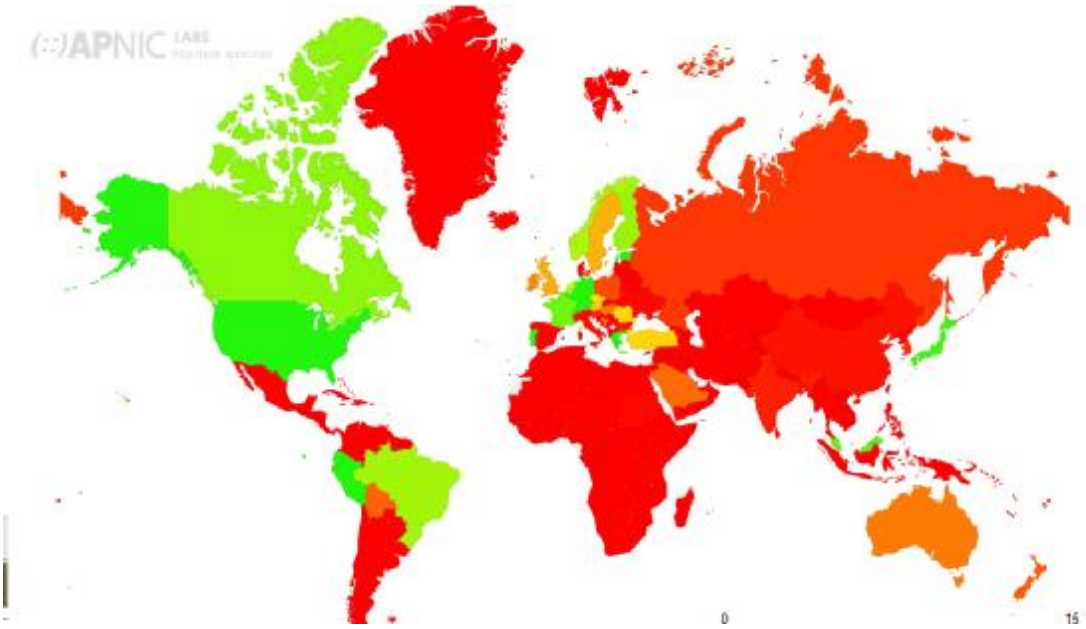
Το πρωτόκολλο IPv6 έχει καλύτερη υποστήριξη του μηχανισμού multicast, που επιτρέπει σε έναν κόμβο να απευθύνει ένα μήνυμα σε ένα σύνολο από παραλήπτες και το μήνυμα να παραδοθεί σε όλους τους παραλήπτες. Η καλύτερη υποστήριξη είναι εμφανής ειδικά για τους κινητούς κόμβους. Το IPv4 παρουσιάζει προβλήματα στην περίπτωση που ο κινητός κόμβος κάνει χρήση του μηχανισμού multicast. Όταν ο κινητός κόμβος δε βρίσκεται στο οικείο του (home) υποδίκτυο δεν μπορεί να αποστείλει multicast πακέτα. Αντίθετα στο IPv6 η υποστήριξη του μηχανισμού multicast είναι ενσωματωμένη και δεν παρουσιάζονται τέτοια προβλήματα. Τέλος το IPv6 προσφέρει καλύτερη διαχείριση της κυκλοφορίας των IP πακέτων αφού χρησιμοποιεί την τεχνική multicast καταργώντας την τεχνική broadcast, η χρήση της

οποίας έχει αποδειχθεί ότι είναι σημαντικός περιοριστικός παράγοντας στην απόδοση ενός δικτύου.

4.2 Χρήση διευθύνσεων IPv6

4.2.1 Σε παγκόσμιο επίπεδο

Στο παρακάτω σχήμα φαίνεται το ποσοστό υιοθέτησης του πρωτοκόλλου IPv6 σε παγκόσμιο επίπεδο. Με **κόκκινο** είναι οι χώρες οι οποίες δεν έχουν ακόμα την δυνατότητα χρήσης IPv6. Με **πράσινο** είναι οι χώρες που έχουν υιοθετήσει σε αρκετά ικανοποιητικό ποσοστό το IPv6 και με **κίτρινο** και **πορτοκαλί** είναι οι χώρες με πολύ μικρά αντίστοιχα ποσοστά υιοθέτησης του.



Σχήμα 14- Υιοθέτηση του IPv6 σε παγκόσμιο επίπεδο

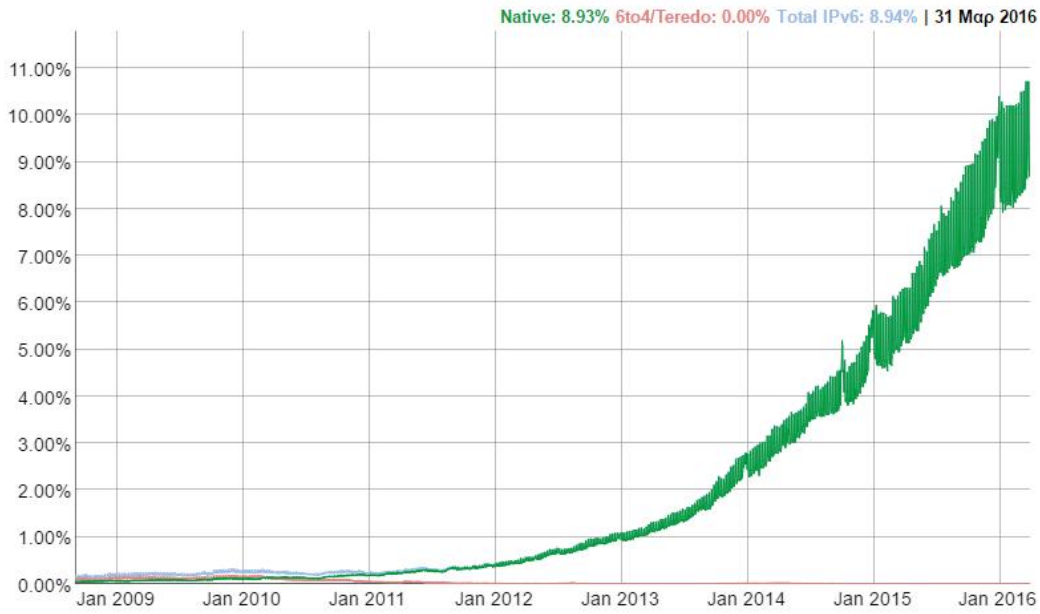
Στον ακόλουθο πίνακα παρουσιάζονται αναλυτικά ποσοστά χρήσης του IPv6 στις πέντε ηπείρους.

Code	Region	IPv6 Capable	IPv6 Preferred	Samples	Weight	Weighted Samples
XA	World	5.29%	4.70%	677741652	1	677741652
XC	Americas	15.76%	14.39%	133750485	1	133750281
XE	Europe	7.73%	7.08%	107831705	1	107825985
XF	Oceania	3.17%	2.77%	5434836	1	5436552
XD	Asia	1.73%	1.32%	360130982	1	360128192
XB	Africa	0.05%	0.04%	70593444	1	70600347
XG	Unclassified	0.00%	0.00%	3124920	0	15

Πίνακας 13-ποσοστά χρήσης διευθύνσεων IPv6 ανά Ήπειρο

Οι εκτιμήσεις κάνουν λόγο για 50% χρήση σε παγκόσμιο επίπεδο μέχρι το 2020.

Στον ακόλουθο πίνακα παρουσιάζονται οι στατιστικές μετρήσεις της εταιρίας GOOGLE για την υιοθέτηση του IPv6 σε παγκόσμια κλίμακα. Το γράφημα δείχνει το ποσοστό των χρηστών που έχουν πρόσβαση στην google χρησιμοποιώντας το IPv6.



4.2.2 Σε εγχώριο επίπεδο (Ελλάδα)

Στην Ελλάδα έχει παρουσιαστεί σημαντική αύξηση της χρήσης του IPv6 και αυτό οφείλεται καταρχήν στην δυνατότητα χρήσης που δίνουν οι πάροχοι των υπηρεσιών διαδικτύου. Μέσα σε περίοδο 6 μηνών μεταξύ του έτους 2014 και 2015 το ποσοστό χρήσης διπλασιάστηκε από 10% σε 20%.

Στο παρακάτω πίνακα φαίνεται η κατάταξη της Ελλάδας στην 5^{η} θέση (σύμφωνα με την Akamai) σε παγκόσμιο επίπεδο στην χτήση του πρωτοκόλλου IPv6.

CC	Country	IPv6 Capable	IPv6 Preferred	Samples	Weight	Weighted Samples
BE	Belgium, Western Europe, Europe	50.00%	47.65%	2530825	0.76	1914721
CH	Switzerland, Western Europe, Europe	30.94%	29.75%	1433369	1.04	1486321
US	United States of America, Northern America, Americas	30.04%	27.31%	86537575	0.67	57675136
PT	Portugal, Southern Europe, Europe	28.63%	27.68%	5035222	0.26	1315984
GR	Greece, Southern Europe, Europe	23.91%	23.33%	6914622	0.19	1344537
DE	Germany, Western Europe, Europe	22.26%	19.96%	1162400	12.28	14279948
AP	Asia Pacific code, Unclassified, World	20.22%	0.01%	155999	0	0
PE	Peru, South America, Americas	18.34%	17.55%	3935220	0.69	2707848
LU	Luxembourg, Western Europe, Europe	16.47%	15.27%	361635	0.31	110327
EE	Estonia, Northern Europe, Europe	15.65%	15.09%	643844	0.33	215236
JP	Japan, Eastern Asia, Asia	14.52%	11.28%	3747349	6.28	23515737
EC	Ecuador, South America, Americas	13.80%	13.38%	3491196	0.74	2589752
MY	Malaysia, South-Eastern Asia, Asia	12.10%	10.53%	6734780	0.63	4240304
NO	Norway, Northern Europe, Europe	11.69%	10.95%	1141497	0.9	1023911
EU	European Union, Western Europe, Europe	11.83%	0.18%	296264	0	0
AT	Austria, Western Europe, Europe	10.47%	10.10%	766275	1.85	1416629
FI	Finland, Northern Europe, Europe	10.40%	9.63%	1123423	0.92	1036334
CZ	Czech Republic, Eastern Europe, Europe	9.59%	9.03%	1619605	0.99	1604519
CA	Canada, Northern America, Americas	9.33%	8.60%	4566451	1.54	7030485

Πίνακας 14 - Κατάταξη της Ελλάδας όσο αναφορά την χρήση IPv6 (Σε παγκόσμιο επίπεδο)

Στην ελληνική εταιρία Forthnet ήδη η πλειοψηφία (~58%) των συνδρομητών χρησιμοποιεί Dual-Stack για την σύνδεση στο Internet, ενώ ένα αρκετά σημαντικό ποσοστό συνδέεται με DS-Lite παρακάμπτοντας το IPv4. Σημαντική αύξηση υπάρχει και στην IPv6 κίνηση, αφού έχει ξεπεράσει το 27% της συνολικής.

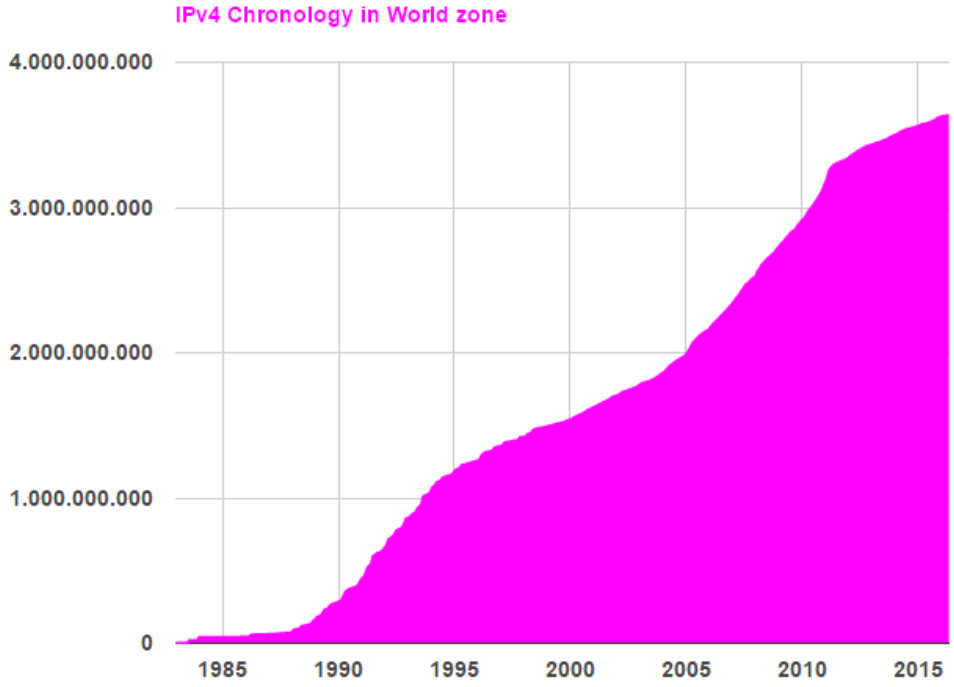
Στην Ελλάδα, Το Εθνικό Δίκτυο Έρευνας & Τεχνολογίας - ΕΔΕΤ έχει αναβαθμίσει το ερευνητικό και εκπαιδευτικό δίκτυο της χώρας, ώστε να υποστηρίζει προηγμένες υπηρεσίες διασύνδεσης με την χρήση του πρωτοκόλλου IPv6. Από το 2003, το μητοπολιτικό δίκτυο της Αθήνας επιτρέπει τη διασύνδεση των εκπαιδευτικών ιδρυμάτων της ευρύτερης περιοχής της Αττικής σε πολύ γρήγορες ταχύτητες, με τον συνδυασμό χρήσης των πρωτοκόλλων IPv4 και IPv6. Επίσης Οι δυνατότητες της διασύνδεσης IPv6 επεκτάθηκαν περισσότερο και το 2004 πραγματοποιήθηκε ο καινούριος κορμός δικτύου ΕΔΕΤ2.

Η προσπάθεια αυτή θα προσφέρει στην ερευνητική και εκπαιδευτική κοινότητα της χώρας δυνατότητες ισότιμης συνεργασίας με αντίστοιχους φορείς της Ευρώπης, Αμερικής και Ασίας ενώ θα προωθήσει την έρευνα μέσα στα ακαδημαϊκά και ερευνητικά μας ιδρύματα. Το Πανελλήνιο Σχολικό Δίκτυο-ΠΣΔ (www.sch.gr) αποτελεί το δίκτυο μέσω του οποίου διασυνδέεται η πλειονότητα των σχολείων της πρωτοβάθμιας και δευτεροβάθμιας εκπαίδευσης καθώς και διοικητικές μονάδες του Υπουργείου Εθνικής Παιδείας και Θρησκευμάτων (ΥΠΕΠΘ).

4.3. Εξάντληση IPv4

Όπως αναφέρθηκε σε προηγούμενο κεφάλαιο, η αύξηση του παγκόσμιου διαδικτύου αυξάνεται με εκθετικό ρυθμό έτσι ώστε το μέγεθός του να διπλασιάζεται σε λιγότερο από ένα χρόνο. Με το σημερινό ρυθμό αύξησης όλα τα διαθέσιμα προθέματα δικτύων που υπάρχουν, σύντομα θα αποδοθούν με αποτέλεσμα τη μη δυνατή περεταίρω ανάπτυξη του διαδικτύου. Οι συνολικές διαθέσιμες διευθύνσεις IPv4 είναι περίπου 4.3 δισεκατομμύρια. Αυτή την στιγμή έχουν διατεθεί σε παγκόσμιο επίπεδο περίπου 3,7 δισεκατομμύρια IPv4 διευθύνσεις. Αυτό σημαίνει πως πολύ σύντομα θα εξαντληθούν οι IPv4 διευθύνσεις λόγω της συνεχής αυξανόμενης ανάγκης για νέες διευθύνσεις.

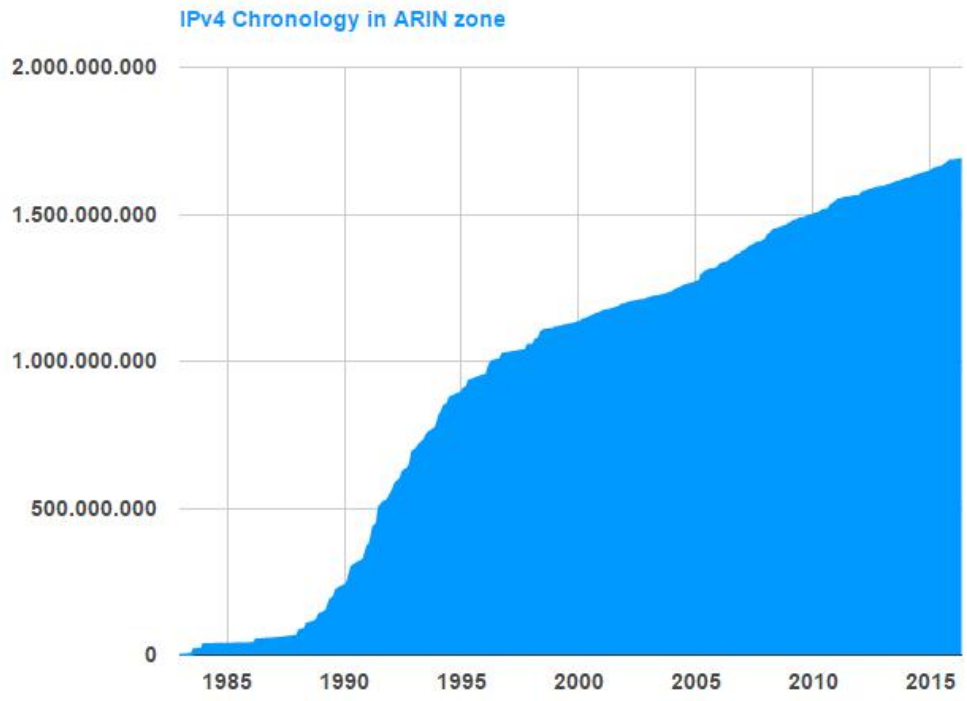
Στον πίνακα 15 φαίνεται σε παγόσμιο επίπεδο η εξάντληση του IPv4



Πίνακας 15–εξάντληση των IPv4 διευθύνσεων

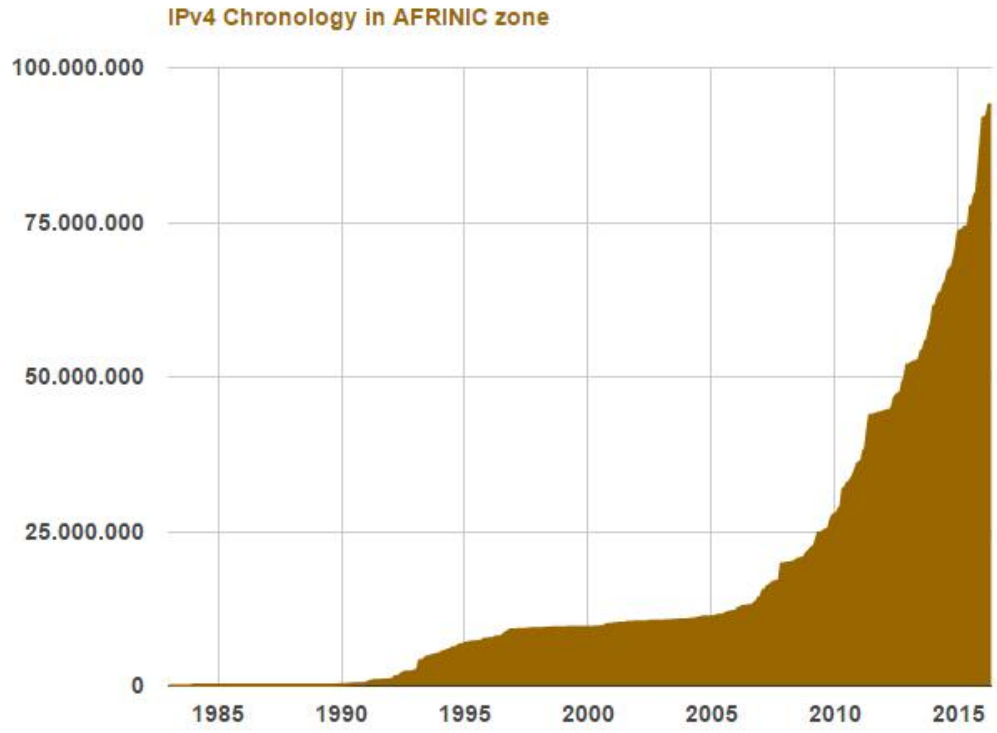
Παρακάτω παρουσιάζεται το ποσοστό χρήσης ανα RIRτου πρωτοκόλλου IPv4:

ARIN



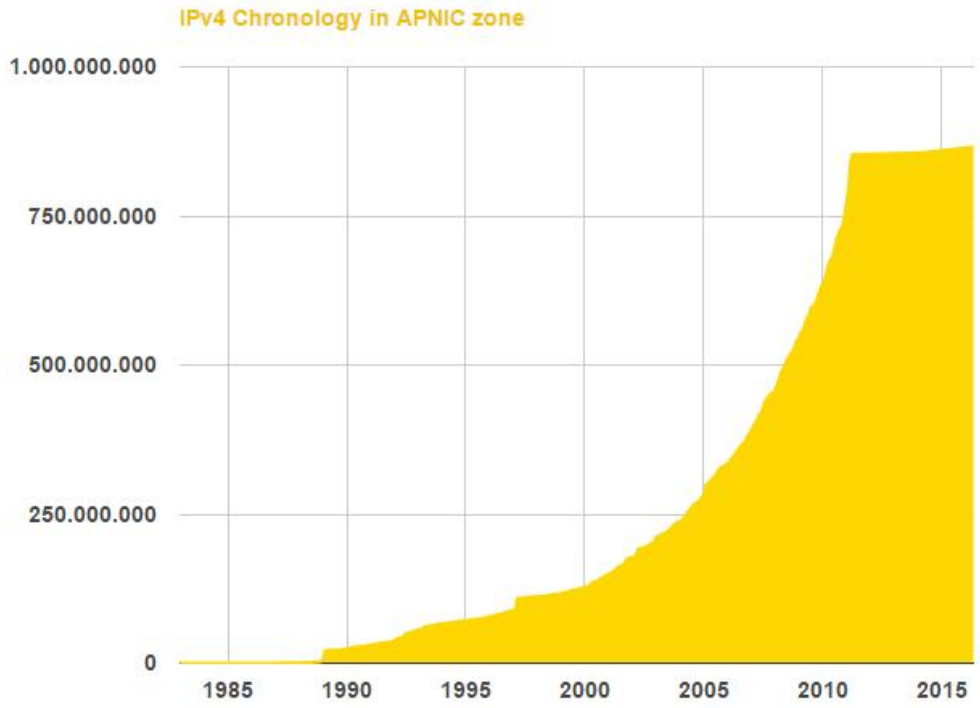
Πίνακας 16–Διατειθέμενες IPv4 διευθύνσεις του ARIN

AFRINIC



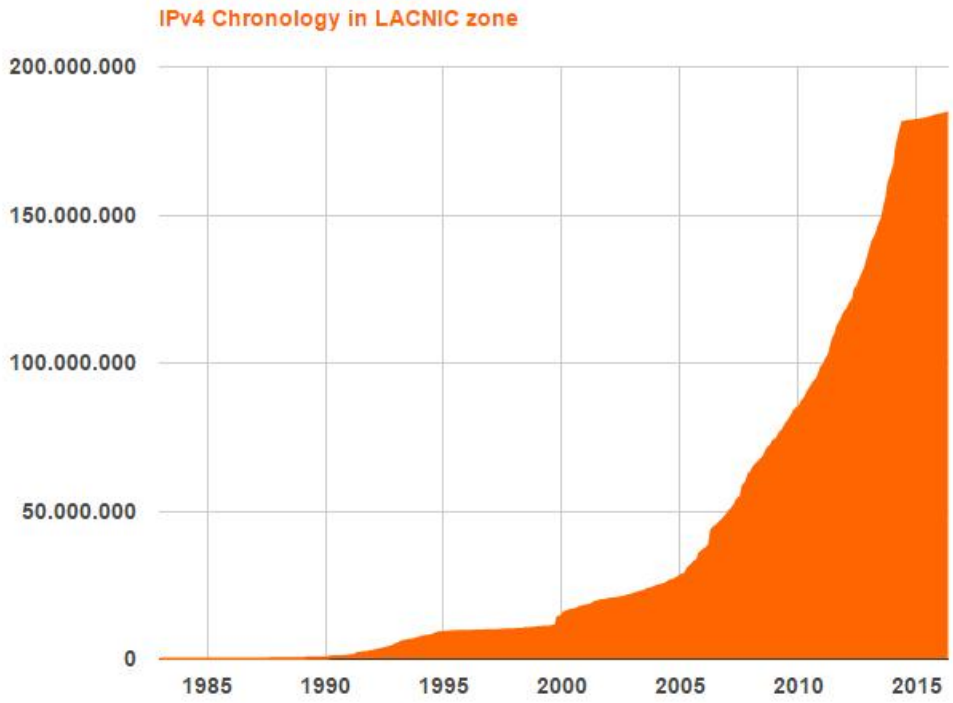
Πίνακας 17–Διατειθέμενες IPv4 διευθύνσεις του AFRINIC

APNIC



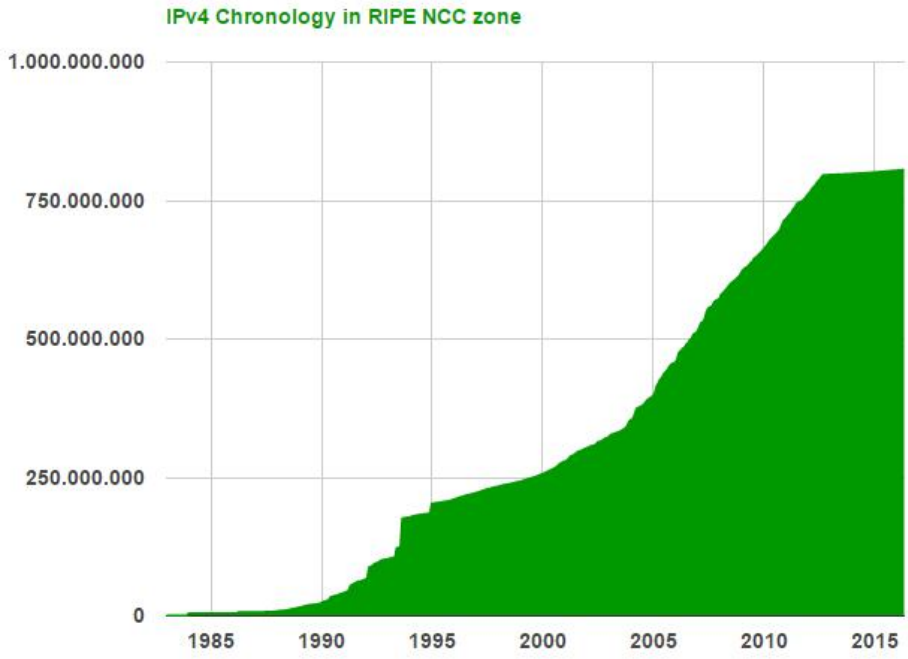
Πίνακας 18–Διατειθέμενες IPv4 διευθύνσεις του APNIC

LACNIC



Πίνακας 19–Διατειθέμενες IPv4 διευθύνσεις του LACNIC

RIPE



Πίνακας20–Διατειθέμενες IPv4 διευθύνσεις του RIPE

ΣΥΜΠΕΡΑΣΜΑΤΑ

Το πρωτόκολλο IPv6 υπερτερεί σε πολλά σημεία σε σχέση με το πρωτόκολλο IPv4. Τα δυνατά σημεία του και τα πλεονεκτήματα του έχουν αναφερθεί και έχουν αναλυθεί παραπάνω τα οφέλη. Όλα αυτά τα οφέλη μπορούν να ικανοποιήσουν τις αυξανόμενες ανάγκες των χρηστών του διαδικτύου.

Παρ' όλα αυτά η μετάβαση από το πρωτόκολλο Ipv4 στο πρωτόκολλο IPv6 δεν γίνεται με ικανοποιητικούς ρυθμούς. Ένας από τους βασικούς λόγους είναι η εξάπλωση του IPv4 και το γεγονός ότι ακόμη χρησιμοποείται ευρέως. Με άλλα λόγια, υπάρχει προς το παρόν μια απροθυμία από τους ISP να χρησιμοποιήσουν τους μηχανισμούς μετάβασης. Θα έπρεπε όμως οι εταιρίες των παρόχων να κατανοήσουν πλήρων τα οφέλη της μετάβασης.

Η μετάβαση αυτή απαιτεί σωστό σχεδιασμό και οργάνωση προκειμένου να γίνει με οικονομικό τρόπο και χωρίς να προκαλέσει προβλήματα στη λειτουργία του δικτύου. Οι τεχνικές και η εμπειρία από αντίστοιχες περιπτώσεις υπάρχουν και η μετάβαση είναι εφικτή. Αρκεί μόνο να γίνει κατανοητό ότι η μετάβαση θα επιφέρει οφέλη και πως η όποια καθυστέρηση στην αποδοχή και εφαρμογή της τεχνολογίας IPv6, οδηγεί σε μειονεκτική θέση.

ΒΙΒΛΙΟΓΡΑΦΙΑ–ΑΝΑΦΟΡΕΣ

- Leiner B.,Cerf V., Clark D. (2009) *A Brief History of the Internet,* ACM SIGCOMM Computer 0Communication Review

- Raphael C. (2011),*Internet History,* International Journal of Technoethics, 2(2), 45-64, April-June 2011

- Thomas G. (1999), *Introduction to the Internet Protocol*, published in www.ccontrols.com, volume 1, issue 4

- Goralski W, (2014), *Learn About Differences in Addressing Between IPv4 and IPv6*, Juniper Networks

- Alied Telesis(2008) , AlliedWare *OS Software Reference*, chapter 15, published: http://www.alliedtelesis.com/media/fount/software_reference/291/at8600/8600sr.pdf

- Hagen S. (2006) , "IPv6 Essentials" 2nd Edition, O'Reilly Media, May 2006.

- Olabenjo Babatunde , Omar Al-Debagy(2014) *A Comparative Review Of Internet Protocol Version 4 (IPv4) and Internet Protocol Version 6 (IPv6),*International Journal of Computer Trends and Technology (IJCTT) – volume 13 number 1 – Jul 2014

- J. Davies (2003) , "Understanding IPv6", 1st Edition
- Bechrouz a. Forouzan (2010) *TCP/IP Protocol suite* , fourth edition

- R. Gilligan, E. Nordmark, (2000) *Transition Mechanisms for IPv6 Hosts and Routers*, RFC 2893, August 2000.

- E. Nordmark, R. Gilligan (2005) *, Basic Transition Mechanisms for IPv6 Hosts and Routers* , Work in Progress, March 2005.

- Amer Nizar (2012) Abu Ali, *Comparison study between IPV4 & IPV6* Philadelphia University, Jordan, CIS department, IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 3, No 1, May 2012

- M. Blanchet (2006*), Migrating to IPv6 A Practical Guide to Implementing IPv6 in Mobile and Fixed Networks, Quıbec, Canada*
- B. Carpenter, K. Moore (2001) , *Connection of IPv6 Domains via IPv4 Clouds,* RFC 3056, February 2001.
- C. Huitema (2001*) An Anycast Prefix for 6to4 Relay Routers* , RFC 3068, June 2001.
- Xianhui Che, Dylan Lewis,(2010) *IPv6: Current Deployment and Migration Status, International Journal of Research and Reviews in Computer Science* (IJRRCS) Vol. 1, No. 2, June 2010
- P. Savola, C. Patel, "Security Considerations for 6to4", RFC 3964, December 2004.
- R. Gilligan, E. Nordmark, "Transition Mechanisms for IPv6 Hosts and Rout-ers", RFC 2893, August 2000.
- E. Nordmark, R. Gilligan, "Basic Transition Mechanisms for IPv6 Hosts and Routers", Work in Progress, March 2005.
- G. Tsirtsis, P. Srisuresh, "Network Address Translation - Protocol Translation (NAT-PT)", RFC 2766, February 2000.
- J. Abley, B. Black, V. Gill, "Goals for IPv6 Site-Multihoming Architectures", RFC 3582, August 2003.
- RFC 2740 “OSPF for IPv6”
- Cisco(2002), IPv6 Routing: OSPFv3
- An introduction to IANA, Presentation Notes, Date 29 September 2008 Kim Davies
- APNIC (2016): https://www.apnic.net/about-APNIC/organization/history-of-apnic/history-of-the-internet2/4
- Ripe (2006): https://www.ripe.net/support/training/material/LIR-Training-Course/LIR-Training-Slides.pdf

· H. Balakrishnan(2009) *Wide-Area Internet Routing* , Massachusetts Institute of Technology Department of Electrical Engineering and Computer Science 6.033January 2009

· P.Smith (2010) Cisco BGP Techniques for Internet Service Providers

· J.Davies (2012) *Understanding IPv6,* third edition

· M. Hill, A. Barnes (2011) *End-User Computing Applications Kennesaw State University,* State University, Faculty Publications

· P. Savola, and C. Patel (2004) , "Security Considerations for 6to4", RFC 3964, December 2004.

· R. Gilligan and E. Nordmark, "Transition Mechanisms for IPv6 Hosts and Routers", RFC 2893, August 2000.

· E. Nordmark and R. Gilligan, "Basic Transition Mechanisms for IPv6 Hosts and Routers", Work in Progress, March, 2005.

· B. Carpenter and C. Jung, "Transmission of IPv6 over IPv4 Domains without Explicit Tunnels", RFC 2529

· http://ccm.net/contents/713-isp-internet-service-providers

· https://en.wikipedia.org/wiki/IPv4

· https://el.wikipedia.org/wiki/ISP

· https://www.arin.net/knowledge/4byte_asns.pdf

· https://en.wikipedia.org/wiki/Local_Internet_registry

· https://en.wikipedia.org/wiki/Autonomous_system_(Internet)

- http://www.adslgr.com/forum/threads/732186
- https://www-public.tem-tsp.eu/~maigron/RIR_Stats/RIR_Delegations/World/IPv4-ByNb.html
- http://www.tcpipguide.com
- http://stats.labs.apnic.net/ipv6
- http://stats.labs.apnic.net/ipv6/XA
- https://www.google.com/intl/en/ipv6/statistics.html